

004
554

D.A. DAVRONBEKOV, SH. U.PULATOV, M.O.SULTONOVA,
U.T. ALIYEV, E.B.TASHMANOV



SIMSIZ KENG POLOSALI TEXNOLOGIYALAR

O'ZBEKISTON RESPUBLIKASI AXBOROT
TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI
RIVOJLANTIRISH VAZIRLIGI

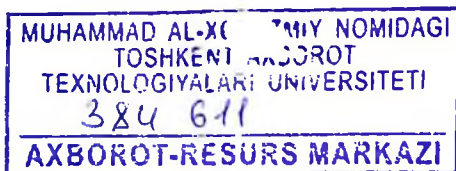
MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI
UNIVERSITETI

D.A. DAVRONBEKOV, SH. U.PULATOV,
M.O.SULTONOVA, U.T. ALIYEV, E.B.TASHMANOV.

SIMSIZ KENG POLOSALI TEXNOLOGIYALAR

Darslik

(Telekommunikatsiya texnologiyalari – 5350100 ta'lim
yo'nalishi uchun)



TOSHKENT – 2018

UO‘K: 004.738.5

KBK: 32.973.202

S 57

D.A. Davronbekov, Sh. U.Pulatov, M.O.Sultonova, U.T. Aliyev, E.B.Tashmanov. Simsiz keng polosali texnologiyalar. T.: «Aloqachi», 2018, 304 b.

ISBN 978–9943–5569–7–3

Oliy ta’limning davlat ta’lim standartiga ko’ra ishlab chiqarish va texnik sohalarida o’qitiladigan “Simsiz keng polosali texnologiyalar” fanining maqsadi telekommunikatsiya sohasi bo’yicha ta’lim oluvchi talabalar tomonidan zamonaviy axborot va telekommunikatsiya tizimlarida tobora keng qo’llanilayotgan simsiz keng polosali texnologiyalarga oid bilimlar, ko’nikmalar va malakani egallashga qaratilgandir. Bunda mavzularning ma’no jihatdan ketma-ketligi o’quv jarayonining modul tamoyillariga va qo’shimcha o’quv axborotini olishga hamda talabalar bilimlarini mustahkamlashga undaydi.

Darslik 5350100–Telekommunikatsiya texnologiyalari ta’lim yo’nalishi bo’yicha mutaxassislarni tayyorlashda o’quv jarayonida foydalanish uchun mo’ljallangan.

UO‘K: 004.738.5

KBK: 32.973.202

S 57

Mufliflar: D.A. Davronbekov, Sh. U.Pulatov, M.O.Sultonova, U.T. Aliyev. E.B.Tashmanov

Taqrizchilar:

PhD M. Djalalov “UNICON.UZ” DUK direktor o’rinbosari,

prof. A.M.Nazarov I.Karimov nomidagi TDTU “Radiotexnika tizimlari va qurilmalari” kafedrası mudiri,

ISBN 978–9943–5569–7–3

© «Aloqachi» nashriyoti, 2018.

KIRISH

Ma'lumki, O'zbekiston Respublikasi Prezidenti Sh.Mirziyoevning 2018 yil 3 fevraldagi "O'zbekiston Respublikasi turizm salohiyatini rivojlantirish uchun qulay sharoitlar yaratish bo'yicha qo'shimcha tashkiliy chora-tadbirlar to'g'risida" 5326-sonli Farmonida - jamoat joylarida Internet tarmog'iga simsiz bepul ulanish hududlarini (Wi-Fi) barpo etgan operatorlar, provayderlar va boshqa xo'jalik yurituvchi sub'ektlar foydalanuvchilarning shaxsini majburiy tartibda aniqlagan holda tegishli sifatdagi ulanishni ta'minlashlari lozim; o'z hududida Internet tarmog'iga simsiz bepul ulanish hududlarini (Wi-Fi) o'rnatgan xo'jalik yurituvchi sub'ektlarning soliq solinadigan bazasi, shu jumladan yagona soliq to'lovi bo'yicha bazasi tegishli sifatdagi simsiz ulanish hududini kengaytirish uchun asbob-uskunalarni xarid qilish va internet-trafikni sotib olishga yo'naltirilgan xarajatlar miqdoriga kamaytiriladi; Internet tarmog'iga simsiz bepul ulanish hududlarida (Wi-Fi) taqdim etilayotgan xizmatlar sifatini nazorat qilish Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi huzuridagi Aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari sohasida nazorat bo'yicha davlat inspeksiyasi tomonidan amalga oshiriladi" – deb ma'ruza qilgan edi [1].

So'nggi yillarda ma'lumotlarni simsiz uzatish tarmoqlari telekommunikatsion industriyaning rivojlantirishning asosiy yo'nalishlaridan biri bo'lib qoldi. Texnologiyalar o'zgardi, lekin uzatishning mazmuni – ma'lumotlar berilgan vaqtda bitta nuqtadan boshqasiga kelishi uchun bir necha turli elementlarni o'zaro ta'sirlashishini tashkil etish o'zgarmasdan qoldi.

Butun dunyoda va O'zbekistonda ma'lumotlarni uzatish tarmoqlarining keskin rivojlanishi quyidagi afzalliklarga bog'liq bo'ldi:

- arxitekturaning tez moslashuvchanligi, ya'ni mobil foydalanuvchilarning ulanishida, harakatlanishida va uzilishida vaqtning sezilarli yo'qotilishlarisiz tarmoqning topologiyasini dinamik o'zgartirish imkoniyati;

- ma'lumotlarni yuqori uzatish tezliklari;
- loyihalashtirish va qurishning tezkorligi;
- ruxsat etilmagan ulanishdan yuqori himoyalanganlik darajasi;

- qimmat turadigan va hamma vaqt ham mumkin bo'lmaydigan optik tolali yoki mis kabelni yotqizish va ijaraga olishni rad etish [4].

Simsiz axborot tizimlari va tarmoqlari yanada katta ommaviylikka ega bo'lib bormoqda, chunki ular an'anaviy simli tarmoqlarga qaraganda qator afzalliklarga ega. Lekin chastotalar spektrining litsenziyalanmaydigan diapazonida ishlaydigan foydalanuvchilarning katta soni halaqitlarning ortishiga va har bir ma'lum tarmoqdagi shovqin darajasining oshishiga olib keladi. Tarmoqning unumdorligiga boshqa radiotexnik vositalarning ishlashi keltirib chiqaradigan halaqitlar ham sezilarli ta'sir qiladi.

Radiotizimlar zamonaviy atamashunoslikda tor polosali va keng polosali radioaloqa tizimlariga bo'linadi. Farq, avvalo qo'llaniladigan tebranishlar tashuvchilari tuzilmalaridan iborat. Tor polosali tizimlarga kiradigan an'anaviy radiovositalar signal tashuvchisi sifatida bir chastotali garmonik tebranishlarni ishlatadi. Bunday tizimlardagi ajratilgan chastotalar diapazonida ko'plab foydalanuvchilarning ishlashi imkoniyatini ta'minlash uchun uzatiladigan signallar chastotalari polosalarini iloji boricha kamaytirishga uriniladi. Keng polosali aloqa tizimlarida tebranishlar tashuvchilari sifatida keng polosali psevdotasodifiy signallar qo'llaniladi. Bunda har bir foydalanuvchining signali chastotalar diapazonining butun ajratilgan oralig'ini egallaydi, alohida signallarni ajratish esa kodli usullarda amalga oshirildi.

IEEE 802.11 standarti ma'lumotlar simsiz keng polosali uzatish tarmoqlarining keskin kengayishi, RadioEthernetdan foydalanish bilan radiokanal bo'yicha Internet tarmog'iga ulanish xizmatlarini taqdim etadigan operatorlar sonining, shuningdek bu xizmatlar foydalanuvchilari sonining ortishi elektromagnit moslashuvchanlik muammosiga olib keldi. Ayniqsa, bu RadioEthernet-provayderlar soni 5-10 taga yetadigan yirik shaharlar uchun xarakterli bo'lib qoldi. Natijada 2,4-2,5 GGs chastotalar diapazoni kuchli o'ta yuklangan va shovqinlashgan bo'lib qoldi [12].

Shovqinlashganlik muammosi ko'rsatilgan diapazon yaqinida GSM-1800 sotali aloqa, radioreleli aloqa tizimlari, idoraviy va tijorat ma'lumotlarni uzatish tarmoqlari va boshqalar intensiv ishlaydigan boshqa hududlar uchun ham dolzarb bo'lib qolmoqda. Bunday vaziyatning yakuniy natijasi radioaloqa sifatining yomonlashishi va mos ravishda oxirgi foydalanuvchiga ko'rsatiladigan xizmatlar

sifatining yomonlashishi bo‘lib qoldi. Bundan tashqari, yaqin vaqtlarda RadioEthernetga yaqin 2,5-2,7 GGs dipazonda ishlaydigan MMDS texnologiyasi asosidagi keng polosali simsiz ulanish tizimlarning qurilishi keltirib chiqaradigan vaziyatning qo‘shimcha o‘tkirlashishi kutilmoqda.

Yuzaga kelgan vaziyat ma’lumotlarni uzatish tarmoqlari operatorlarini o‘z tizimlari radiokanallarida halaqilar sathlarini kamaytirish uchun usullar va vositalarni izlashga majburlamoqda. Shunga ko‘ra, halaqitbardoshlikni oshirish masalalarini yechilishining bo‘lishi mumkin yo‘llarini, ma’lumotlarni simsiz uzatish tarmoqlarida radioaloqa sifatini yaxshilashga asosiy yondashishlarni tahlil qilish dolzarb hisoblanadi.

1-BOB. SIMSIZ KENG POLOSALI ALOQA TIZIMLARINING RIVOJLANISHI

1.1. Simsiz keng polosali ulanish texnologiyalarning rivojlanish tarixi va tavsifi

Simsiz keng polosali ulanish (SKPU) texnologiyalari infokommunikatsion texnologiyalarning nimsinfi hisoblanadi va bir-biridan olisdagi ikki va undan ortiq ob'ektlar oralig'ida simli ulanishsiz axborot uzatish uchun ishlatiladi. Simsiz aloqa uchun radioto'lqinlar, infraqizil, optik yoki lazerli nurlanishlar ishlatilishi mumkin. Hozirgi vaqtda foydalanuvchilarga Wi-Fi, WiMAX, Bluetooth, RFID, ZigBee kabi "tijorat" nomlari bilan ma'lum bo'lgan ko'plab simsiz texnologiyalar mavjud. Ularni har biri o'zining qo'llanish sohasini aniqlaydigan ma'lum xarakteristikalar to'plamlariga ega [23].

Simsiz keng polosali ulanish texnologiyalari simsiz va tarmoq texnologiyalari sinergiyasi namunasi hisoblanadi va juda katta rivojlanish istiqboliga ega. Shu sabab simsiz keng polosali texnologiyalar tarixining boshlanishi deb, qaysidur ma'noda, ilk radioaloqa paydo bo'lishini hisoblash mumkin. Ma'lumki, radioaloqaning birinchi omadli sinovlari 1893 yilda serb olimi Nikola Tesla, keyinchalik 1895 yilda A.S.Popov va Italiyalik Guglielmo Markoni (*Guglielmo Marconi*) tomonlaridan bir-birlaridan mustaqil ravishda amalga oshirildi. Bu kashfiyotlar birinchi marta simsiz axborot uzatish imkoniyatini ko'rsatdi va bu bilan aloqa rivojlanishi tarixida yangi erani boshladi. Keyin esa insoniyat qadamma-qadam simsiz aloqa va axborot uzatish tizimlarida yanada katta yutuqlarga erishdi, xususan:

- XX asrning 20 yillarida amplitudaviy modulyatsiyaning birinchi tijorat radiobloklari paydo bo'ldi;
- 1933 yilda chastotaviy modulyatsiyali radio kashf qilindi va televidenie paydo bo'ldi;
- 1946 yilda AT&T va Bell Systems (AQSh) kompaniyalari bo'lajak sotali tizimlarning timsoli bo'lgan harakatdagi telefon aloqa tajriba tizimini (ingl. *MTS*) ishga tushirishdi;
- 70 yillarning oxirlarida sotali aloqaning birinchi avlod - 1G tizimlari ishga tushirildi;

- 1973 yilda lokal kompyuter tarmoqlarning birinchi protokoli - Ethernet ishlab chiqildi (keyinchalik u IEEE 802.3 maqomini oldi);
- 80 yillarda ma'lumot uzatish bo'yicha harbiy tizim - ARPANET dastlab milliy, keyin esa xalqaro miqyosdagi umumiy foydalanish tarmog'i - INTERNET ga aylandi.
- XX asrning 90 yillarining boshida ma'lumot uzatish tarmoqlariga simsiz keng polosali ulanish usulining birinchi ishlanmalari paydo bo'ldi.

Shunday qilib, simsiz (avvalom bor, sotali) texnologiyalar simli (tarmoq) texnologiyalarning shiddatli rivojlanishi bilan chambarchas holda, hamda kompyuter va Internet texnologiyalarining ommaviylashishi tufayli hayotimizga uzluksiz holda kirib kelmoqda va tezkor rivojlanib, o'zlari ham yangi xizmatlar va qurilmalar yaratilishiga zamin bo'lmoqda [5].

Shu munosabat bilan simsiz texnologiyalarining lokal (WLAN), o'rta va qisqa masofalardagi (WPAN) va shahar va tuman ko'lamlaridagi (WMAN) tarmoqlarini rivojlanishi istiqbolli hisoblanadi.

Simsiz texnologiyalar standartlarini ishlab chiqishning boshlang'ich nuqtasi sifatida 1989 yilda IEEE (Elektronika va elektrotexnika bo'yicha muhandislar instituti) qoshida 802.11 qo'mitasi tashkil etilishi hisoblanadi. Qo'mita birinchi navbatda kichik (lokal) o'lchamlardagi simsiz tarmoqlarni ishlab chiqish bilan shug'ullandi va shu asnoda Wi-Fi tizimlari paydo bo'ldi. Ushbu g'oya asta-sekin "so'ngi milya" aloqasi va shahar hamda hududiy tarmoqlar uchun ham qo'llana boshladi va bu o'tgan asrning 90- yillarining oxirlarida IEEE 802.16 (WiMAX) standartlar guruhini paydo bo'lishiga olib keldi [8].

Hozirgi vaqtda Wi-Fi va WiMAX tizimlari yanada ommaviylashib bormoqda. Simsiz texnologiyalar foydalanuvchilarining eng o'suvchi segmenti sifatida korporativ mijozlar (ya'ni, tashkilot ishchilari) bo'lmoqdalar. Ma'lumotlarni simsiz uzatish xizmati muhim strategik vosita bo'lib qolmoqda: u mehnat unumdorligini oshirmoqda (xizmatchilar korporativ axborotlarga har doim va har joyda ulana olishadi, yangiliklar haqida tezroq xabardor bo'lishadi), mijozlarga ko'rsatilayotgan xizmatlar sifatini oshirmoqda (mijozlar talablarini tezroq qabul qilib, ularni tezroq qondirish mumkin) va raqobatli afzalliklarni yaratmoqda

(axborot almashuvi tezligini oshirish va shu bilan qaror qabul qilish tezligini ham oshirish mumkin).

Simsiz texnologiyalarning rivojlanishida uy foydalanuvchilari ham katta rol o'ynashadi. Uy tarmog'ida qancha ko'p qurilmalar bo'lsa, ularni bog'laydigan simlar ham uyni shunchalik kuchli o'rab oladi. Va bu simsiz texnologiyalarga o'tishga sabab bo'ladi. Zamonaviy uyning qulaylik darajasini oshirish, ya'ni uning barcha tuzilmalari va ob'ektlarini (kompyuterlar, televizor, raqamli fotokamera, uy musiqiy markazi, qo'riqlash tizimi, iqlim tizimi, maishiy texnika va boshqalar) bir tizimga birlashtirish – bu “aqli uy” g'oyasining asosidir va bunda simsiz texnologiyalardan foydalanish ko'zda tutilgan.

Bu yerda shuni ta'kidlab ketish zarurki, simsiz keng polosali texnologiyalarning rivojlanishi axborot xavfsizligini ta'minlash masalalarini yanada dolzarb qiladi. Simsiz tarmoqlar ishlatilganda asosiy tahdidlar xabarlarini, parollarni, kredit kartochkalar nomerlarini ilib olish, to'langan ulanish vaqtini o'g'irlash, kommunikatsion markazlar ishiga aralashish va boshqalar hisoblanadi. Bu muammolar aloqa standartlarini takomillashtirish jarayonida hal qilinadi [2].

1.2. Simsiz keng polosali simsiz texnologiyalarni tasniflashga yondashishlar

Simsiz texnologiyalar nazariyasida ularni tasniflashda turli yondashishlar mavjud. Jumladan, raqamli va analog, tor va keng polosali texnologiyalar ajratiladi. Bu ajratishlarga aniqlik kiritish uchun bir qancha tushuntirishlarni keltiramiz.

Raqamli texnologiyalar xaqida gap ketganda ko'pincha signal ham raqamli (diskret) shaklga ega bo'lishi tushuniladi. Bu tushuncha ko'proq simli tarmoqlar uchun to'g'ri bo'ladi. Simsiz tarmoqlarda esa “raqamli” belgisi radiokanal orqali uzatiladigan axborotlarga tegishli, ammo radiosignalni o'zi esa hali ham garmonika shaklidagi modulyatsiyalangan analog signali bo'ladi.

Tor va keng polosali tizimlar orasidagi farqni ham oson aniqlab bo'lmaydi (ular orasidagi chegara ham texnologiyalar rivojlangan sari yuqoriga siljimoqda). Shuningdek, bu belgiga nisbatan ham simli va simsiz texnologiyalarda qabul qilingan tushunchalar orasida farq kuzatiladi. Masalan, simli tarmoq texnologiyalarida ma'lumotni tor polosada (ingl. *baseband*) uzatish deganda raqamli uzatish shakli

tushuniladi (ya'ni, diskret elektr yoki optik impulslar vositasi bilan). Va aksincha, keng polosa (angl. *broadband*) sifatida elektron yoki optik to'liqlarni ishlatadigan analog kanallar nazarda tutiladi. Simsiz tarmoqlarda nazariy qabul qilinishicha, ishchi polosasining kengligi F bu polosaning markaziy chastotasi f_c dan ancha kam (ya'ni, $F/f_c \ll 1$) bo'lgan tizim tor polosali hisoblanadi. Aks holda, tizim keng polosali hisoblanadi. Amalda esa hozirgi vaqtda 1,25 MGsdan 40M Gsgacha kenglikdagi kanallarni ishlatadigan texnologiyalar keng polosali tizimlar turkumiga kiritiladi. Shuningdek, keng polosali texnologiyalar yuqori ma'lumot uzatish tezligini (1 Mbit/sekundan dan past emas) ta'minlaydi [5].

Mazkur qo'llanmada keng polosali simsiz raqamli tizimlar sinfiga kiradigan texnologiyalar yoritiladi va ularni sinflarga bo'lishda ko'pincha quyidagi yondashuvlar ishlatiladi:

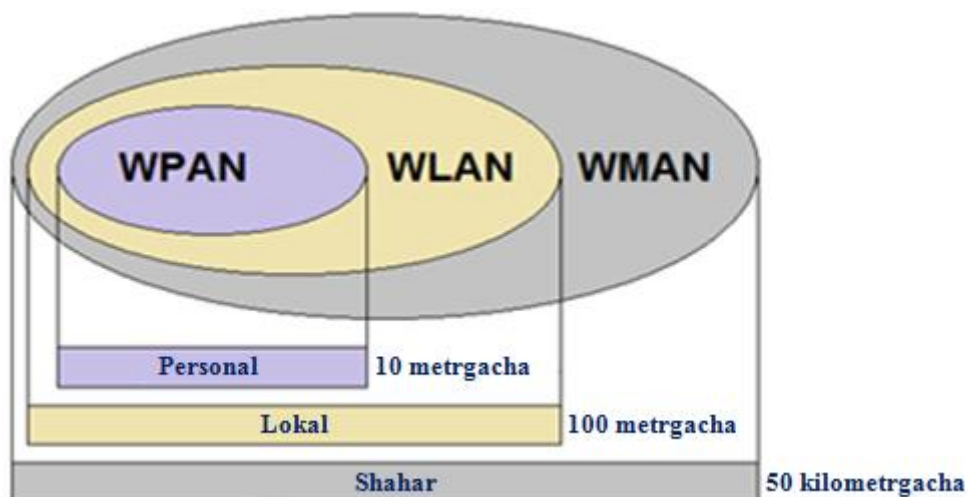
1. Aloqaning uzoqligi bo'yicha tarmoqlar quyidagi sinflarga ajratiladi:

- Bir necha detsimetrlardan bir necha dekametrlargacha radioqamrovga ega simsiz personal tarmoqlar (ingl. *Wireless Personal Area Networks - WPAN*). Periferiya qurilmalari, turli hisoblagichlar, xabarchilar va boshqalar bilan aloqa uchun mo'ljallangan. Bu texnologiyalarga misollar Bluetooth, RFID, ZigBee texnologiyalar hisoblanadi.

- Bir necha yuzlab metrlargacha ta'sir etish radiusili simsiz lokal tarmoqlar (ingl. *Wireless Local Area Networks - WLAN*). Ular ofis (tashkilot) ichidagi (ba'zan ofislararo) aloqani tashkil etish uchun mo'ljallangan. Ular qatoriga Wi-Fi, DECT, Femto-sota kabi texnologiyalarni qo'shish mumkin.

- Bir necha, hatto o'nlab kilometrlargacha qamrov radiusiga ega shahar (hudud) ko'lamidagi simsiz tarmoqlar (ingl. *Wireless Metropolitan Area Networks - WMAN*). Yirik shahar atrofida yoki tumanlarda xizmat ko'rsatadigan tarmoqlarni yaratish uchun mo'ljallangan tizimlar. Ular sifatida WiMAX va WiBro texnologiyalari, sotali va trunking, shuningdek radio va teleuzatish tizimlari misol bo'lishi mumkin (1.1- rasm) [17].

Shuningdek, ba'zan global ko'lamdagi simsiz tarmoqlar (ingl. *Wireless World wide Area Networks - WWAN*) ham alohida ajratiladi. Ular qatoriga avvalom bor yo'ldoshli aloqa tizimlari, shuningdek global rouming tufayli sotali aloqa tizimlari ham kiritiladi.



1.1- rasm. Aloqaning uzatish bo'yicha simsiz texnologiyalarning sinflarga bo'linishi

2. Tarmoqlar topologiyasi bo'yicha quyidagi ulanish rejimlari ajratiladi:

- tarmoqning ikki tuguni bevosita ulanadigan "nuqta - nuqta" rejimi.

- bir ulanish nuqtasi (bazaviy stansiya) ko'p sonli abonent qurilmalari bilan ulanadigan "nuqta – ko'p nuqta" rejimi (1.2- rasm).

3. Qo'llanish turi bo'yicha simsiz tarmoqlar quyidagilarga bo'linadi:

- o'z zarurlari uchun tashkilotlar va kompaniyalar tomonidan yaratiladigan korporativ tarmoqlar.

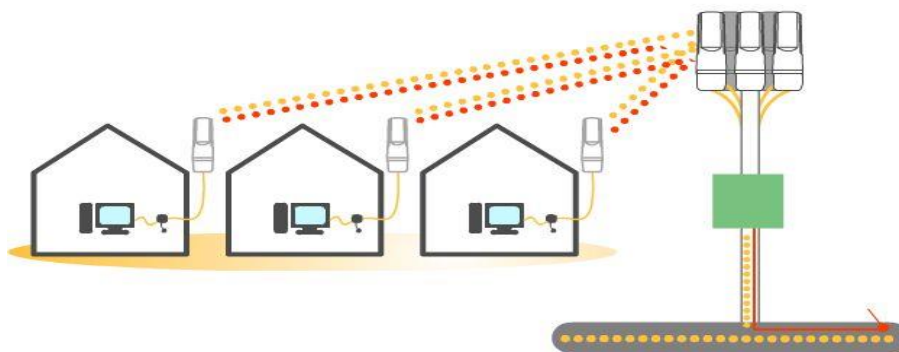
- tijorat xizmatlarini ko'rsatish uchun aloqa operatorlari tomonidan yaratiladigan tarmoqlar.

4. Shuningdek qisqa va sig'imli tasniflagich sifatida SKPU texnologiyalarning ikki eng muhim xarakteristikalarini bir vaqtda taqqoslab ko'rsatish ham mumkin. Ular quyidagilar hisoblanadi:

- ma'lumot uzatishning maksimal tezligi;
- maksimal aloqa masofasi (1.3- rasm).

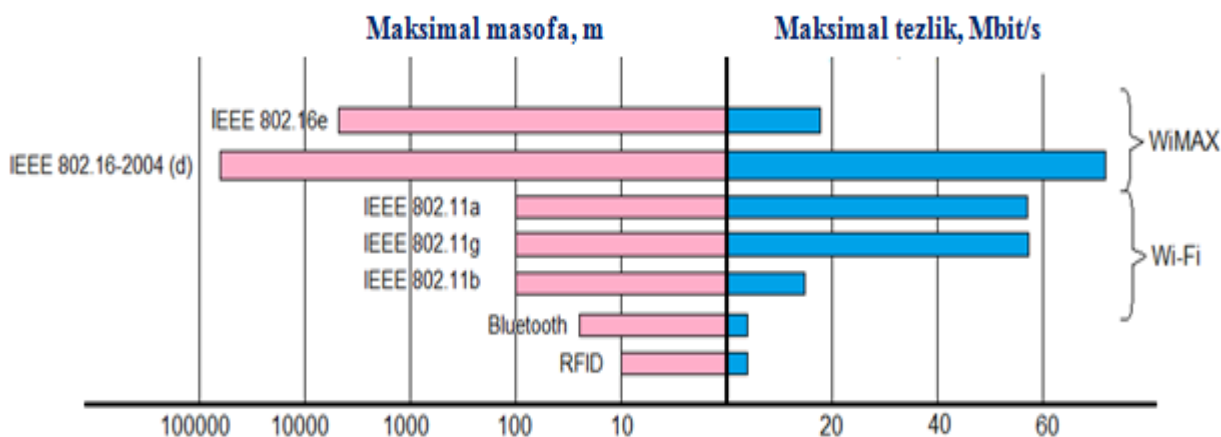


a)



b)

1.2– rasm. Tarmoq topologiyasi bo‘yicha simsiz texnologiyalarning sinflarga bo‘linishi



1.3- rasm. Ma’lumotlarni uzatish tezligi va aloqaning uzoqligi bo‘yicha simsiz texnologiyalarning sinflarga bo‘linishi

Xulosa qilib shuni ta’kidlash lozimki, keng polosali simsiz aloqa tizimlarini sinflarga bo‘lishga yondashuvlarda (boshqa murakkab va rivojlanayotgan tizimlardagi kabi) klassifikatsiya mezonlarining o‘zi ham bir xil emasligini va o‘zgaruvchanligini hisobga olish zarur [4].

1.3. Wi-Fi (IEEE 802.11) texnologiyasi

Wi-Fi (ingl. *Wireles Fidelity* – boshlanishida “simsiz aniqliq” deb ifodalangan) texnologiyasi deb Wi-Fi Allianse konsorsiumi tomonidan ishlab chiqilgan WLAN sinfiga qarashli va IEEE institutining 802.11 standartlar turkumiga kirgan tizim hisoblanadi. Ushbu texnologiya yuqori sifatli ovoz yozish va eshitirish standarti Hi-Fi (ingl. *High Fidelity* - “yuqori aniqlik”) ga o‘xshatib nomlangan.

Wi-Fi tarmoqlaridan foydalanish simli tarmoqlar qurish mumkin bo‘lmagan yoki iqtisodiy tarafdin maqsadga muvofiq bo‘lmagan joylarda tavsiya etiladi. Hozirgi vaqtda Wi-Fi tarmoqlari ham korporativ, ham xususiy foydalanuvchilar tomonidan keng ishlatilmoqda. Zamonaviy Wi-Fi tizimlarida ma’lumot uzatish tezligi muayyan sharoitlarda 600Mbit/sek. largacha yetadi. Wi-Fi tarmoqlarida aloqaning turg‘un va mobil rejimlari qo‘llab-quvvatlanadi. Abonent qabul qilgich / uzatkich uskunasi – “Wi-Fi adapteri” bilan jihozlangan mobil terminallar (KPK, smartfonlar va noutbuklar) lokal tarmoqlarga va ulanish nuqtasi yoki “xot-spot” deb nomlangan nuqtalar orqali Internetga ulanishi mumkin.

Yuqorida aytib o‘tilganidek, WLAN sinfidagi tarmoqlarning yagona standarti ustida ishlar IEEE instituti qoshida yaratilgan 802.11 ishchi guruhi doirasida boshlangan edi. Wi-Fi texnologiyasining ilk namunasi 1991 yilda Nivegeyn shahrida (Niderlandiya) NCR Corporation/AT&T (keyinchalik Lucent va Agere Systems) kompaniyasi tomonidan ishlab chiqildi. Uskuna dastlab kassa apparatlarida ishlatish uchun mo‘ljallangan va bozorga WaveLAN nomida chiqarilgan edi. O‘shandayoq bu uskunalardan 1dan 2Mbit/sek.gacha ma’lumot uzatish tezligini ta’minlay olardi. Wi-Fi texnologiyasini asosiy ishlab chiquvchisi - janob Vik Xeyz (*Vic Hayes*) “Wi-Fi otasi” degan nom oldi va keyingi IEEE 802.11b, 802.11a va 802.11g standartlarini ishlab chiqishda qatnashgan jamoaning a’zosi bo‘ldi [12].

1997 yilda IEEE 802.11 belgisini olgan birinchi Wi-Fi standarti paydo bo‘ldi. Bu standart radiochastota va infraqizil to‘lqinlarida ishlashga mo‘ljallangan bo‘lib, 1 va 2 Mbit/sek. ma’lumot uzatish tezliklarini taqdim etdi. Radiochastota kanalida chastotalarda sakrash (rus. *pereskok*) hisobiga spektrni kengaytirish (ingl. *Frequency Hopping Spread Spectrum, FHSS*) va to‘g‘ri ketma-ketlik hisobiga

spektrni kengaytirish (ingl. *Direct Sequence Spread Spectrum, DSSS*) usullari ishlatildi.

Ammo, xatto 1997 yil uchun ham 1 – 2Mbit/sek. tezliklar yetarli bo‘lmadi va 802.11 guruhi yangi yuqoriroq tezliklarni taqdim etadigan standartlarni ishlab chiqish ustida harakatlar boshladi. Bu vaqtga kelib ko‘plab davlatlarda Wi-Fi tarmoqlari uchun HTI tomonidan tavsiya etilgan 2400-2483,5MGs va 5150-5350MGs diapazonlaridagi polosalarga ruxsat berildi va har ikkala diapazonlarda standartlar yaratish ustida parallel ishlar olib borildi [2].

Dastlab 1999 yilning 16 sentyabrida 2,4GGs diapazoniga mo‘ljallangan va ma’lumot uzatish tezligini nazariy jihatdan 33Mbit/sek ga oshirgan IEEE 802.11b standarti paydo bo‘ldi. Ishlatilgan asosiy modulyatsiya/kodlash SSK (ingl. *Complementary Code Keying*) usuli 11 Mbit/sek gacha tezlikni ta’minladi va qo‘shimcha PBCC (ingl. *Packet Binary Convolutional Coding*) paketli binar o‘rashli kodlash (rus. *svyortochnoe kodirovanie*) usuli tezlikni 22 va 33Mbit/sek. gacha oshirdi.

5GGs diapazoni uchun mo‘ljallangan IEEE 802.11a standarti “11b” versiyasidan keyinroq, ya’ni 1999 yilning sentyabrida, paydo bo‘lsa-da, lekin xarakteristikalar bo‘yicha undan o‘zib ketdi. U 54Mbit/sek. gacha ma’lumot uzatish tezligiga erishdi. Bunga o‘sha paytda prinsipial yangi bo‘lgan OFDM mexanizmidan foydalanish tufayli erishildi.

2003 yil iyunida IEEE 802.11b standartining takomillashtirilgan versiyasi - IEEE 802.11g paydo bo‘ldi. U “11b” ning chastota diapazonida ishlar edi va “11a” ning tezligini (ya’ni 54Mbit/sek.) ta’minlar edi.

Nihoyat 2009 yilning 11 sentyabrida uzoq kutilgan IEEE 802.11n standarti dunyoga keldi. Uni paydo bo‘lishi Wi-Fi texnologiyalarida yangi “sakrash” bo‘ldi. “11n” standartida MIMO texnologiyasi, MAS-paketlarni agregatsiyalash usuli, 40MGs chastotalar polosasidan foydalanish kabi ko‘plab texnologik yangiliklar qo‘llanildi va birgalikda bu standartdagi yuqori ma’lumot uzatish tezligini ta’minladi (nazariy jihatdan 600Mbit/sek. gacha). “11n” standarti avvalgi barcha standartlar (ya’ni, “a”, “b” va “g” versiyalari) bilan moslasha oladi va bugungi kunga kelib (2011 yilning boshi) dunyoda eng ko‘p tarqalgan Wi-Fi standarti bo‘lib qoldi.

Hozirgi vaqtda o'zining xarakteristikalarini bo'yicha 4G texnologiyalari talablariga mos bo'la oladigan standartning keyingi versiyasi, xususan IEEE 802.11ac standarti ishlab chiqildi [15].

1.4. WiMAX (IEEE 802.16) texnologiyasi

Worldwide Interoperability for Microwave Access (WiMAX, inglizchadan, O'YuCh diapazonida ulanish bo'yicha butun dunyo hamkorligi) - bu IEEE instituti (802.16 guruhi) tomonidan standartlashtirilgan katta masofalarda "so'nggi milya" muammosini alternativ yechimi sifatida qayd qilingan simli liniyalar va kabel texnologiyalarini to'ldiruvchi keng polosali simsiz ulanish texnologiyasidir. WiMAX texnologiyasidan shahar miqyosida keng polosali ulanish tarmoqlarini (ingl. *Metropolitan Area Networks, MAN*) yaratish, simsiz ulanish nuqtalarini tashkil qilish ("nuqta - ko'p nuqta" rejimi), bir-biridan olis ob'ektlar orasida yuqori sifatli aloqa tashkil etish ("nuqta - nuqta" rejimi) va shunga o'xshash masalalarni yechish uchun foydalanish mumkin.

Umuman olganda, IEEE 802.16 standartining bazaviy xarakteristikalarini 50 kilometr gacha bo'lgan ta'sirning uzoqligi darajasini, to'g'ri ko'rinish zonasidan tashqarida ishlash imkoniyatini, BS ning bir sektorida (jami BS 6 tagacha sektorga ega bo'lishi mumkin) ma'lumot almashuv tezligini maksimal (pik) holatda 70Mbit/sek. gacha ko'tarilishini ko'zda tutadi. WiMAX tarmoqlarining jihozlari 2 - 11GGs diapazonida 10-20MGs kenglikdagi bir necha kanallarda ishlashi mumkin. Chastota diapazonlarning bunchalik keng tanlanishi dunyoning ko'plab mamlakatlari spetsifikatsiya(tavsifnoma)larini hisobga olish uchun qilingan.

Shunday qilib, WiMAX ma'lumot uzatish tezligi bo'yicha simli tarmoqlar bilan taqqoslana oladigan va unumdorlik hamda qoplash bo'yicha zamonaviy Wi-Fi tarmoqlaridan yuqoriroq bo'lgan Internetga tezkor ulanish uchun yaratilgan texnologiya hisoblanadi. O'z navbatida, aynan Wi-Fi lokal tarmoqlari yoki foydalanuvchilarning turli tijorat va maishiy simli tarmoqlari WiMAX "magistral tarmoqlari"ning davomi bo'lib xizmat qilishi mumkin. Ideal holatda, WiMAX, soha standartlariga asoslangan bo'lib, shaharlar va qishloqlarda uy foydalanuvchilari, korxonalar va mobil simsiz tarmoqlar uchun yuqori tezlikdagi, shu bilan birga, nisbatan

qimmat bo'lmagan aloqani tashkil etish uchun ishlab chiqilgan texnologiya hisoblanadi [4].

Nazorat savollari

1. Qanday “tjorat” nomlari bilan ma'lum bo'lgan simsiz texnologiyalar mavjud?

2. Radioaloqaning birinchi omadli sinovlari kimlar tomonidan amalga oshirilgan?

3. ARPANET bilan INTERNET orasida qanday bog`liqlik bor?

4. Wi-Fi va WiMAX tizimlari yanada ommaviylashish sababini tushuntiring.

2- BOB. Wi-Fi (IEEE 802.11 STANDARTI) SIMSIZ KENG POLOSALI ULANISH TEXNOLOGIYASI

Simsiz lokal tarmoqlarning eng ommaviy standarti IEEE 802.11 standarti hisoblanadi. **IEEE** – ingl. *Institute of Electrical and Electronics Engineers* (Elektr va elektronika bo'yicha muxandislar instituti) simli va simsiz axborot uzatish tarmoqlari sohasida standartlar ishlab chiqish bilan shug'ullanadi. Simsiz tarmoqlar standartlarini yaratish sohasidagi boshlang'ich nuqta sifatida IEEE tashkiloti tomonidan 1990 yilda 802.11 qo'mitasining tashkil etilishi hisoblanadi. Bu guruh 2,4 GGs chastotada, 1 - 2 Mbit/sekund ulanish tezliklarida ishlaydigan radioqurilmalar va tarmoqlar uchun umumiy standartni ishlab chiqish bilan shug'ullandi. Standart ustida ishlar 7 yildan keyin yakunlandi va 1997 yilning iyunida birinchi 802.11 spesifikasiya ratifikatsiya qilindi. IEEE 802.11 standarti simli tarmoqlar uchun ko'plab standartlarni ishlab chiqadigan mustaqil xalqaro tashkilotdan WLAN mahsulotlari uchun birinchi standart hisoblanadi. Bugungi kunda ushbu texnologiyaning yangi standartlari (IEEE 802.11n) 300 Mbit/sekundgacha tezlikni bir necha yuzlab metr masofalargacha ta'minlashga qodir [14].

802.11 standartlari to'plami 802.11 MAS nimdarajasi bilan ishlatilishi mumkin bo'lgan fizik darajaning (Physical Layer Protocol-PHY) qator ishlatilishi texnologiyalarini aniqlaydi. PHY darajalari quyidagilar (2.1- rasm):

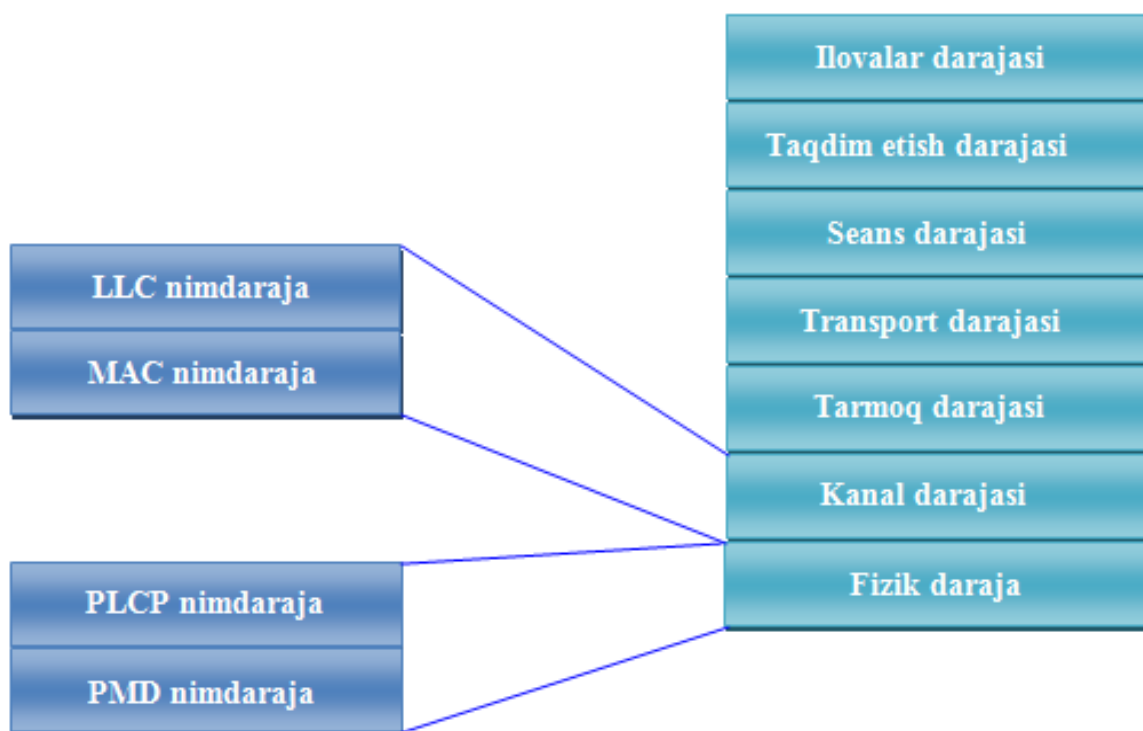
- 802.11 standartining 2,4 GGs diapazondagi chastotani sakrashsimon qayta sozlashli (FHSS) PHY darajasi;
- 802.11 standartining 2,4 GGs diapazondagi to'g'ridan-to'g'ri ketma-ketlikli usulda spektrni kengaytirishli (DSSS) PHY darajasi;
- 802.11b standartining 2,4 GGs diapazonda komplementar kodlashli PHY darajasi;
- 802.11a standartining 5 GGs diapazondagi ortogonal chastotaviy multipleksirlashli (OFDM) PHY darajasi;
- 802.11g standartining 2,4 GGs diapazondagi kengaytirilgan fizik darajasi (Extended Rate Physical Layer-ERP).

802.11 standarti fizik darajalarining asosiy vazifasi MAS nimdarajasi uchun simsiz uzatish mexanizmlarini ta'minlash, shuningdek simsiz muhit holatini baholash va u haqida MAS nimdarajaga xabar berish kabi ikkilamchi funksiyalarni bajarilishi qo'llab-quvvatlash hisoblanadi. MAS va PHY darajalari mustaqil

bo'lishi uchun shunday ishlab chiqildi. Aynan MAS va PHY nimdarajalari orasidagi mustaqillik 802.11b, 802.11a va 802.11g standartlaridagi qo'shimcha yuqori tezlikli fizik darajalarni ishlatilishiga imkon berdi.

802.11 standarti fizik darajalarining har biri ikkita nimdarajaga ega:

- Physical Layer Convergence Procedure (PLCP). Fizik daraja holatini aniqlash protsedurasi;
- Medium Dependent (PMD). Fizik darajaning uzatish muhitiga bog'liq bo'lgan nimdarajasi.



2.1- rasm. PHY darajaning nimdarajalari

PLCP nimdaraja borligicha simsiz muhit orqali ma'lumotlarni u yoki bu uzatish va qabul qilish usuli ishlatiladigan PMD nimdarajasidan foydalaniladigan MAC-stansiyalar orasida MAC protokoli ma'lumotlari elementlarining (MAC Protocol Data Units-MPDU) harakatlantirilishi amalga oshiriladigan o'zaro ta'sirlashishni ta'minlash darajasi hisoblanadi. PLCP va PMD nimdarajalar 802.11 standartining turli variantlari uchun farq qiladi.

Fizik darajalarni o'rganishga kirishishda oldin fizik darajaning tashkil etuvchilaridan biri bo'lgan skremblirlashni ko'rib chiqamiz.

Zamonaviy uzatkichlar asosida yotadigan ma'lumotlarni yuqori tezlikda uzatish mumkin bo'lgan xususiyatlardan biri bu uzatish uchun taqdim etiladigan ma'lumotlar uzatkich nuqtai nazaridan tasodifiy tarzda kelishi haqida ko'zda tutish hisoblanadi. Bu ko'zda tutishsiz fizik darajaning qolgan tashkil etuvchilarining qo'llanilishi hisobiga olinadigan ko'plab afzalliklarini ishlatib bo'lmasdi.

Lekin bo'ladiki, qabul qilinadigan ma'lumotlar yetarlicha tasodifiy emas va aslida nollar va birlarning takrorlanadigan to'plamlari va uzun ketma-ketliklaridan iborat bo'lishi mumkin.

Skremblirlash (elementlarning joylarini almashtirilishi) bu qabul qilinadigan ma'lumotlar tasodifiyga o'xshab ketadigan qilinadigan usul hisoblanadi. Bunga ma'lumotlarni tuzilmalashtirilganidan tasodifiy o'xshab ketishiga aylantirish uchun ketma-ketlik bitlarini joylarini almashtirish yo'li bilan erishiladi. Bu protsedura ba'zan "ma'lumotlar oqimini oqlash" deyiladi. Qabullagichning deskrembleri keyin dastlabki tuzilmalashtirilgan ketma-ketlikni olish uchun tasodifiy ketma-ketlikni teskari o'zgartirishni bajaradi. Ko'plab skremblirlash usullari o'zi sinxronlashadigan usullarga kiradi. Bu deskrembler skrembler orqali mustaqil sinxronlashtirilishi mumkinligini bildiradi.

2.1. IEEE 802.11 standartning arxitekturasi. IEEE 802.11 protokollar steki

Tabiiyki, IEEE 802.11 standarti protokollari steki 802 qo'mita standartlarining umumiy tuzilmasiga mos keladi, ya'ni MAC (Media Access Control) darajasiga ulanishni va LLS (Logical Link Control) ma'lumotlarni mantiqiy uzatishni boshqarish nimdarajalarili fizik va kanalli darajalardan tashkil topgan. Protokollar steki bu tarmoqda tugunlarning o'zaro ta'sirlashishini tashkil etish uchun etarli bo'lgan tarmoq protokollarining ierarxik tashkil etilgan to'plami hisoblanadi. Protokollar tarmoqda bir vaqtda ishlaydi, demak, protokollarning ishlashi to'qnashuvlar yoki tugallanmagan operatsiyalar vujudga kelmaydigan tarzda tashkil etilishi kerak. Shuning uchun protokollar steki aerarxik qurilgan darajalarga bo'linadi, ulardan har biri aniq bir vazifani – ma'lumotlarni tayyorlash, qabul qilish, uzatish va ular bilan keyingi amallarni bajaradi.

802 oilaning barcha texnologiyalaridagi kabi 802.11 texnologiya ikkita pastki, ya'ni fizik daraja va MAC daraja orqali aniqlanadi, LLC

daraja esa barcha LAN texnologiyalari uchun umumiy standart bo'lgan o'z funksiyalarini bajaradi (2.1- rasm) [3].

Fizik darajada ishlatiladigan chastotalar diapazoni, kodlash usuli va demak, ma'lumotlarni uzatish tezligi bilan farqlanadigan bir necha spesifikasiyalar variantlari mavjud. Fizik darajaning barcha variantlari MAC darajaning o'sha bir algoritmi bilan ishlaydi, lekin MAC darajaning ba'zi vaqt parametrlari ishlatiladigan fizik darajaga bog'liq.

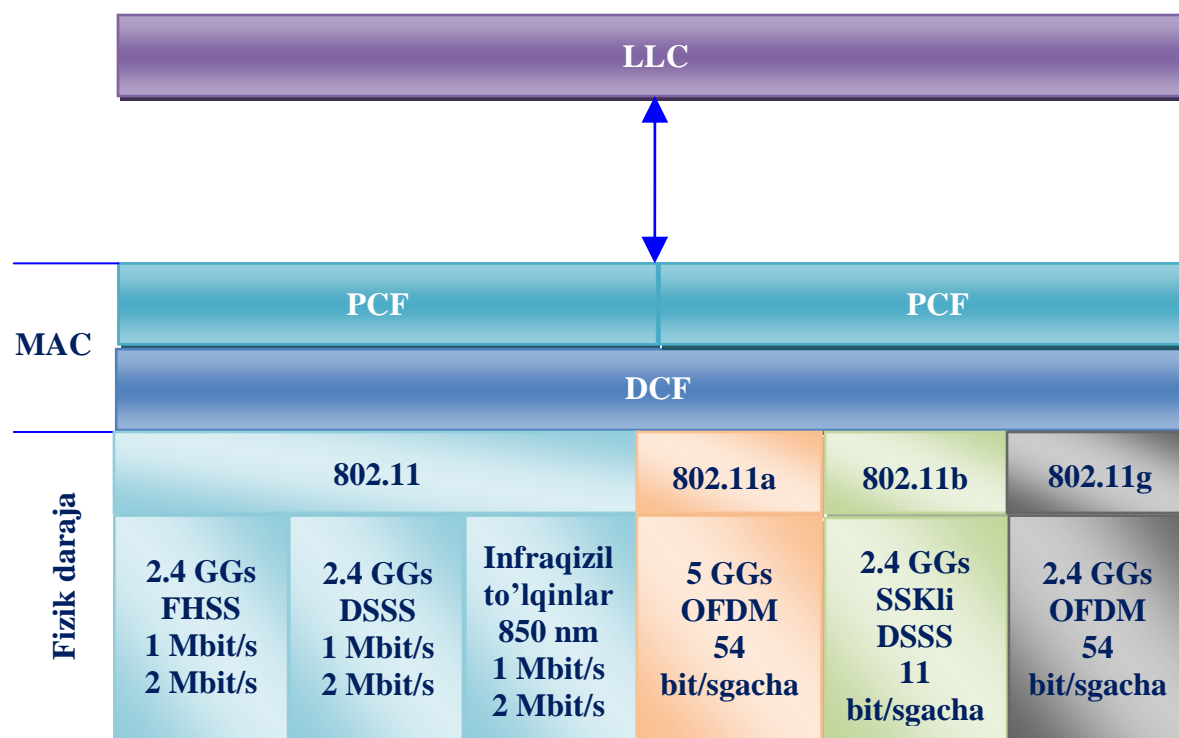
2.2. IEEE 802.11 standarti muhitiga ulanish darajasi

IEEE 802.11 tarmoqlarda MAS daraja ajratiladigan muhitga ikki ulanish rejimini ta'minlaydi (2.2- rasm):

- DSF taqsimlangan rejim (Distributed Coordination Function);
- PSF markazlashtirilgan rejim (Point Coordination Function).

DSF taqsimlangan ulanish rejimi

Dastlab DSF taqsimlangan rejimda ulanishni qanday ta'minlanishini ko'rib chiqamiz. Bu rejimda *tashuvchini nazorat qilish va kolliziyalarni oldini olishli ko'p tomonlama ulanish usuli* (Carrier Sense Multiple Access with Collision Avoidance-CSMA/CA) ishlatiladi.



2.2- rasm. IEEE 802.11 protokollari steki

Simsiz tarmoqlarda samarasiz bo‘lgan CSMA/CA usuli bo‘yicha kolliziyalarni to‘g‘ridan-to‘g‘ri tanish (raspoznovaniya) o‘rniga bu yerda ularni bilvosita aniqlash ishlatiladi. Buning uchun har bir uzatilgan kadr yuborilishi kerak bo‘lgan stansiyaning ijobiy kvitansiyasi kadri bilan tasdiqlanishi kerak. Agar kelishilgan taym-aut tugashi bilan kvitansiya kelmasa yuboruvchi-stansiya kolliziya bo‘lgan deb hisoblaydi.

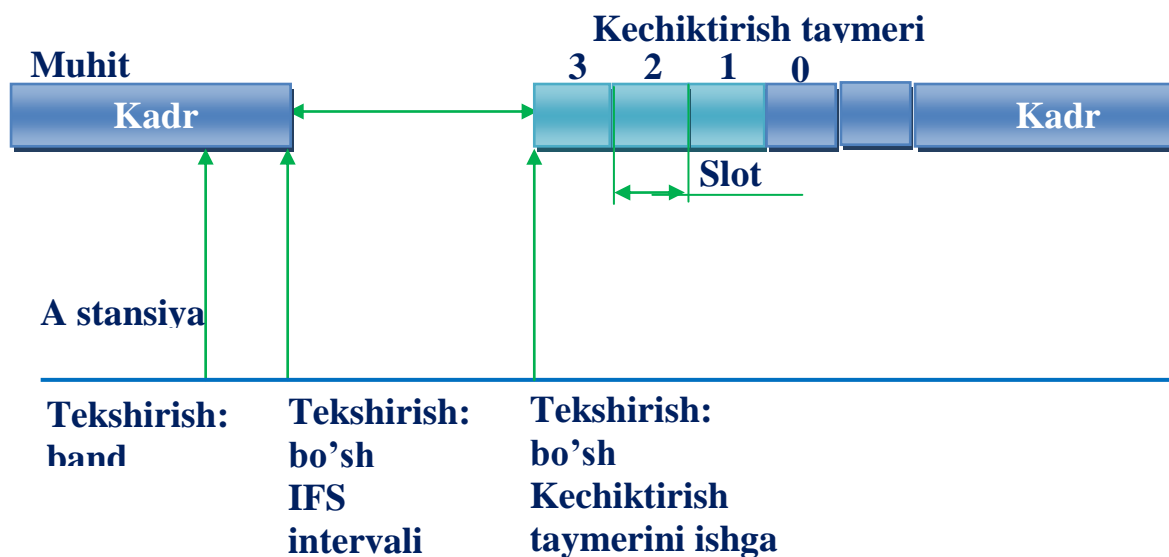
DSF ulanish rejimi stansiyalarning sinxronlashtirilishini talab qiladi. 802.11 spesifikatsiyada bu muammo yetarlicha ustalik bilan yechiladi. Vaqt intervallari navbatdagi kadrning uzatilishi tugashi momentidan boshlab hisoblay boshlanadi (2.3- rasm). Bu qandaydir maxsus sinxronlashtirish signallarini uzatilishini talab qilmaydi va paket o‘lchamini slot o‘lchami bilan chegaralamaydi, chunki slotlar faqat kadrni uzatilishi boshlanishi haqida qaror qabul qilinishida e‘tiborga olinadi.

Kadrni uzatishni istaydigan stansiya muhitni oldindan eshitib ko‘rishi kerak. IEEE 802.11 standarti kanalda ikki *fizik va virtual* aktivlikni nazorat qilish (tashuvchini aniqlash) mexanizmini ko‘zda tutadi. Birinchi mexanizm fizik darajada ishlatilgan va antennada signal sathini aniqlash va uni bo‘sh bo‘lgan vaqt bilan taqqoslashga mo‘ljallangan. Tashuvchini aniqlashning virtual mexanizmi shunga asoslanganki, uzatiladigan ma’lumotlar kadrlarida, shuningdek ASK va RTS/CTS boshqarish kadrlarda paketlarni (paketlar guruhi) uzatish va tasdiqlashni olish uchun zarur bo‘lgan vaqt haqida axborotlar bo‘lishiga asoslangan. Tarmoqning barcha qurilmalari joriy uzatish haqida axborotlarni oladi va kanal qancha vaqt band bo‘lishini aniqlashi mumkin, ya’ni qurilma aloqa o‘rnatilganda barchaga kanalni qancha vaqtga egallashini xabar qiladi. Stansiya kadrning uzatilishini tugashini qayd etishi bilan u kadrlararo intervalga (IFS) teng bo‘lgan vaqt intervalini hisoblashi kerak. Agar IFS tugaganidan keyin muhit hali ham bo‘sh bo‘lsa qayd etilgan uzunlikdagi slotlarni hisoblash boshlanadi. Kadrni faqat muhit bo‘sh bo‘lgan sharoitda slotlardan birining boshlanishida uzatish mumkin. Stansiya uzatish uchun slotni CSMA/CA usulida ishlatilganiga o‘xshash kesilgan eksponensial kechiktirish ikkilik algoritmiga asoslanib tanlaydi. Slotning nomeri $[0, CW]$ intervalda bir tekis taqsimlangan tasodifiy butun son sifatida tanlanadi, bu yerda “CW” “Contention Window” ni (raqobat oynasi) bildiradi [4].

Bu yetarlicha oson bo‘lmagan ulanish usulini 2.3-rasm misolida ko‘rib chiqamiz. A stansiya kesilgan eksponensial kechiktirish ikkilik algoritmiga asosan uzatish uchun 3 slotni tanlagan bo‘lsin. Bunda u kechiktirish taymeriga (uning vazifasi keyingi bayon etishda aniqlanadi) 3 qiymatni tayinlaydi va har bir slotning boshlanishida muhitning holatini tekshirishni boshlaydi. Agar muhit bo‘sh bo‘lsa, u holda kechiktirish taymeridagi qiymatdan 1 ayiriladi, va agar natija nolga teng bo‘lsa kadrni uzatish boshlanadi.

Shunday qilib, barcha slotlarning, shu jumladan tanlangan slotning band bo‘lmashligi sharti ta‘minlanadi. Bu shart uzatishni boshlanishi uchun zarur hisoblanadi.

Agar qandaydir slotning boshlanishida muhit band bo‘lsa, u holda birni ayirish bo‘lib o‘tmaydi va taymer “muzlaydi”. Bu holda stansiya uzatish uchun faqat slotni tanlash algoritmini o‘zgartirish bilan muhitga ulanishning yangi siklini boshlaydi. Avvalgi sikldagidek, stansiya muhitni kuzatadi va u bo‘shaganida kadrlararo interval davomida pauza qiladi. Agar muhit bo‘sh qolsa, u holda stansiya “muzlatilgan” taymer qiymatini slot nomeri sifatida ishlatadi va yuqoridagi bo‘sh slotlarni tekshirish protsedurasini muzlatilgan kechiktirish taymeri qiymatidan boshlab birni ayirish bilan bajaradi.



2.3- rasm. DSF ulanish rejimi

Slotning o‘lchami signalni kodlash usuliga bog‘liq. FHSS usuli uchun slotning o‘lchami 28 mks ni, DSSS usuli uchun 1 mks ni tashkil etadi. Slotning o‘lchami shunday tanlanadiki, u tarmoqning ikkita istalgan stansiyasi orasidagi signalning tarqalishi vaqtiga muhitning

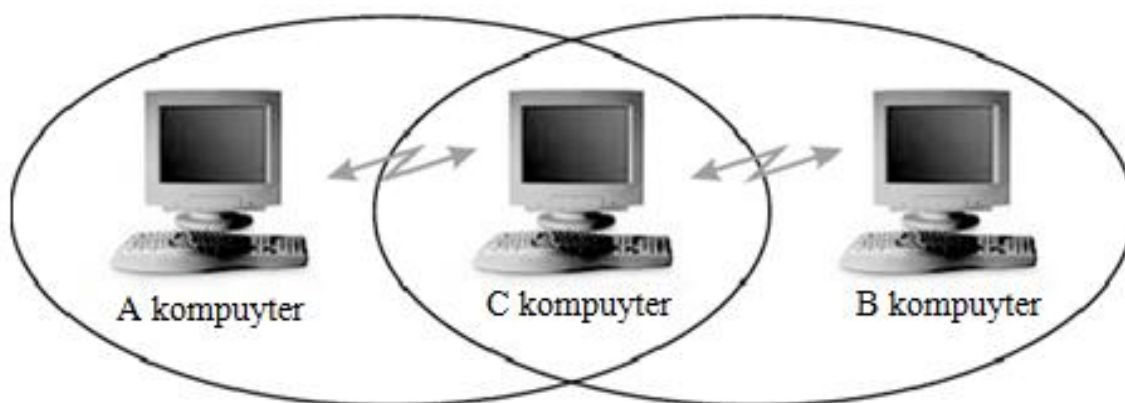
bandligini aniqlashga ketadigan vaqtni qo'shgandagidan ortiq bo'ladi. Agar bunday shart bajarilmasa, u holda tarmoqning har bir stansiyasi slotlarni eshitishda u uzatish uchun oldingi tanlagan slotida kadrni uzatishni boshlashini to'g'ri aniqlay oladi. Bu o'z navbatida quyidagini bildiradi.

Kolliziya faqat bir necha stansiyalar uzatish uchun o'sha bir slotni tanlagan hollarda o'z o'rniga ega bo'lishi mumkin.

Bu holda kadrlar buziladi va yuborilishi kerak bo'lgan stansiyalardan kvitansiyalar kelmaydi. Yuboruvchilar ma'lum vaqt davomida kvitansiyalarni olmasdan kolliziya faktini qayd etadi va o'z kadrlarini yana uzatishga urinadi. Kadrni uzatishga har bir muvaffaqiyatsiz urinishda undan slot nomeri tanlanadigan $[0, CW]$ interval ikkiga ortadi. Agar, masalan, oynaning boshlang'ich o'lchami 8 ga teng (ya'ni $CW=7$) tanlangan bo'lsa, u holda birinchi kolliziyadan keyin oynaning o'lchami 16 ga ($CW=15$), ikkinchi ketma-ket kolliziyadan keyin 32 va h.k. teng bo'lishi kerak. 802.11 standartga muvofiq CW ning boshlang'ich qiymati simsiz lokal tarmoqda ishlatiladigan fizik darajaga bog'liq ravishda tanlanishi kerak.

CSMA/CA usulidagi kabi, bu usulda bitta kadrni uzatishga muvaffaqiyatsiz urinishlar soni chegaralangan, lekin 802.11 standarti bu yuqori chegaraning aniq qiymatini bermaydi. N urinishlar yuqori chegarasiga yetilganda, kadr tashlab yuboriladi, ketma-ket kolliziyalar hisoblagichida esa nol o'rnatiladi. Bu hisoblagichda kadr bir necha muvaffaqiyatsiz urinishlardan keyin baribir muvaffaqiyatli uzatilgan bo'lsa ham nol o'rnatiladi.

Simsiz tarmoqlarda yashirin terminal muammosi deyiladigan, ikkita qurilma (A va V) bir-birlaridan olisda joylashgan va bir-birlarini eshitmaydigan, lekin ularning ikkalasi ham uchinchi S qurilmaning qamrab olish zonasiga tushadigan holatlar (2.4-rasm) bo'lishi mumkin. Agar har ikkala A va V qurilmalar uzatishni boshlasa, u holda ular prinsipial jihatdan konfliktli holatni va paketlar nima uchun o'tmayotganligini aniqlay olmaydi [4].



2.4- rasm. Yashirin terminal muammosi

2.3. IEEE 802.11 standartlari: IEEE 802.11; IEEE 802.11b standartlari

Ma'lumotlarni simsiz uzatish tizimlarining yetarlicha ko'plab standartlari mavjud, lekin amalda ulardan uchtasi IEEE 802.11a, IEEE 802.11b va IEEE 802.11g standartlari keng tarqaldi. Bu standartlar uzatish tezligi, chastotalar diapazoni, signalni modulyatsiyalash usuli va boshqa ko'plab xarakteristikalari bo'yicha farqlanadi.

Oddiy simli lokal Ethernet tarmoqlar o'tkazish qobiliyatiga deyarli ekvivalent bo'lgan IEEE 802.11b standartdagi ma'lumotlarni yuqori uzatish tezligi (11 Mbit/sekundgacha), shuningdek 2,4 GGs diapazonga mo'ljallanganligi tufayli, bu standart simsiz tarmoqlar qurilmalari ishlab chiqaruvchilarida eng keng tarqaldi [14].

Binobarin, maksimal 11 Mbit/sekund tezlikda ishlaydigan qurilma pastroq tezliklarda ishlaydigan qurilmalarga qaraganda kam ishlash radiusiga ega, IEEE 802.11b standartda signal sifati yomonlashganda tezlikni avtomatik kamaytirish ko'zda tutilgan.

IEEE 802.11a standarti 54 Mbit/sekundgacha ma'lumotlarni uzatish tezliklarida 802.11 standartlar oilasidan eng keng polosaga ega.

2,4 GGs chastotalar sohasiga mo'ljallangan bazaviy standartdan farqli ravishda IEEE 802.11a spesifikatsiyalarida 5 GGs diapazonda ishlash ko'zda tutilgan. Signalni modulyatsiya qilish usuli sifatida ortogonal chastotaviy multipleksirlash (OFDM) tanlangan.

IEEE 802.11a standartning kamchiliklariga 5 GGs chastotalar uchun radiouzatkichlarning yuqori iste'mol quvvati, shuningdek kam ishlash radiusi kiradi.

IEEE 802.11g standart IEEE 802.11b standartning mantiqiy rivojlantirilishi hisoblanadi va o'sha chastotalar diapazonida ma'lumotlarni uzatilishini ko'zda tutadi. Bundan tashqari, IEEE 802.11g standart IEEE 802.11b standart bilan to'liq moslashadi, ya'ni IEEE 802.11g standartning istalgan qurilmasi IEEE 802.11b standartning qurilmalari bilan ishlay olishi kerak. IEEE 802.11g standartda ma'lumotlarni maksimal uzatish tezligi 54 Mbit/sekundni tashkil etadi, shuning uchun bugungi kunda u simsiz aloqaning eng istiqbolli standarti hisoblanadi.

IEEE 802.11g standartni ishlab chiqishda raqobat qiluvchi texnologiyalarning ikki qismlari OFDM ortogonal chastotaviy bo'lish va IEEE 802.11g standartda opsion ishlatilgan RVSS ikkilik paketli o'ramali kodlash usuli ko'rib chiqildi. Natijada IEEE 802.11g standarti kelishuvli yechimga ega bo'ldi. Bazaviylar sifatida OFDM va SSK texnologiyalari qo'llanildi, opsional esa RVSS texnologiyasidan foydalanish ko'zda tutildi.

IEEE 802.11 standarti

Dastlabki IEEE 802.11 standart fizik darajada uchta uzatish usulini aniqlaydi:

- infraqizil to'lqinlar diapazonida uzatish;
- 2,4 GGs diapazonda chastotani sakrashsimon qayta sozlash (FHSS) yo'li bilan spektrni kengaytirish texnologiyasi;
- 2,4 GGs diapazonda to'g'ridan-to'g'ri ketma-ketlik usuli bilan spektrni kengaytirishli (DSSS) keng polosali modulyatsiya texnologiyasi.

Infraqizil to'lqinlar diapazonida uzatish

Uzatish muhiti yarim o'tkazgichli lazer diodi yoki yorug'lik diodi (LED) orqali generatsiyalanadigan 850 nm diapazondagi infraqizil to'lqinlar hisoblanadi. Infraqizil to'lqinlar devorlar orqali o'tmaydi, LAN qamrab olish hududi to'g'ridan ko'rish zonasi bilan chegaralanadi. Standart uchta yo'naltirilmagan antennadan, shundan qaytish va nurlanishni fokusli yo'naltirish nurlanishni tarqalishi yo'nalishlari variantlarini ko'zda tutadi. Birinchi holda tor nur linzalar tizimi yordamida tarqaladi. Fokusli yo'naltirilgan nurlantirish ikki nuqtali, masalan ikkita binolar orasidagi aloqani tashkil etish uchun mo'ljallangan.

Chastotani sakrashsimon qayta sozlash (FHSS) simsiz lokal tarmoqlar

FHSS simsiz lokal tarmoqlar 1 va 2 Mbit/sekund uzatish tezliklarida ishlaydi. FHSS qurilmalari ularning ishlashi uchun mo'ljallangan 2,402 dan 2,480 GGs chastotalar polosalariga 79 ta yopilmaydigan kanallarga bo'linadi. 79 ta kanallarning har birining kengligi 1 MGs ni tashkil etadi, shuning uchun FHSS simsiz lokal tarmoqlar 1 MGs dan nisbatan yuqori simvollarni uzatish tezliklari va kanaldan kanalga nisbatan kichik qayta sozlanish tezliklarini ishlatadi.

Chastotani qayta sozlanishi ketma-ketligi quyidagi parametrlarga ega bo'lishi kerak: sakrab o'tishlar chastotasi minimum 6 ta kanallar orasida (6 MGs) sekundiga 2,5 martadan kam bo'lmasligi kerak. Berkutiladigan qoplash zonalari kolliziyalar sonini minimallashtirish uchun bo'lishi mumkin sakrab o'tishlar ketma-ketligi uchta ketma-ketliklar to'plamiga bo'linishi kerak, ularni uzunligi Shimoliy Amerika va Yevropaning katta qismi uchun 26 ni tashkil etadi. 2.1-jadvalda minimal berkitilishni ta'minlaydigan chastotani sakrashsimon qayta sozlash sxemasi keltirilgan [4].

Chastotani sakrashsimon qayta sozlash sxemasi bo'lishi mumkin bir kanaldan boshqasiga shoshilmasdan shunday o'tishni ta'minlaydiki, har bir sakrashdan keyin minimum 6 MGs ga teng chastotalar polosasi qoplanadi, shu tufayli ko'p sotali tarmoqlarda kolliziyalarni vujudga kelishi imkoniyatlari minimallashtiriladi.

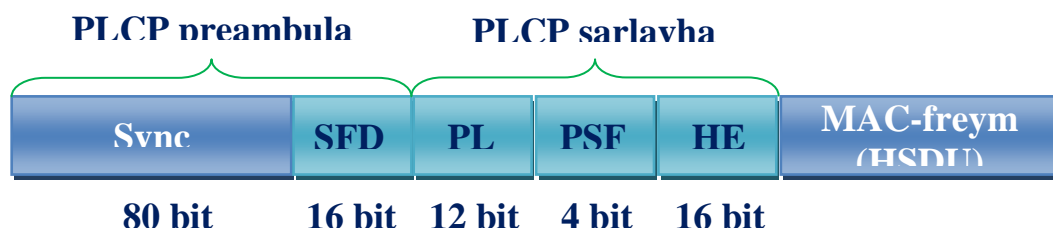
2.1- jadval.

Shimoliy Amerika va Yevropa uchun FHSS sxemasi

To'plam	Chastotani sakrashsimon qayta sozlash sxemasi
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,67,60,63,66,69,72,75}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
3	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}

MAC daraja FHSS simsiz lokal tarmoqlarda PLCP yoki PSDU (PLCP Service Data Unit) ma'lumotlari xizmat elementi ham deyiladigan MAS-freymni o'tkazganidan keyin PLCP nimdaraja PRDU freymni (PRDU-PLCR protokoli ma'lumotlari elementi)

shakllantirish uchun MAS-freymni boshlanishiga ikkita maydonni qo‘shadi. 2.5- rasmda PLCP nimdaraja FHSS freymining formati keltirilgan.



2.5- rasm. PLCP nimdaraja FHSS freymining formati

PLCP preambulasi ikki maydonchalardan iborat:

- 80 bit o‘lchamli *Syns maydonchasi*. 0 va 1 raqamlar almashib keladigan satr 0 dan boshlanadi. Qabul qiluvchi stansiya bu maydonni imkoniyati bo‘lganida antennani tanlash haqida qarorni qabul qilish, chastotani o‘zgarishini tuzatish (frequency offset) va paketlarni taqsimlanishini sinxronlashtirish (packet timing) uchun ishlatadi;

- 16 bit o‘lchamli *freymni boshlanishi bayrog‘i (Start of Frame Delimiter, SFD) maydonchasi*. Qabul qiluvchi stansiya uchun freymlarning sinxronlashtirilishini (frame timing) ta‘minlashdagi o‘ziga xos satrlardan (0000, 1100, 1011, 1101, chapdan chetdagi birinchi bit) iborat.

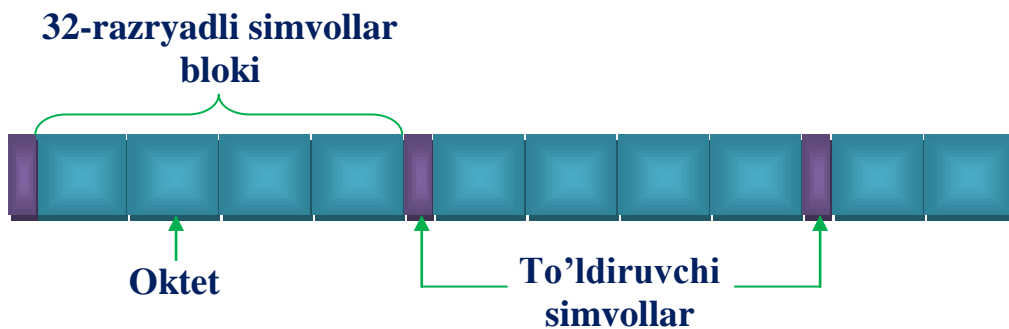
PLCP freym sarlavhasi uchta maydonchalardan iborat:

- 12 bit o‘lchamli *PLCP (PSDU), PSDU Length Word (PLW) ma‘lumotlari xizmat elementi uzunligi so‘zi*. MAS (PSDU) freymi o‘lchamlarini oktetlarda ko‘rsatadi;

- 4 bit o‘lchamli *PLCP signalli maydoni (Signaling Field PLCP-PSF)*. Aniq bir freym ma‘lumotlarni uzatish tezligini ko‘rsatadi.

- *NES (Header Error Check)*. Freymning nazorat yig‘indisi.

PLCP (PSDU) ma‘lumotlari xizmat elementi kirish bitlari ketma-ketliklarini “oqlash” (randomizatsiya) maqsadida skrembirlash operatsiyasi orqali o‘tadi. Natijada olingan PSDU 2.6-rasmda keltirilgan. To‘ldiruvchi simvollar barcha 32-simvulli bloklar orasiga qo‘yiladi. Bu to‘ldiruvchi simvollar keyingi qayta ishlagda nojo‘ya samaralarga olib kelishi mumkin bo‘lgan ma‘lumotlardagi istalgan tizimli o‘zgarishlarni, masalan birlar nollardan ko‘p yoki aksincha xatoliklarni tuzatadi.



2.6- rasm. FHSS texnologiyasidagi skrembirlangan PSDU

PLCP nimdaraja freymni bitlar oqimiga o'zgartiradi va uni PMD nimdarajaga uzatadi. FHSS texnologiyasining PMD nimdarajasi ma'lumotlar oqimini Gauss chastotaviy modulyatsiyasiga (Gaussian Frequency Shift Keying-GFSK) asoslangan modulyatsiyadan foydalanib modulyatsiyalaydi.

To'g'ridan-to'g'ri ketma-ketlik usuli bilan spektrni kengaytirishli DSSS keng polosali modulyatsiyani ishlatadigan simsiz lokal tarmoqlar

802.11 standart spesifikatsiyasida boshqa to'g'ridan-to'g'ri ketma-ketlik usuli bilan spektrni kengaytirishli (DSSS) keng polosali modulyatsiya texnologiyasi asosidagi fizik darajaning ishlatilishi haqida ham so'z borgan. 1997 yildagi 802.11 standartda ko'rsatilganidek, DSSS texnologiya 1 va 2 Mbit/sekund uzatish tezliklarida ishlaydi.

FHSS texnologiyasida ishlatiladigan PLCP nimdarajaga o'xshash 802.11 standartning DSSS texnologiyasida PLCP nimdaraja PRDU ni shakllantirish uchun MAS-freymga ikkita PLCP preambula va PLCP sarlavha maydonlarini qo'shadi. Freymning formati 2.7- rasmda keltirilgan.



2.7- rasm. PLCP nimdaraja DSSS freymi formati
PLCP preambulasi ikkita maydonchalardan tashkil topgan:

- *Birlardan iborat satr bo'lgan 128 bit kenglikdagi Syns maydonchasi.* Bu maydonchaniing vazifasi qabul qiluvchi stansiya uchun sinxronlashtirishni ta'minlash hisoblanadi;

16 bit kenglikdagi SFD maydoncha. Unda o'zga xos Ox3A0 satr mavjud. Uning vazifasi qabul qiluvchi stansiya uchun taymingni (timing) ta'minlash hisoblanadi.

PLCP sarlavhasi to'rtta maydonchalardan tashkil topgan:

- *Bu freym uchun modulyatsiya turi va uzatish tezligini ko'rsatadigan 8 bit kenglikdagi Signal maydonchasi;*

- *8 bit kenglikli Service maydonchasi zahirallashtirilgan.* Bu standart spesifikatsiyasini ishlab chiqish vaqtida noaniq qoldi. U standartning bo'lajak modifikatsiyalarida kerak bo'ladi;

- *MAC-freym qismini uzatish uchun zarur bo'ladigan mikrosekundlar sonini ko'rsatadigan 16 bit kenglikdagi Length maydonchasi;*

- *CRC maydoncha.* 16-bitli nazorat yig'indisi.

PLCP nimdaraja freymni bitlar oqimiga o'zgartiradi va uni PMD nimdarajaga uzatadi. Butun PRDU ma'lumotlarni randomizatsiyalash maqsadida skremblirash jarayoni orqali o'tadi.

Skremblirlangan PLCP preambula doimo 1 Mbit/sekund tezlikda uzatiladi, shu bilan bir vaqtda skremblirlangan MRDU freym Signal maydonchasida ko'rsatilgan tezlikda uzatiladi. PMD nimdaraja quyidagi modulyatsiya turlaridan foydalanish bilan "oqlangan" bitlar oqimini modulyatsiyalaydi:

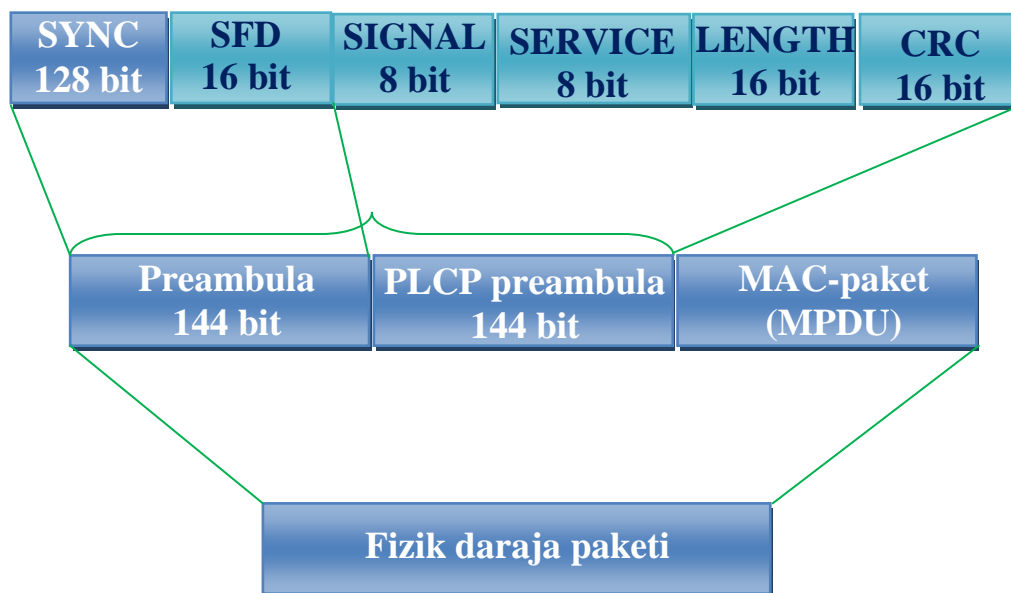
- 1 Mbit/sekund uzatish tezligi uchun ikkilik nisbiy fazaviy modulyatsiya (Differential Binary Phase Shift Keying-DBPSK);

- 2 Mbit/sekund uzatish tezligi uchun kvadraturali nisbiy fazaviy modulyatsiya (Differential Quadraure Phase Shift Keying-DQPSK).

IEEE 802.11b standarti

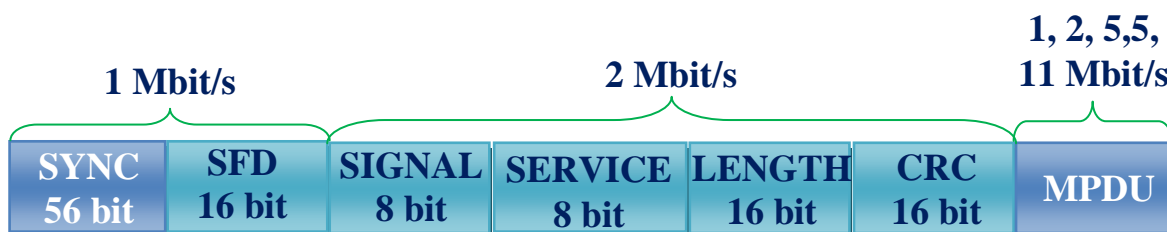
Fizik darajada MAC-kadrlarga (MRDU) preambula va o'z PLCP-sarlavhasidan iborat fizik daraja sarlavhasi qo'shiladi (2.8-rasm). Preambula qabullagichni sozlash uchun boshlang'ich sinxron ketma-ketlik va kadrning boshlanishi 16-bitli kodi bo'lgan (SFD) F3A016 sonidan iborat bo'ladi. PLCP-sarlavha GISIGNAL (modulyatsiya turi va tezligi haqida axborotlar), SERVICE (qo'shimcha, shu jumladan yuqori tezlikli kengaytirishlar va RVSS-modulyatsiya haqida axborotlar) va LENGTH (kadrning sarlavha qismidan keyingi uzatish uchun zarur bo'ladigan mikrosekundlardagi

vaqt) maydonlaridan tashkil topgan. Barcha uchta sarlavhalar maydonlari 16-bitli CRC nazorat yig'indisi bilan himoyalangan.



2.8- rasm. IEEE 802.11b tarmog'ı fizik darajasi kadrlari tuzilmasi

IEEE 802.11b standartda ikki uzun va qisqa turlardagi sarlavhalar ko'zda tutilgan (2.9- rasm).



2.9- rasm. IEEE 802.11b tarmog'ı kadrlar qisqa sarlavhasi

2.4. IEEE 802.11a, IEEE 802.11g va IEEE 802.11n standartlari

1997 yilda IEEE 802.11 belgisini olgan birinchi Wi-Fi standarti paydo bo'ldi. Bu standart radiochastota va infraqizil to'lqinlarida ishlashga mo'ljallangan bo'lib, 1 va 2 Mbit/sekund ma'lumot uzatish tezliklarini taqdim etdi. Radiochastota kanalida chastotalarda sakrash (rus. *pereskok*) hisobiga spektrni kengaytirish (ingl. *Frequency Hopping Spread Spectrum, FHSS*) va to'g'ri ketma-ketlik hisobiga spektrni kengaytirish (ingl. *Direct Sequence Spread Spectrum, DSSS*) usullari ishlatildi.

Ammo, xatto 1997 yil uchun ham 1 – 2Mbit/s tezliklar yetarli bo‘lmadi va 802.11 guruhi yangi yuqoriroq tezliklarni taqdim etadigan standartlarni ishlab chiqish ustida harakatlar boshladi. Bu vaqtga kelib ko‘plab davlatlarda Wi-Fi tarmoqlari uchun HTI tomonidan tavsiya etilgan 2400-2483,5 MGs va 5150-5350 MGs diapazonlaridagi polosalarga ruxsat berildi va har ikkala diapazonlarda standartlar yaratish ustida parallel ishlar olib borildi [4].

IEEE 802.11a — Wi-Fi tarmoqlar standarti hisoblanadi.

5 GGs U-NII (*ingl.*) chastotaviy dipazon ishlatiladi.

IEEE 802.11b standartning standartlashtirilishi va 802.11g standartning joriy etilishi tufayli bu standartning kam ishlatilishiga qaramasdan u ham chastota va modulyatsiyalash tomonidan o‘zgartirildi. OFDM ko‘plab nimchastotalarda ma’lumotlarni parallel uzatishga imkon beradi. Bu halaqitlarga barqarorlikni oshiradi va bittadan ortiq ma’lumotlar oqimlari uzatilar ekan, yuqori o‘tkazish qobiliyati ta’minlanadi.

IEEE 802.11a idealsharoitlarda 54 Mb/sgacha tezlikni ta’minlashi mumkin. Pastroq ideal sharoitlarda (yoki toza signalda) qurilmalar 48 Mb/s, 36 Mb/s, 24 Mb/s, 18 Mb/s, 12 Mb/s va 6 Mb/s tezliklarda ishlashi mumkin [3].

IEEE 802.11a standarti 802.11b yoki 802.11g standartlar bilan moslashmaydi.

Uzoq vaqt IEEE 802.11b keng tarqalgan standart bo‘ldi, uning asosida ko‘plab simsiz lokal tarmoqlar qurildi. Hozir uning o‘rnini IEEE 802.11g standarti egallagan bo‘lib, uni ham yuqori tezlikli IEEE 802.11n standarti asta-sekin surib chiqarmoqda.

IEEE 802.11g standarti 2002 yilning oktyabrida tasdiqlangan. Bu standart 54 Mbit/sgacha ulanish tezligini ta’minlash va bu bilan 11 Mbit/s ulanish tezligini ta’minlaydigan IEEE 802.11b standartdan ustun bo‘lish bilan 2,4 GGs chastotalar diapazonida ishlashni ko‘zda tutadi. Bundan tashqari, u IEEE 802.11b standarti bilan teskari moslashuvchanlikni ta’minlaydi. IEEE 802.11g standartning teskari moslashuvchanligi DSSS modulyatsiyalash rejimda va bog‘lanish tezligi sekundiga 11 megabitgacha cheklanganida yoki tezlik 54 Mbit/sgacha yetishi mumkin bo‘lgan OFDM modulyatsiyalash rejimida ishlatilishi mumkin. Shunday qilib, bu standart simsiz tarmoqlarni qurishda eng to‘g‘ri keladigan standart hisoblanadi.

IEEE 802.11n — Wi-Fi tarmoqlar uchun 802.11 standartning versiyasi hisoblanadi.

Bu standart 2009 yilning 11 sentyabrida tasdiqlangan.

802.11n standarti boshqa 802.11n qurilmalari ishlash rejimidan foydalanish shartida 802.11g standartlari qurilmalariga (ularning maksimal uzatish tezligi 54 Mbit/sga teng) qaraganda ma'lumotlarni uzatish tezligini deyarli to'rt martaga oshiradi. Nazariy jihatdan 802.11n ma'lumotlarni birdaniga to'rtta antennalar bo'yicha uzatishni qo'llash bilan 600 Mbit/sgacha ma'lumotlarni uzatish tezligini ta'minlay oladi. Bitta antennaga 150 Mbit/sgachadan to'g'ri keladi.

802.11n qurilmalari 2,4—2,5 yoki 5,0 GGs diapazonlarda ishlaydi.

Bundan tashqari, 802.11n qurilmalari quyidagi uchta rejimlarda ishlashi mumkin:

- 802.11b/g va 802.11a qurilmalarini qo'llashni ta'minlash uchun olingan (Legacy) rejim;
- 802.11b/g, 802.11ai 802.11n qurilmalarini qo'llash uchun ta'minlanadigan aralash (Mixed) rejimi;
- “toza” 802.11n rejim (aynan bu rejimda 802.11n standarti ta'minlaydigan oshirilgan tezlik va oshirilgan ma'lumotlarni uzatish masofasi ustunliklaridan foydalanish mumkin).

802.11n standartning xomaki versiyasini (DRAFT 2.0) ko'plab zamonaviy qurilmalarni qo'llaydi. Standartning yakuniy versiyasi (DRAFT 11.0) 2009 yilning 11 sentyabrida qabul qilingan va 300 Mbit/sgacha tezlik, MIMO sifatida ma'lum bo'lgan ko'p kanalli kirish/chiqish va katta qamrab olishni ta'minlaydi [3].

Standartning o'ziga xos xususiyatlari:

Ma'lumotlarni real uzatish tezligi

Ma'lumotlarni real uzatish tezligi doimo kanalli tezlikdan past bo'ladi. Wi-Fi uchun ma'lumotlarni real uzatish tezligi odatda kam tomonga ikki martadan ortiqqa farqlanadi.

Bundan tashqari, real o'tkazish qobiliyatini cheklaydigan yana bir necha omillar mavjud:

- Kanal doimo mijozlar orasida bo'linadi;
- Xizmat trafigini uzatish bilan ulanish nuqtasi doimo minimal tezlikda ishlayotgan mijozga sozlanadi ;
- Halaqitlarning mavjudligi (ulanish nuqtasining yonida ishlaydigan mikroto'lqinli pechlar, “radio-enagalar”, bluetooth-qurilmalar, radiotelefonlar).

Ta'kidlash kerakki, 802.11b standartda ishlashda yoki u bilan moslashadigan rejimni ta'minlashda faqat uchta bir-birlarini

qoplamaydigan, ya'ni bir-birlariga halaqit qilmaydigan kanallar mavjud bo'ladi. Ya'ni, agar devorning ortida qo'shnida ulanish nuqtasi 1-nchi kanalda ishlayotgan bo'lsa, sizda esa uyda 3-kanal bo'lsa, u holda bu ulanish nuqtalari bir-birlariga halaqit qiladi, bu bilan ma'lumotlarni ulanish tezligini pasaytiradi.

Ikkita chastotalar diapzonlari

802.11n standart bo'yicha qurilmalar 2,4 yoki 5 GGs diapzonlarini ishlatishi mumkin, bu radiochastotali halaqitlar ta'sirini kamaytirish bilan aloqaning ishonchliligini oshiradi. 2008 yilda 802.11n standartining deyarli barcha mijozlari CardBus va ExpressCard asosida faqat 2,4 GGs diapazonda ishlay oladi, har ikkala diapazonlarni esa ayrim o'rnatiladigan adapterlar qo'llaydi.

40 MHz kenglikdagi kanal

802.11n spetsifikatsiyada 20 MGs kenglikdagi standart kanallar, shuningdek 40 MGs keng polosali kanallar ko'zda tutilgan. Bu yechim o'tkazish qobiliyatini oshiradi. Ta'kidlash kerakki, 2,4 GGs diapazonda faqat ikkita kesishmaydigan keng polosali kanalni joylashtirish mumkin.

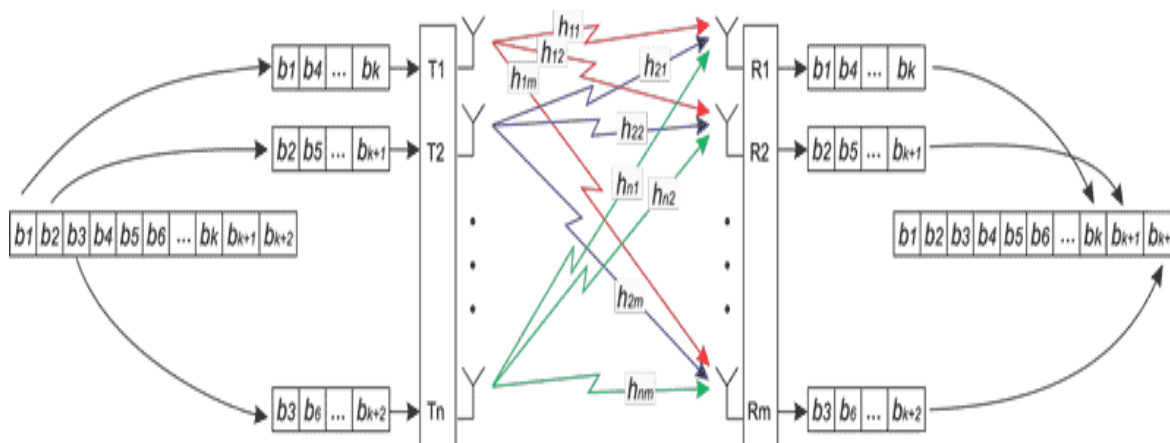
802.11n standarti muhim yangi joriy etish MIMO (ingl. *Multiple Input, Multiple Output* — «ko'p kirishlar, ko'p chiqishlar») kiritadi, u yordamida fazoviy multiplekslash – bir necha axborot oqimlarini bitta kanal bo'yicha bir vaqtda uzatish, shuningdek signalni yetkazilishi uchun halaqitlar ta'siri va ma'lumotlarni yo'qotilishini minimallashtiradigan, lekin bir necha antennalarning bo'lishini talab qiladigan ko'p nurli tarqatishdan foydalanish amalga oshiriladi. Aynan ma'lumotlarni bir vaqtda uzatish va qabul qilish 802.11n qurilmalarining o'tkazish qobiliyatini yuqoriroq qiladi.

2013 yilning boshlanishiga kelib ishlab chiqaruvchilar taklif etayotgan ulanish nuqtalarining ko'pchiligi MIMO 2×2 yoki 1×1, ya'ni SISO (bir oqimli uzatish) rejimni qo'llaydi. Mobil qurilmalarga o'rnatilgan Wi-Fi-adapterlar odatda SISO rejimni qo'llaydi.

Nazariy jihatdan, n ta uzatish va n ta qabullash antennalarili MIMO-tizimi SISO tizimiga qaraganda n martaga katta maksimal o'tkazish oralig'ini ta'minlashi mumkin. Bu uzatkich ma'lumotlarni oqimini mustaqil bitlar ketma-ketliklariga bo'lishi va ularni antennalar massividan foydalanish bilan qayta uzatishi orqali erishiladi. Bunday uzatish texnikasi fazoviy multiplekslash deyiladi. Ta'kidlaymizki, barcha antennalar ma'lumotlarni bir-birlariga bog'liq bo'lmagan holda o'sha bir chastotalar diapazonida uzatadi.

n ta uzatish va n ta qabullash antennalaridan iborat boʻlgan MIMO-tizimini koʻrib chiqamiz (2.10-rasm). Bunday tizimda uzatkich n ta oʻzaro bogʻliq boʻlmagan signallarni n ta antennalarni qoʻllash bilan uzatadi. Qabullash tomonida m ta antennalardan har biri barcha uzatish antennalaridan n ta signallarning superpozitsiyasi hisoblanadigan signallarni oladi. Shunday qilib, birinchi antenna qabul qiladigan R_1 signalni quyidagi koʻrinishda berish mumkin:

$$R_1 = h_{11}T_1 + h_{21}T_2 + \dots + h_{n1}T_n$$



2.10- rasm. MIMO texnologiyasining ishlatilishi prinsipi

Har bir qabullash antenasi uchun bunday tenglamani yozish bilan quyidagi tenglamalar tizimini olamiz:

$$\begin{cases} R_1 = h_{11}T_1 + h_{21}T_2 + \dots + h_{n1}T_n; \\ R_2 = h_{12}T_1 + h_{22}T_2 + \dots + h_{n2}T_n; \\ \dots \\ R_m = h_{1m}T_1 + h_{2m}T_2 + \dots + h_{nm}T_n. \end{cases}$$

Yoki bu ifoda matritsali koʻrinishda yozilsa:

$$[R] = [H] \cdot [T]$$

bu yerda $[H]$ — MIMO-aloqa kanalini tavsiflaydigan oʻtkazish matritsasi.

Qabullash tomonida dekoder barcha signallarni qayta tiklay olishi uchun u avvalo $m \times n$ uzatish kanallaridan har birini xarakterlaydigan

h_{ij} koeffitsientlarni aniqlashi kerak. h_{ij} koeffitsientlarni aniqlash uchun MIMO texnologiyasida paket preambulasi ishlatiladi.

Matritsaning koeffitsientlarini aniqlash bilan uzatilgan signalni oson qayta tiklash mumkin:

$$[T] = [H]^{-1} \cdot [R]$$

bu yerda $[H]^{-1}$ — $[H]$ o'tkazish matritsasi teskari matritsa.

Ta'kidlash muhimki, MIMO texnologiyasida bir necha uzatish va qabullash antennalarining qo'llanilish bir necha fazoviy surilgan nimkanallarni ishlatilishi hisobiga aloqa kanalining o'tkazish qobiliyatini oshirishga imkon beradi.

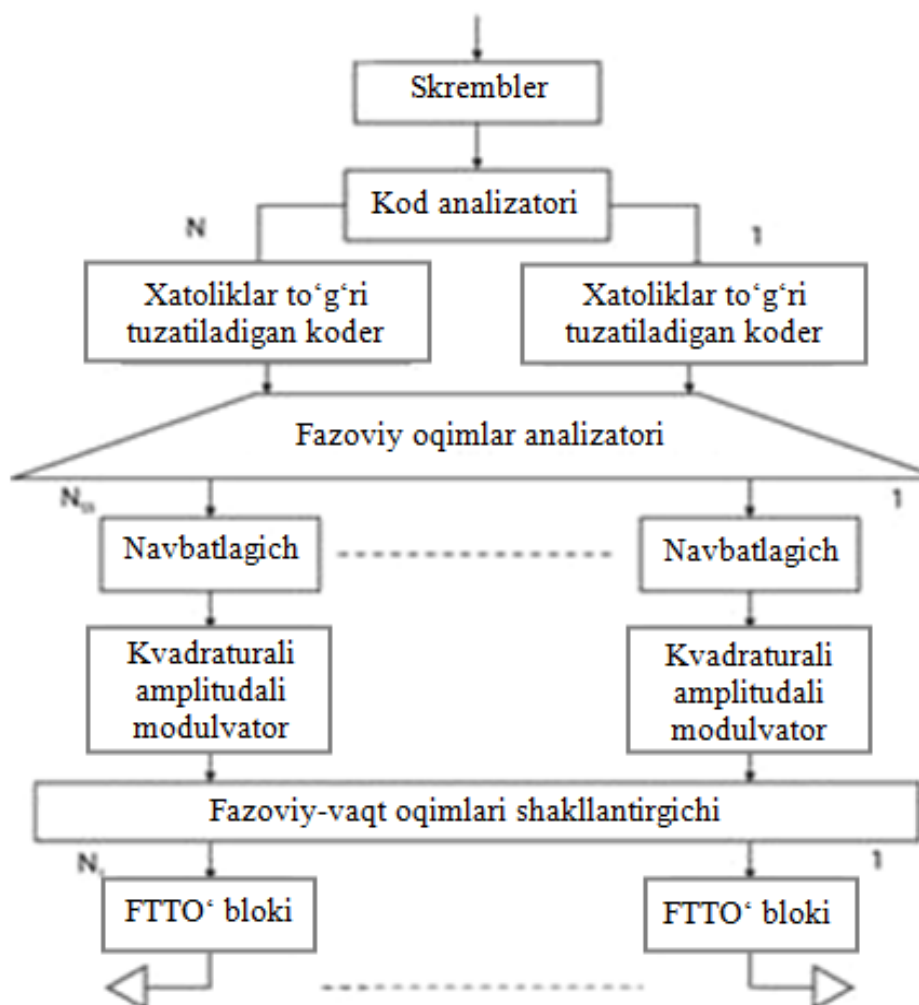
MIMO texnologiyasi kodlash usuliga hech qanday ta'sir etmaydi va prinsip jihatdan istalgan ma'lumotlarni fizik va mantiqiy kodlash usullari bilan birgalikda ishlatilishi mumkin.

802.11n uzatkichi va qabullagichi

IEEE 802.11n standartida ulanish nuqtasi va simsiz adapterda to'rttagacha antennalardan foydalanishga ruxsat etiladi. Majburiy rejim ulanish nuqtasida ikkita antennalarni va simsiz adapterda bitta antennani qo'llashni ko'zda tutadi. IEEE 802.11n standartida ham 20 MGs kenglikdagi standart kanallar, ham ikkilangan kenglikli kanallar ko'zda tutilgan.

Uzatkichning umumiy tuzilish sxemasi 2.11- rasmda tasvirlangan. Uzatiladigan ma'lumotlar bir xil simvollarning uzun ketma-ketliklaridan qochish uchun kodga qo'shimcha nollar va birlarni qo'yadigan (psevdo-tasodifiy shovqin bilan niqoblash) skrembler orqali o'tadi. Keyin ma'lumotlar N oqimlarga bo'linadi va xatoliklar to'g'ri tuzatiladigan koderiga (FEC) beriladi. Agar uchta yoki to'rtta uzatish kanallari ishlatilsa, bir yoki ikkita antennalarli $N = 1$ oqimli tizimlar uchun $N = 2$ bo'ladi.

Kodlangan ketma-ketlik alohida fazoviy oqimlarga bo'linadi. Har oqimdagi bitlar navbatlashadi (blokli xatoliklarni yo'qotish uchun), keyin esa modulyatsiyalanadi. Keyin Fur'e tez o'zgartirish bloki orqali o'tadigan va antennalarga beriladigan fazoviy-vaqt oqimlarini shakllantirish bo'lib o'tadi. Fazoviy-vaqt oqimlarining soni antennalar soniga teng. Uzatkichning tuzilmasiga o'xshash, lekin barcha amallar teskari tartibda bajariladigan qabullagichning tuzilmasi 2.12- rasmda tasvirlangan.



2.11- rasm. MIMO-OFDM uzatkichining umumiy tuzilmasi

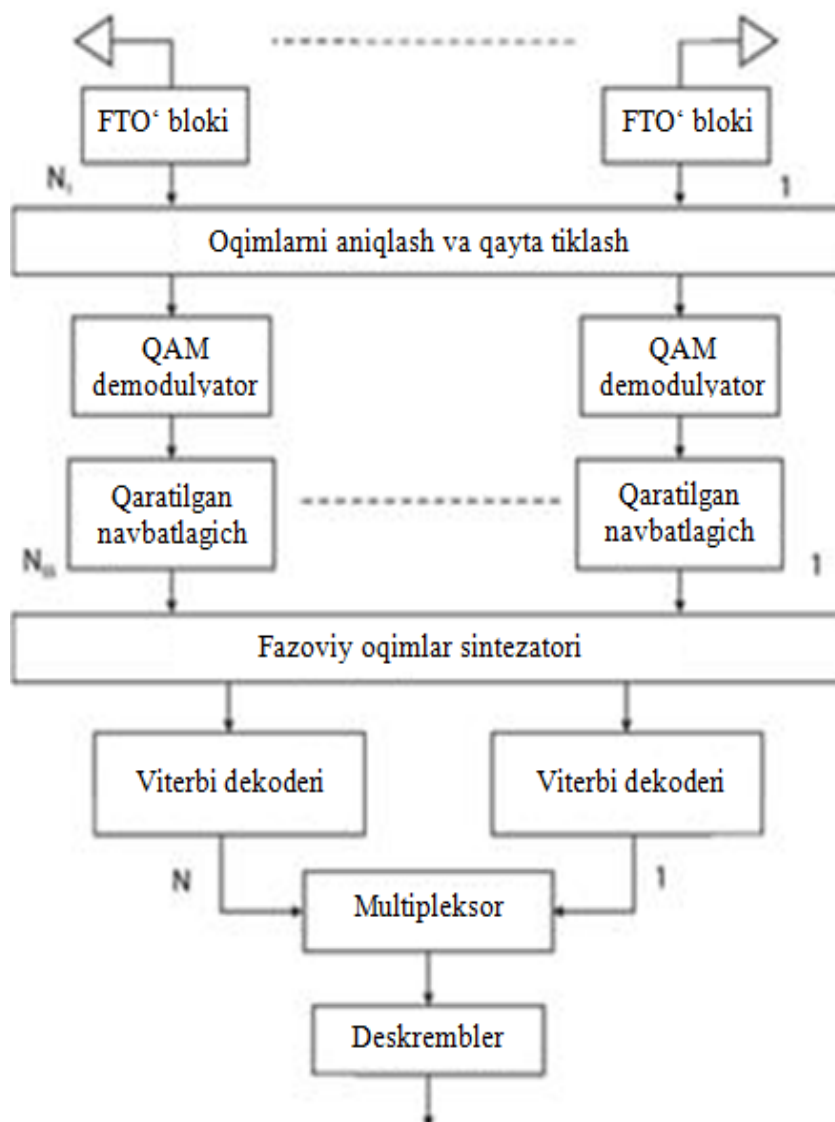
Antennalar

IEEE 802.11n qurilmalarida odatda ma'lumotlarni uzatish va qabul qilish zanjirlari uchun 3×3 yoki 2×3 konfiguratsiyadagi antennalar ishlatiladi, lekin vaqt o'tishi bilan boshqalar ham qo'llanishi mumkin. Oddiyroq modellar bitta uzatuvchi va ikkita qabul qiluvchi radiozanjirlardan iborat (chunki abonentlar odatda ma'lumotlarni uzatmaydi, balki yuklaydi) sxemani ishlatadi. Ma'lumotlarni uzatish tezligiga oshirilgan talablarli foydalanuvchilar 4×4 konfiguratsiyali antennalarli modellarni ishlatishi mumkin bo'ladi.

Ethernet tarmog'i orqali ta'minot

IEEE 802.3af-2003 (PoE) tarmoq ta'minoti standarti 3×3 va undan yuqori antennalar konfiguratsiyalarili ulanish nuqtalarining elektr ta'minoti uchun zarur bo'ladigan quvvatni ta'minlamaydi. Uni almashtirishga maksimal quvvatni ikki martaga oshirilishini ko'zda

tutadigan IEEE 802.3at-2009 keldi, bu 4×4 konfiguratsiyali antennalarli qurilmalarni ta'minlash uchun yetarli bo'ladi.



2.12- rasm. MIMO-OFDM qabullagichining umumiy tuzilmasi

Tarmoqdagi zaif joylar

Bu standartni qo'llaydigan ulanish nuqtalarida o'tkazish qobiliyati 100 Mbit/sdan ortishini hisobga olganda, Fast Ethernet kanallari tarmoq trafigi yo'lida zaif joy bo'lib qolishi mumkin. Shuning uchun simsiz tarmoqni qurishda Gigabit Ethernet kommutatorlaridan foydalanish kerak.

Teskari moslashuvchanlik

IEEE 802.11n asosidagi komponentlar 2,4 GGs diapazondagi 802.11b va 802.11g standartlari qurilmalari va 5 GGs diapazondagi 802.11a standarti qurilmalar bilan moslashuvchan. Kutilmoqdaki,

yangi 802.11n tarmoqlarida yana bir qancha vaqt eskirgan standartlarni ishlatadigan mijozlar ishlab turadi, shuning uchun simsiz LHTlarni qurishda ularni qo'llashni ko'zda tutish kerak bo'ladi [3].

Wi-Fi zonalari shakllari

Radioto'lqinlarning tarqalishiga halaqitlar bo'lmaganida simsiz lokal tarmoqlarning zonalari sferik shaklga ega bo'ladi. 802.11n standartida ko'zda tutilgan MIMO texnologiyasi va fazoviy multiplekslash zonalarni kam oldindan aytiladigan va muntazam qiladi, chunki shakl binodagi sharoitlarga bog'liq bo'la boshlaydi. Shunday qilib, tarmoqni rejalashtirish uchun nazorat-o'lchash vositalari modernizatsiyalashli talab qilishi mumkin.

Modulyatsiyalash indeksi va kodlash sxemalari

802.11n simsiz ulanish nuqtalari va mijozlari kanalning kengligi va fazoviy oqimlarni (ingl. *spatial streams*) muvofiqlashtirishni amalga oshiradi. Fazoviy oqimlar soni antennalarning soniga bog'liq bo'ladi. Maksimal nazariy o'tkazish qobiliyatiga faqat 4x4 konfiguratsiyada – 4 ta uzatish va 4 ta qabullash antennalarida erishish mumkin.

802.11n standarti modulyatsiyalash indeksi va kodlash sxemalarini (ingl. *modulation and Coding Scheme. MCS*) 0 dan (eng sekin, lekin ishonchli rejimga mos keladi) 31 gacha (eng tezkor, lekin radiohalaqitlarga sezgir rejim) butun sonlar ko'rinishida aniqlaydi. Indeks radiochastotani modulyatsiyalash turini, kodlash tezligini (ingl. *coding rate*), himoya intervalini (ingl. *guard interval*) va kanalning kengligini aniqlaydi. Bu parametrlar birgalikda 6,5 Mbit/sdan boshlab 600 Mbit/s gacha nazariy ma'lumotlarni uzatish tezligini aniqlaydi.

Modulyatsiyalash turi (masalan, 802.11dan BPSK yoki 802.11a dan QAM) va kodlash tezligi ma'lumotlarni efirga uzatish tezligini aniqlaydi. Yangiroq modulyatsiyalash turlari samaraliroq va yuqoriroq ma'lumotlarni uzatish tezliklarini ta'minlashi mumkin, eskiroqlari esa teskari moslashuvchanlikni ta'minlashga xizmat qiladi. 300 Mbit/s maksimal bog'lanish tezligiga erishish uchun ham ulanish nuqtasi, ham mijozning qurilmasi ikkita fazoviy oqimni va ikkilangan 40 MGs kanal kengligini ta'minlashi kerak.

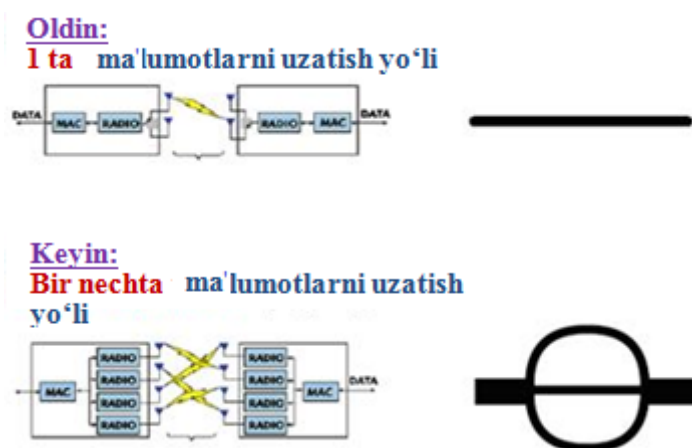
802.11n spetsifikatsiyasi 2009 yilning 11 sentyabrida tasdiqlangan

802.11n standartida ma'lumotlarni yuqoriroq tezliklarda uzatilishi omillari

Yuqorida aytilganidek, 802.11n standartida ma'lumotlarni uzatish tezligini oshirish uchun uchta asosiy mexanizmlar qo'llaniladi:

- bir necha qabullagich-uzatikichlar va radiosignalning maxsus uzatish va qabullash algoritmlarining qo'llanilishi;
- signal chastotalar polosasini 20 dan 40 MGsgacha oshirilishi;
- tarmoqqa ulanish darajasi protokolini optimallashtirish.

Bu mexanizmlardan har birini ko'rib chiqamiz.

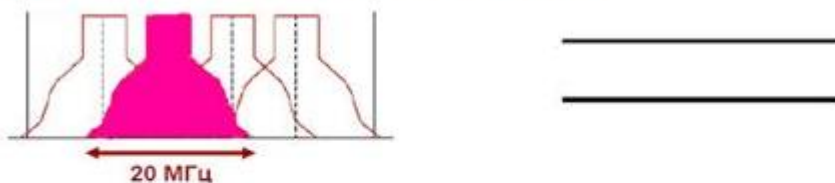


2.13- rasm. Ma'lumotlarni uzatish tezligini oshirilishining birinchi omili

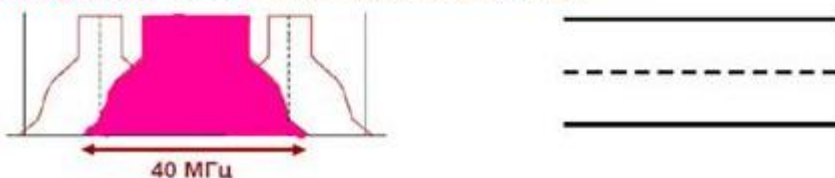
Birinchi omil. MIMO qo'llanilishi bilan o'sha bir kanalda bir necha ma'lumotlar oqimlarini bir vaqtda uzatish va keyin ularni qabullashda murakkab ishlov berish algoritmlari yordamida qayta tiklash imkoniyati paydo bo'ladi. Buni avtomobil yo'llariga o'xshatish bilan aytish mumkinki, oldin A va V nuqtalarni birlashtiradigan faqat bitta yo'l bo'lgan bo'lsa, endi bunday yo'llar bir nechta va tizimning umumiy o'tkazish qobiliyati oshadi.

Ikkinchi omil mumkin chastotalar polosasi kengligini oshirilishi hisoblanadi. Aloqa kanalining nazariy erishiladigan o'tkazish qobiliyati u egallaydigan chastotalar polosasiga to'g'ridan-to'g'ri bog'liq bo'ladi. Yangi standartda 20 MGs bo'yicha qo'shni kanallarni birlashtirilishi va bunday tarzda o'tkazish qobiliyatini deyarli ikki martaga oshirilishi imkoniyati paydo bo'ldi. Avtomagistrallarga o'xshatish bilan aytish mumkinki, harakatlanish uchun mumkin polosalar soni ikki martaga oshdi.

Oldin:
Bir polosali ma'lumotlarni uzatish magistrali



Keyin:
Ikki polosali ma'lumotlarni uzatish magistrali

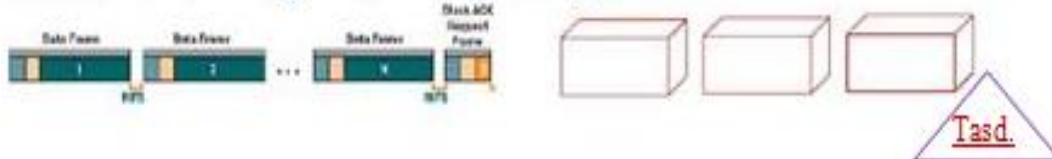


2.14- rasm. Ma'lumotlarni uzatish tezligini oshirilishining ikkinchi omili

Oldin:
Har bir kadrni tasdiqlanishi
Kadrlar orasidagi katta vaqt oralig'i



Keyin:
Kadrlar blokini tasdiqlanishi
Kadrlar orasidagi kichik vaqt oralig'i



2.15- rasm. Ma'lumotlarni uzatish tezligini oshirilishining uchinchi omili

Birinchi ikkita omillar fizik kanalga tegishli bo'ldi. Unumdorlikni oshirilishining uchinchi muhim omili muhitga ulanish darajasi protokolini optimallashtirilishi hisoblanadi. Oldingi versiyalarda har bir uzatilgan kadrni (ma'lumotlarni porsiyasini) qabul qilish tomonidan tasdiqlanishi kerak edi. Yangi versiyada blokli tasdiqlash imkoniyati kiritilgan. Ma'lumotlarni qabullagich bir necha

muvaffaqiyatli qabul qilingan kadrlarga birdaniga bir necha tasdiqlashni uzatadi, bu kanalning umumiy o'tkazish qobiliyatini xizmat xabarlar bilan yuklanishini kamaytiradi. Bundan tashqari, kadrlar orasidagi vaqt oralig'i kamaytirilgan, bu ham foydali o'tkazish polosasini oshirishga imkon beradi. Kundalik hayotga o'xshatish bilan yuklarni tashish uchun konteynerlarli kadrlarni taqqoslash mumkin. 802.11n yangi qoidalari konteynerlar orasidagi masofani kamaytirishga imkon berdi va dispetcherga har bir yukni alohida emas, balki yuklar guruhini tasdiqlashga imkon berdi.

IEEE 802.11ac standarti

Texnologiyani rivojlanishining navbatdagi bosqichi oldingi masofa va bog'lanishning stabiligi saqlanishi bilan 1 Gb/s dan ortiq maksimal o'tkazish qobiliyatini ta'minlay oladigan standartni yaratilishi bilan belgilandi (2.16-rasm). Masala 2011 yilda xomaki variantlar – draft - 802.11/ac nomini olgan yangi Wi-Fi standartini chiqishi bilan hal etildi. Lekin yakuniy sertifikatlashtirish va standartni tasdiqlanishi faqat 2013 yilning oxirida bo'lib o'tdi va 802.11/ac ni qo'llaydigan birinchi qurilmalar sotuvda 2014 yildan paydo bo'la boshladi [12].

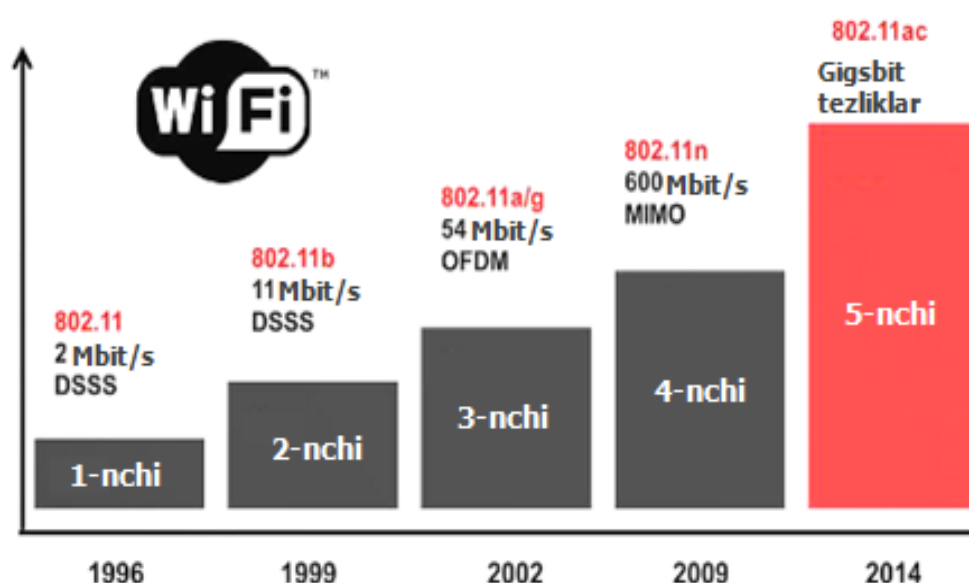
Yangi 802.11/ac standartni oldingi 802.11/n standartdan farqi nimada? Farqlar ko'p va ular juda sezilarli. Bu o'sha bir chastotada ishlatiladigan ko'p sonli va katta kenglikli kanallarga, shuningdek bu diapazonning kam shovqinlanganligiga bog'liq. 5 GGs diapazondan foydalanishga qaramasdan, 802.11/ac qo'llanadigan qurilmalar oldingi Wi-Fi versiyalari bilan to'liq moslashuvchan.

Tabiiyki, 802.11/ac da ma'lumotlarni uzatish tezligi ortdi, u bitta kanalga 866 Mb/s ni tashkil etdi. Bunday raqamlarga kanalning maksimal kengiligini 160 MGsga oshirish va 256 QAM modulyatsiyalashni ishlatilishi bilan erishildi. Haqiqatda, ta'kidlash kerakki, hozirda mumkin bo'lgan qurilmalarda kanallar 80 MGs bilan cheklangan, lekin keyinchalik 160 MGs li kanallarni qo'llaydigan qurilmalarning chiqishi kutilmoqda.

MIMOdan OFDM multiplekslashni qo'llash, shuningdek 8 ta fazoviy ma'lumotlar oqimlaridan sinxron foydalanish imkoniyati bilan farqlanadigan MU-MIMO texnologiyasi joriy etilgan, bu istiqbolda deyarli 7 Gb/s gacha tezliklarga erishishga imkon beradi. Aytish kerakki, OFDM ni qo'llashda texnologiya Wi-Fi da oldingi ishlatiladiganidan qandaydir prinsipiial yangilik yo'q. Lekin farq shundan iboratki, 802.11/nda barcha oqimlar ma'lumotlarni bitta

abonentga uzatish uchun ishlatilgan. Bu sxemaning kamchiligi kanalning resurlaridan juda noratsional foydalanish hisoblanadi, masalan, 15 Mb/s tezlikda ma'lumotlar oqimini uzatishda abonent kanalning 150 Mb/s o'tkazish qobiliyatli kanalni to'liq egallagan. WI-FI ulanish nuqtasi faqat u bilan ishlagan, shu bilan bir vaqtda qolgan qurilmalar ma'umotlarni uzatishga o'z navbatini kutgan.

Kanal kengligini oshirilishi, 256 QAM modulyatsiyalashni ishlatilishi va 8 ta fazoviy kanallarni qo'llashi tufayli Wi-Fi 802.11ac standart juda yuqori 7 Gb/s gacha tezlik potensialiga ega, MU-MIMOdan foydalanish esa yirik tarmoqlarda ishlashda unumdorlikni sezilarli ortishini ta'minlaydi [5].



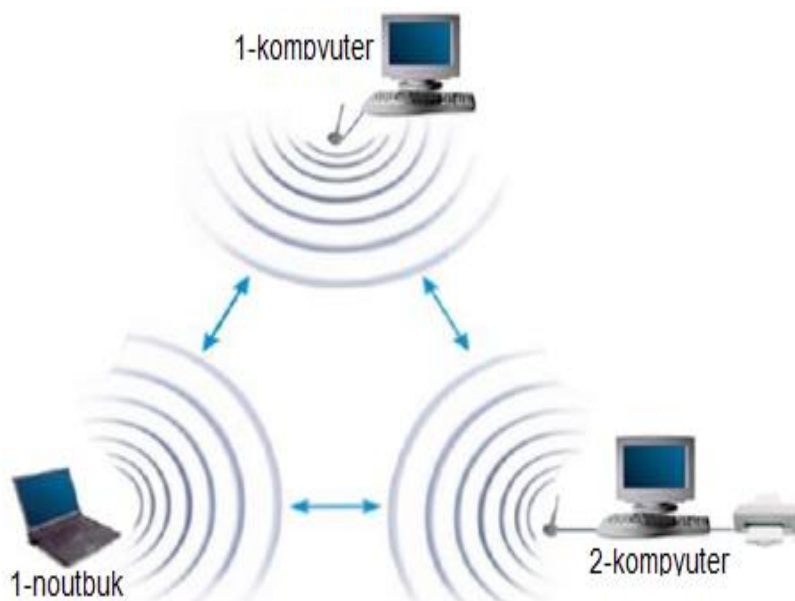
2.16- rasm. IEEE 802.11 standartlarida tezliklarni ortishi

2.5. Simsiz tarmoqlarni tashkil etish va rejalashtirilishi. Ad Hoc rejimi. Infratuzilmali rejim, WDS, WDS with AP rejimlar.

Ad Hoc rejimi

Simsiz tarmoqqa ulanish uchun adapter to'g'ridan-to'g'ri boshqa adapterlar bilan aloqa o'rnatishi mumkin. Bunday tarmoq simsiz bir rangli yoki Ad Hoc ("holatga) tarmoq deyiladi. Ad Hoc rejimida (2.17- rasm) mijozlar bir-birlari bilan to'g'ridan-to'g'ri aloqa o'rnatadi. "Nuqta-nuqta" turi bo'yicha bir rangli o'zaro ta'sirlashish o'rnatiladi va kompyuterlar ulanish nuqtalarini qo'llanilishsiz to'g'ridan-to'g'ri o'zaro ta'sirlashishadi. Bunda simli lokal tarmoqqa

ulanish uchun interfeysga ega bo'lmagan faqat bitta xizmat ko'rsatish zonasi hosil bo'ladi [4].



2.17- rasm. Ad Hoc rejimi

Bu rejimning asosiy afzalligi tashkil etishning oddiyligi hisoblanadi. U qo'shimcha qurilmalarni (ulanish nuqtasi) talab qilmaydi. Rejim ma'lumotlarni uzatish uchun vaqtinchalik tarmoqlarni yaratish uchun qo'llanilishi mumkin.

Lekin, shuni e'tiborga olish kerakki, Ad Hoc rejimi ishlatiladigan qurilmaga bog'liq bo'lmagan holda 11 Mbit/sekunddan ortiq bo'lmagan tezlikdagi bog'lanishni o'rnatishga imkon beradi. Ma'lumotlarni almashtirish real tezligi pastroq bo'ladi va $11/N$ Mbit/sekunddan ortiq bo'lmagan tezlikni tashkil etadi, bu yerda N-tarmoqdagi qurilmalar soni. Aloqaning uzoq masofaliligi 100 metrgachani tashkil etadi, ma'lumotlarni uzatish tezligi esa masofaning ortishi bilan tez kamayadi.

Uzoq vaqtli simsiz tarmoqlarni tashkil etish uchun infratuzilmali rejimni ishlatish kerak bo'ladi.

Simsiz tarmoqni Ad Hoc rejimida sozlashni ikki usulda o'rnatilgan Windows XP yoki Windows Vista xizmatlari va D-Link qurilma komplektida bo'ladigan D-Link AirPlus XtremeG Wireless Utility dasturi yordamida amalga oshirish mumkin.

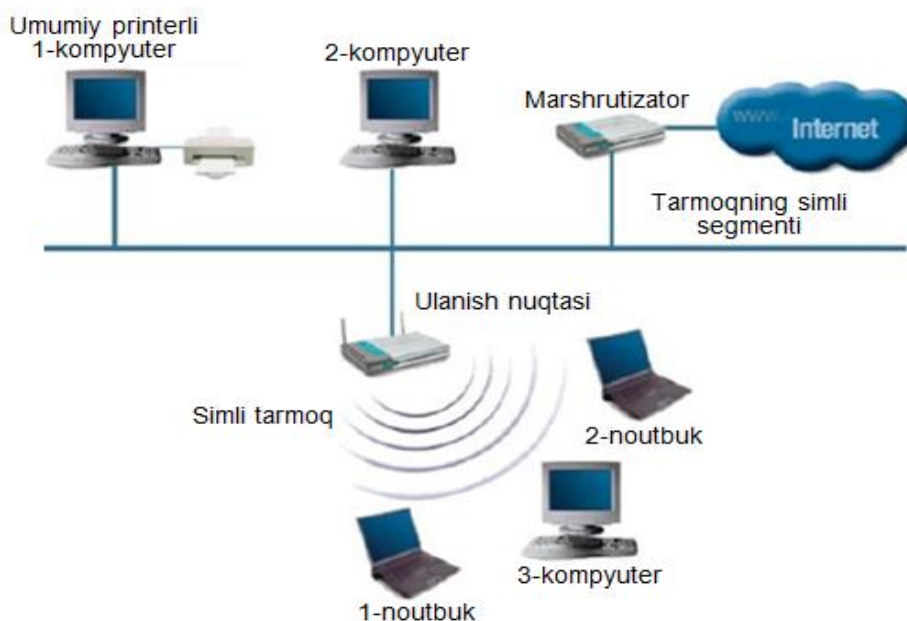
Infratuzilmali rejim

Bu rejimda ulanish nuqtasi mijoz kompyuterlarining aloqasini ta'minlaydi (2.18- rasm). Ulanish nuqtasiga simsiz kommutator

sifatida qarash mumkin. Mijoz stansiyalari biri boshqasi bilan to‘g‘ridan-to‘g‘ri bog‘lanmaydi, ulanish nuqtasi bilan bog‘lanadi, u esa endi paketlarni manzillariga yo‘naltiradi [4].

Ulanish nuqtasi Ethernet portga ega, u orqali bazaviy xizmat ko‘rsatish zonasi simli yoki aralash tarmoqqa, ya’ni tarmoq infratuzilmasiga bog‘lanadi.

Simsiz ulanish nuqtasini infratuzilmali rejimda sozlash simli interfeys, ya’ni Ethernet-bog‘lanishdan foydalanib amalga oshiriladi. Simsiz interfeysdan foydalanilganda ko‘p sonli ulanish nuqtalari bo‘lganida sozlashlarda murakkabliklar yuzaga keladi.



2.18- rasm. Infratuzilmali rejim

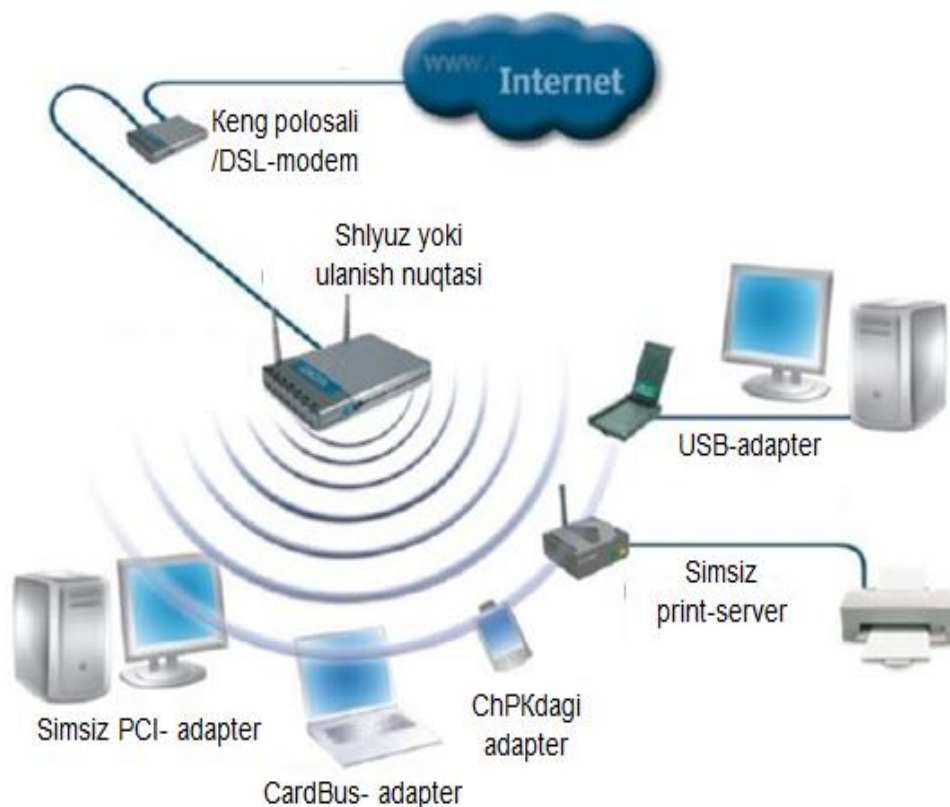
Ofis tarmog‘i

Uncha katta bo‘lmagan ofis yoki uyda foydalanish uchun oddiy simsiz tarmoq (Small Office/Home Office-SOHO) bitta ulanish nuqtasi asosida qurilishi mumkin (2.19-rasm).

Tarmoqni tashkil etish uchun adapterlar infratuzilmali rejimga, ulanish nuqtalari esa ulanish nuqtalari rejimiga o‘tkaziladi. Bunda tarmoqning barcha foydalanuvchilari joylashgan bitta xizmat ko‘rsatish zonasi hosil bo‘ladi [4].

Kichik tarmoqda ulanish nuqtasini joylashtirishda barcha ish o‘rinlarida yetarlicha aloqa sifatini, shuningdek, nuqtaning o‘zini joylashtirishda qulaylikni ta’minlash kerak. Oddiy yechim ulanish

nuqtasini shipga mahkamlash kerak, bunda elektr ta'minoti va simli tarmoq simlari ship ustidan yoki qutilarda o'tkaziladi.



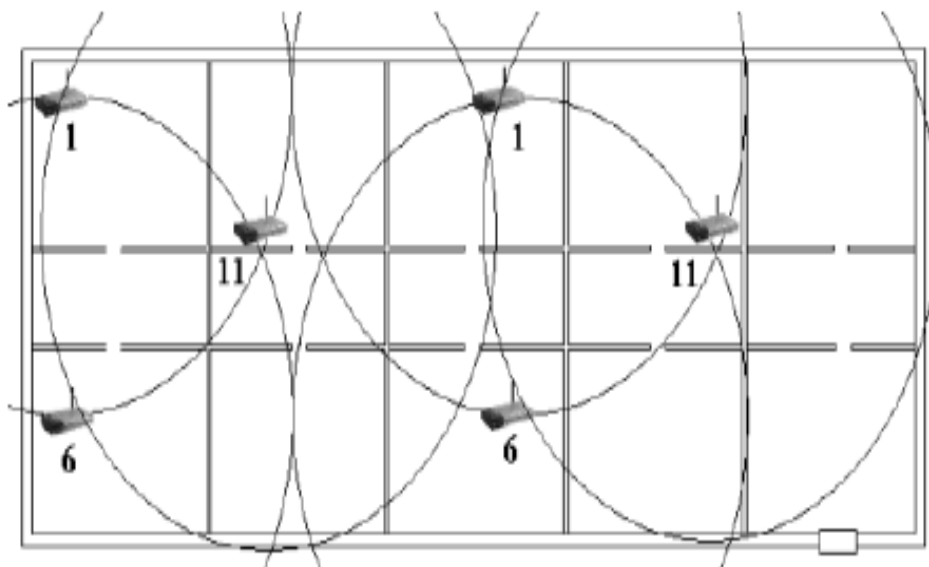
2.19- rasm. Ofis tarmog'i

Shuni e'tiborga olish zarurki, tarmoq kengaytirilganda va foydalanuvchilar soni ortganda aloqa tezligi kamayadi (foydalanuvchilar soniga proporsional). Eng ma'qul foydalanuvchilar soni 16-20. Bundan tashqari, aloqa tezligi va sifati mijoz va nuqta orasidagi masofaga ham bog'liq bo'ladi. Bu bazaviy tarmoqning kengaytirilishini talab qilishi mumkin.

Tarmoqni kengaytirish uchun ulanish nuqtasining uplink-portini ishlatish mumkin. U ham tarmoqqa xizmat ko'rsatish bazaviy zonalarini birlashtirish uchun, ham mavjud simli yoki simsiz infratuzilmaga integratsiyalanishi, masalan, boshqa bo'linmalarning ajratilgan resurslariga foydalanuvchilarni ulanishlarini ta'minlash uchun yoki Internetga ulanishi uchun ishlatilishi mumkin.

Tarmoqni kengaytirishda o'zaro halaqitlar va uzatish tezligini kamayishidan qochish uchun qo'shni ulanish nuqtalarining chastotalari bir-birlarini qoplamasligi kerak. Bunga chastota bo'yicha 1, 6 va 11 qoplanmaydigan kanallarga qo'shni nuqtalarni sozlash bilan erishiladi. Bunday tarzda, 1, 6 va 11 kanallarli qo'shni nuqtalar teng

tomonli uchburchakning uchlarida bo‘lib qolishi natijasida joylarini almashtirish bilan chastotalarni bir-birlarini qoplamasdan katta maydonni simsiz aloqa bilan qamrab olish mumkin (2.20- rasm).



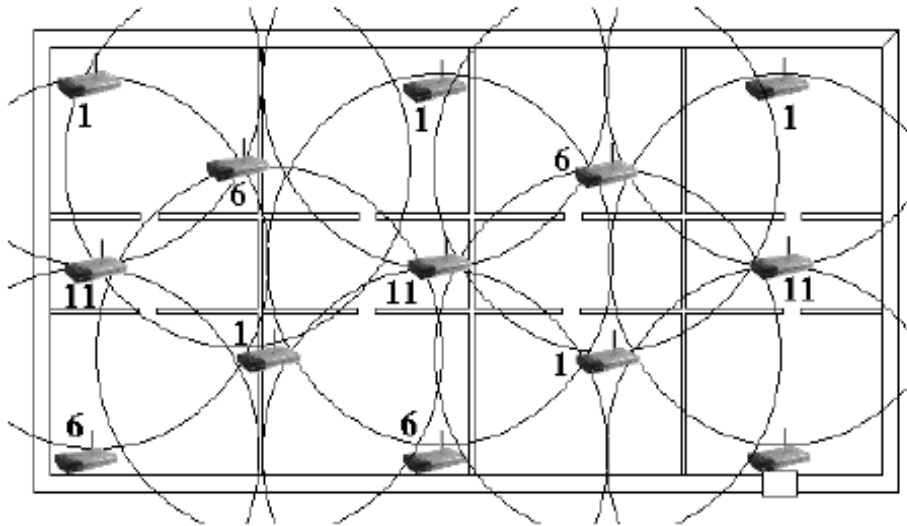
2.20- rasm. Simsiz tarmoqni kengaytirish

Simsiz tarmoqlarni qurishga ishlatiladigan ilovalar turlicha ta'sir qiladi. Eng muhim omillarga quyidagilar kiradi:

- bitta mijozga hisoblaganda hisoblangan tezlik;
- ishlatiladigan ilovalar turlari;
- ma'lumotlarni uzatishdagi kechikishlar.

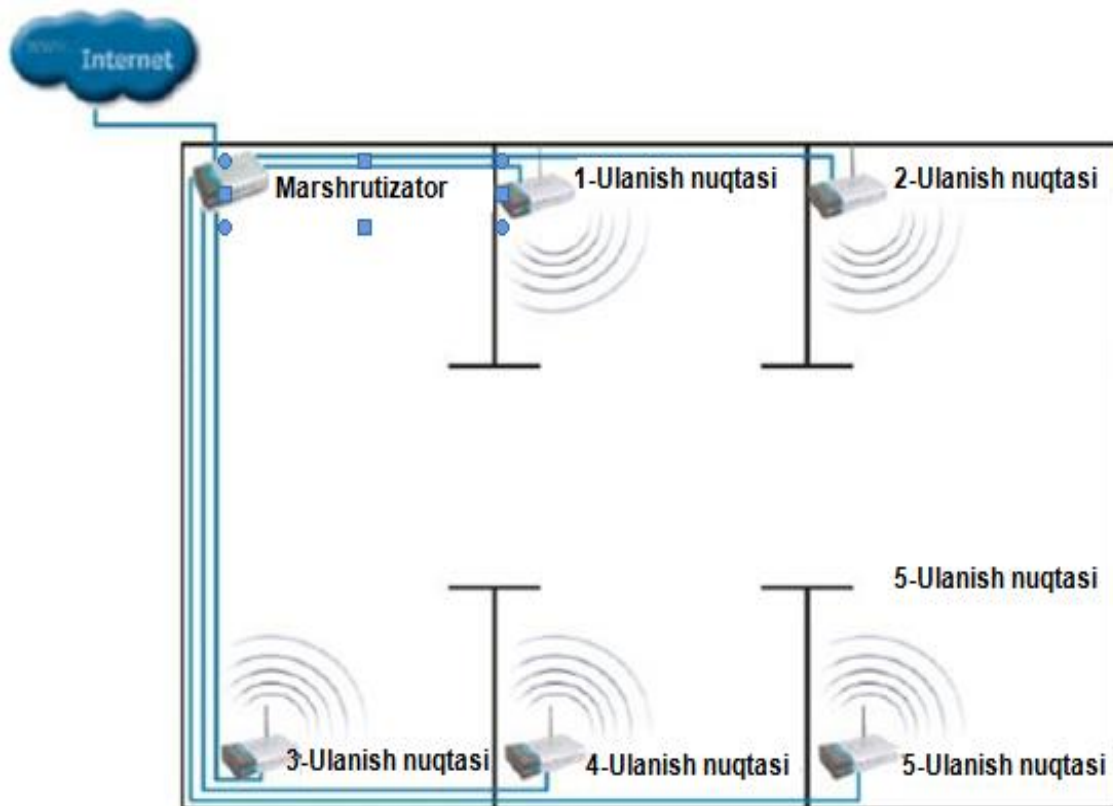
Har bir mijozning hisoblangan tezligi xizmat ko'rsatish zonasiga yangi mijozlarni kiritilishi bilan kamayadi. Demak, agar uyda yoki ofisda tezlikka talabchan bo'lgan ilova ishlatiladigan bo'lsa (masalan, Skype Internet-telefoniya dasturi) maydon birligiga ulanish nuqtalari sonini oshirish zarur bo'ladi (2.21-rasm).

Ulanish nuqtalari ishlash chegaralarini aniqlash uchun Network Stumbler dasturi o'rnatilgan noutbuk ishlatiladi. U ulanish nuqtasidan masofaga bog'liq ravishda adapter qanday tezlikda ishlashini ko'rsatadi. Uzoqlashish bilan tezlik avtomatik kamayadi va bo'sag'aviy darajaga yetganida yangi nuqtani o'rnatish kerak bo'ladi.



2.21- rasm. Simsiz tarmoqni maksimal tezlikli kengaytirish

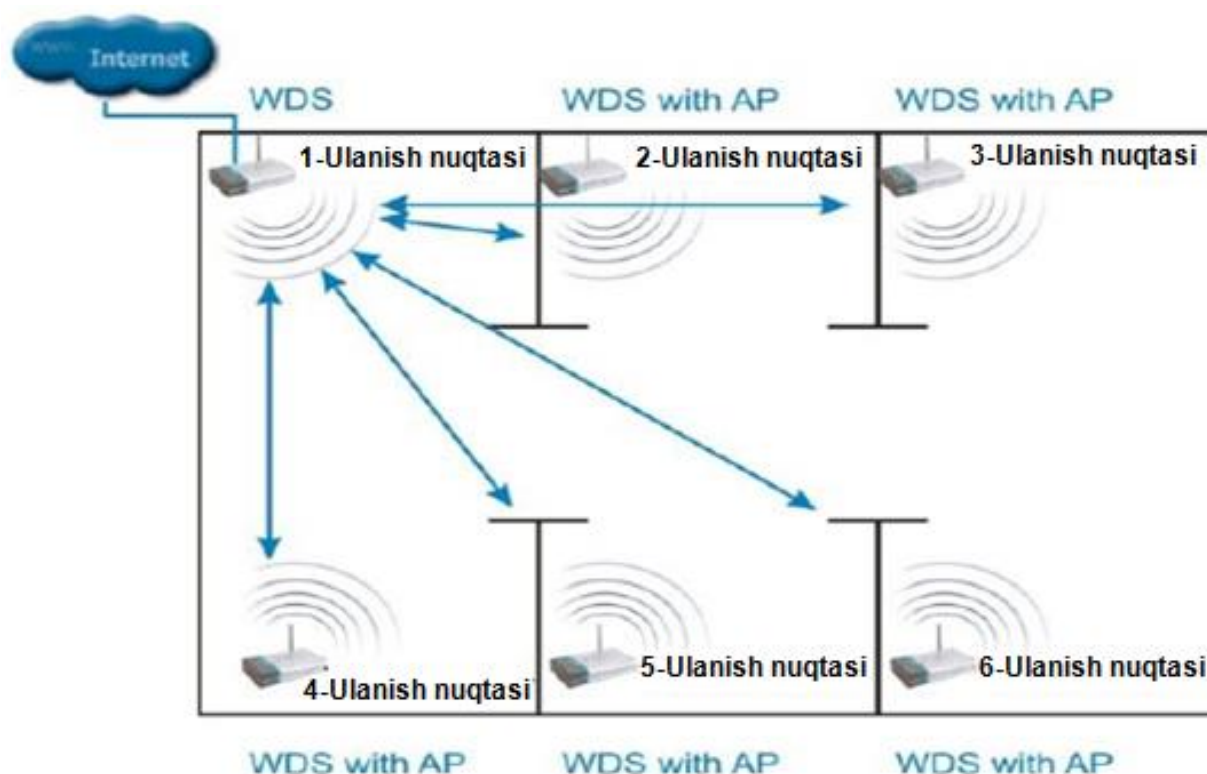
Ofisda barcha ulanish nuqtalarini lokal tarmoqqa birlashtirishni bir necha usullarda amalga oshirish mumkin. Tashkil etishning eng oddiy va eng keng tarqalgan usuli simli infratuzilma orqali birlashtirish hisoblanadi (2.22- rasm).



2.22- rasm. Simli infratuzilma orqali ulanish nuqtalarini birlashtirish

Bunday holda uplink-porti orqali o‘ralgan juftlik simlar yordamida ulanish nuqtasiga ulanadigan kommutator o‘rnatiladi. Shuningdek, bu kommutatorga keng polosali Internetni ulash mumkin. Bunday ulanishning afzalligi ulanish nuqtasining ishlash zonalarini turli kanallarga sozlashning oddiyligi, kamchiligi esa ulanish nuqtalaridan kommutatorga kabel qo‘yilishi hisoblanadi.

Ikkinchi usul WDS kengaytirilgan rejimdan foydalanishli ulanish hisoblanadi (2.23- rasm).



2.23- rasm. WDS kengaytirilgan rejimdan foydalanishli ulanish nuqtalarini birlashtirish

2.6. Tarmoqlarning ishlash rejimlari va ularning tashkillashtirish xususiyatlari

Simsiz lokal tarmoqni tashkil etishda atrof-muhitning bir necha o‘ziga xos xususiyatlarini hisobga olish zarur. Aloqa sifati va uzoq masofaliligiga signal o‘tishi kerak bo‘lgan devorlar, to‘siqlar va boshqa ob‘ektlar soni kabi ko‘plab fizik omillar ta’sir qiladi. Odatda masofa materiallar turlariga va binodagi boshqa elektr asboblardan radiochastotaviy shovqinga bog‘liq bo‘ladi. Aloqa sifatini oshirish uchun quyidagi bazaviy prinsiplarga rioya qilish kerak bo‘ladi [4]:

1. Simsiz tarmoq abonentlari orasidagi devorlar va to'siqlar sonini kamaytirish. Har bir devor va to'siq maksimal radiusdan 1 metrdan 25 metrgachani oladi. Ulanish nuqtasi va abonentlarni shunday joylashtirish kerakki, ular orasidagi to'siqlar soni minimal bo'lishi kerak.

2. Tarmoq ulanish nuqtasi va abonentlari orasidagi burchakni tekshirish. Qalinligi 0,5 metrli devor 30 gradus burchakda radioto'lqinlar uchun 1 metr qalinlikka ega bo'lib qoladi. 2 gradus burchakda esa to'siq 12 metr qalinlikka ega bo'ladi. Tarmoq abonentlarini shunday joylashtirish kerakki, signal to'siqlar yoki devorlarga 90 gradus ostida o'tishi kerak.

3. Qurilish materiallari signalning o'tishiga turlicha ta'sir qiladi. Butunligicha metall eshiklar yoki alyuminiy qoplamalar radioto'lqinlarning uzatilishiga yomon ta'sir qiladi. Iloji boricha tarmoq abonentlari orasida metall yoki temir-beton to'siqlar bo'lmasligi kerak.

4. Signal quvvatini tekshirish dasturiy ta'minoti yordamida antennani eng yaxshi qabul qilishga o'rnatish kerak.

5. Simsiz tarmoq abonentlaridan radiohalaqitlarni generatsiyalaydigan elektr qurilmalarni mikroto'lqinli pechlarni, monitorlarni, elektr motorlarni, uzluksiz elektr ta'minoti manbalarini iloji boricha 1-2 metr masofaga uzoqlashtirish. Halaqitlarni kamaytirish uchun bu asboblarni ishonchli yerga ulanishi kerak.

6. Agar 2,4 GHz standartdagi simsiz telefonlar yoki X-10 qurilmalar (masalan, signalizatsiya tizimlari) ishlatilayotgan bo'lsa, simsiz aloqa sifati sezilarli yomonlashadi yoki uziladi.

Oddiy yashash joylari uchun aloqa masofasi alohida muammo emas. Agar uy chegaralarida ishonchsiz aloqa bo'lsa, u holda ulanish nuqtasini simsiz tarmoq bilan bog'lash kerak bo'lgan xonalar orasiga joylashtirish kerak.

Simsiz tarmoq ishlash zonasiga tushadigan ulanish nuqtalarini topish va ular ishlaydigan kanallarni aniqlash uchun Network Stumbler dasturidan foydalanish mumkin. U yordamida, shuningdek tanlangan kanallardagi "signal-shovqin" nisbatini baholash mumkin.

Wi-Fi tarmoqlarida signalning ko'p nurli tarqalishi (Multipath)

Ko'p nurli tarqalish har bir marta turlicha namoyon bo'ladi. Tushunib olish muhimki, ma'lum sharoitlarda alohida samaralar kuchliroq namoyon bo'ladi, masalan, sezilarli qaytarish xonada katta

metall shkaflar bo'lganida yoki antenna liftning shaxtasi va eshiklari yonida joylashganida kuchliroq namoyon bo'ladi. Istalgan holda bu samaralar bitta dastlabki signaldan ko'plab nusxalarni va ko'plab yo'llarni vujudga kelishi sharoitlarini yaratadi. Bularning barchasini Wi-Fi 802.11 standarti tarmoqlariga to'liq darajada qo'llash mumkin [3].

Binolarining ichida qaytarilgan Wi-Fi signallari va ularning aks-signallarini (Wi-Fi dastlabki signallari nusxalarini) uzun koridorlar, devorlar, stollar, javonlar, shuningdek ko'p sonli boshqa to'siqlar sharoitlari orqali kelib chiqishi mumkin. Aeroportlar angarlari, ombor angarlar, zavodlar va fabrikalar sexlari kabi ko'p metalli ichki zonalar ko'p sonli qaytarish sirtlari tufayli Wi-Fi signallarini ko'p nurli tarqalishi yuqori darajasili ob'ektlar hisoblanadi. Odatda aynan qaytarilgan signallar Wi-Fi signallarini ko'p nurli tarqalishining asosiy sababi hisoblanadi.

Ko'chada (binodan tashqarida) Wi-Fi signallarini ko'p nurli tarqalishini yo'llardan, suvning katta sirtidan (ko'llar, daryolar va h.k.), binolardan va o'ziga xos sharoitlar vujudga kelganida atmosferadan qaytishlar keltirib chiqarishi mumkin.

Shunday qilib, ko'plab turli yo'nalishlarda o'zgaradigan (yaqinlash yoki uzoqlashishda egiladigan) signallarga ega bo'lamiz. Wi-Fi asosiy dastlabki signali qabullash antnennasiga yetib boradi, lekin yo'nalishlari o'zgargan signallar ko'plab nusxalari ham va ko'plab qaytarishlardan keyin mutlaqo oldindan bilib bo'lmaydigan xarakteristikalariga (fazaga, amplitudaga va h.k.) ega bo'lish bilan qabullash antennasiga yetib borishi mumkin. Odatda qaytarilgan signallar uchun asosiy signalga qaragan katta yo'lni bosib o'tish zarurati tufayli qabullash antennasiga yetib borishi uchun bir qancha ko'p vaqt talab qilinadi. Vaqt bo'yicha farq nanosekundlarda o'lchanishi mumkin. Bu vaqt bo'yicha farq signalning tarqalishi kechikishi (delayspread) deyiladi. Bunda ayrim texnologiyalar bunday kechikishlarga ko'proq, boshqalari kamroq uchraydi.

Radiosignallar uchun ko'p nurli tarqalish samarasi ijobiy va salbiy bo'lishi mumkin. Ko'pincha salbiy hisoblanadi. Signallar nusxalarining ko'plab yo'llari fazalaridagi farqlar tufayli qabullagichdagi kombinatsiyalangan signal ko'pincha so'nadi yoki buziladi.

Ko'p nurli tarqalish eskirgan Wi-Fi 802.11 a/b/g standartlar tarmoqlari uchun juda jiddiy muammo hisoblanadi. Yo'naltirilgan

antennalardan foydalanish salbiy samarani kamaytirishga kam imkoniyat beradi. Shuningdek Wi-Fi qabullash antennalarini surilishi (diversity) ijobiy ta'sir etishi mumkin. Ba'zan WiFi-qurilmaga uzatish quvatini pasaytirish yoki kichik kuchaytirish koeffitsientli antennalardan foydalanish yordam beradi.

Zamonaviy Wi-Fi 802.11n standarti tarmoqlari uchun signalning ko'r nurlari tarqalishi muammolarini kompensatsiyalashning sezilarli ko'p mexanizmlari mavjud. Bu yerda katta ijobiy samarani ham uzatish, ham qabullash tomonlarida Wi-Fi antennalari suriladigan MIMO texnologiyasining, shuningdek musbat interfrensiya sharoitlarini sun'iy yaratish va natijaviy kuchaytirish uchun qabul qilingan signallarni raqamli ishlov berish bilan kombinatsiyalash kabi texnikaning (MRC/Maximum Ratio Combining) qo'llanilishi ko'rsatadi.

Quyida sanab o'tilgan qurilmalar keng polosali tarmoqlar bo'yicha simsiz aloqa uchun halaqitlarni hosil qilishi mumkin (2.24-rasm).

Mikroto'lqinli pechlar

Agar kompyuter yoki Wi-Fi bazaviy stansiyasi yaqinida mikroto'lqinli pech ishlasa, u halaqitlarni generatsiyalashi mumkin.

Sun'iy yo'ldoshli televidenie tizimlari

Ayrim sun'iy yo'ldosh antennalari bilan birga ishlatiladigan koaksial kabel yoki biriktirgichlar halaqitlar manbalari bo'lishi mumkin.

Elektr energiya manbalari

Elektr energiyasi liniyalari, elektrlashtirilgan temir yo'llar va kuch nimstansiyalari kabi ayrim tashqi elektr kuchlanish manbalari AirPort bazaviy stansiya, AirPort Time Capsule qurilmalar Wi-Fi yoki marshrutizator elektr o'tkazgichli devorga yoki elektr quri atrofida joylashtirilganida halaqitlar manbalari bo'lishi mumkin.

2,4 yoki 5 GGs diapazonlardan ishlaydigan radiotelefonlar

Chaqiruvlarni qabul qilishda 2,4 yoki 5 GGs diapazonlardan ishlaydigan radiotelefonlar simsiz qurilmalar yoki tarmoqlarning ishlashiga halaqitlarni hosil qilishi mumkin.

Simsiz yuqori chastotali videosignalni uzatkichlar

2,4 yoki 5 GGs diapazonlardan ishlaydigan videosignalni simsiz uzatish uzatkichlari simsiz qurilmalar yoki tarmoqlarning ishlashiga halaqitlarni hosil qilishi mumkin.



2.24- rasm. Ulanish nuqtasiga halaqitlar manbalarini ta'siri

Simsiz dinamiklar

2,4 yoki 5 GGs diapazonlardan ishlaydigan simsiz dinamiklar simsiz qurilmalar yoki tarmoqlarning ishlashiga halaqitlarni hosil qilishi mumkin.

Ayrim tashqi monitorlar va SK-ekranlar

Ayrim monitorlar, ayniqsa, 2,4 GGs chastotadagi 11 va 14 kanallar orasidagi diapazonda sezilarli bo'lgan garmonik halaqitlarni hosil qiladi. Yopiq qopqoqli va ulangan tashqi monitorli noutbukdan foydalanishda halaqitlar yetarlicha sezilarli bo'lishi mumkin.

Yetarli bo'lmagan ekranlashtirilgan kabellar

Tashqi qattiq disklar yoki yetarli bo'lmagan ekranlashtirilgan kabellar simsiz qurilmalar uchun halaqitlarni hosil qilishi mumkin.

Boshqa simsiz qurilmalari

Wi-Fi tarmog'i bo'yicha ulangan qurilmaning ishlashiga 2,4 yoki 5 GGs diapazonda ishlaydigan simsiz asboblari ham, masalan, mikroto'lqinli uzatkichlar, simsiz kameralar, radioenagalar va Wi-Fi tarmog'i bo'yicha ulangan qo'shnilar qurilmalari halaqit quriladi.

Hamma vaqt ham qurilma 2,4 yoki 5 GGs diapazonda ishlayotganligini birdaniga aniqlab bo'lavermaydi. Ishchi diapazonlar haqidagi malumotlar qurilmaga ilova qilinadigan hujjatlarda bo'lishi

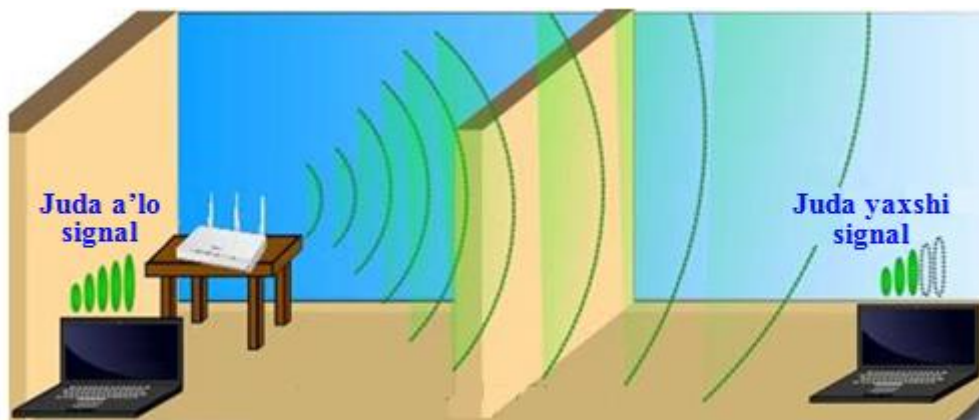
kerak. Bunday qurilmalar simsiz, ikki diapazonli yoki “Wi-Fini qo‘llaydigan” qurilmalar deyiladi.

Simsiz aloqa uchun to‘siqlar

Wi-Fi aloqa sifatiga binoda qurilmalarning joylashishi va atrofdagi binolar qurilgan qurilish materiallari ham ta’sir qilishi mumkin (2.25-rasm). Iloji boricha simsi aloqa uchun to‘siqlardan qochish kerak. Signal to‘siqlarsiz o‘tishi uchun Wi-Fi qurilmalarning joylashishini o‘zgartirish kerak.

Misollar:

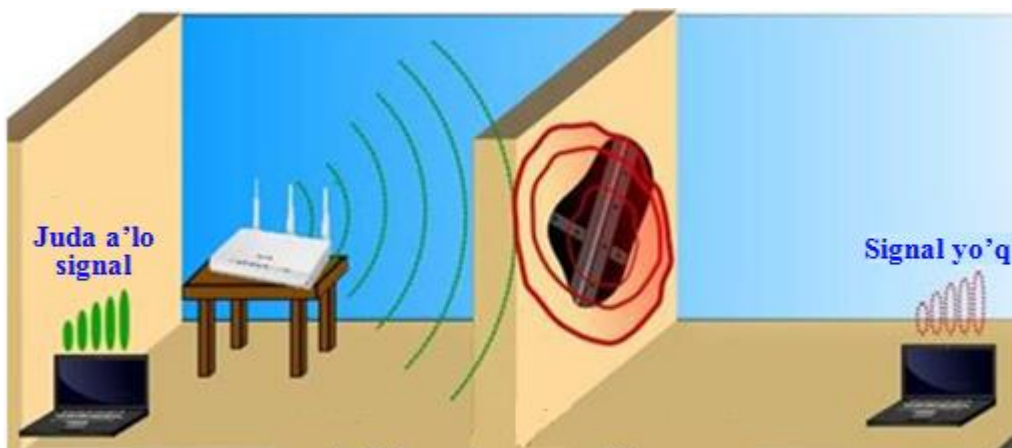
-kompyuterning tizimli bloki usti metalli stol ostida joylashgan. Stolda simsiz sichqonchani ishlatish kerak. Usti metalli stol sichqonchadan kompyuterga signallarni uzatilishiga to‘sqinlik qiladi. Bunda qurilmalarni moslashtirishning iloji bo‘lmaydi yoki kursor ekranda titraydi.



2.25- rasm. To‘siqlardan signallarning o‘tishi

-AirPort bazaviy stansiya qo‘shni xonada joylashgan. Xonalar orasidagi devor metall armaturalardan foydalanilgan betondan qurilgan. Bu bazaviy stansiyadan kompyuterga uzatiladigan Wi-Fi signallari kuchsizlantirishi yoki to‘siq qo‘yishi mumkin. Natijada ulanish tezligi past bo‘ladi yoki Wi-Fi signal kuchsiz bo‘ladi yoki umuman Wi-Fi tarmoqqa ulanish bo‘lmaydi (2.26-rasm).

Quyida 2.2- jadvalda radiochastotalar signallarini qaytarish yoki yutish qobiliyatiga ega bo‘lgan materiallar sanab o‘tilgan.



2.26- rasm. Metall almaturali devor tufayli signalning kuchsizlanishi

2.2- jadval

Radiochastotalar signallarini qaytarish yoki yutish qobiliyatiga ega bo'lgan materiallar

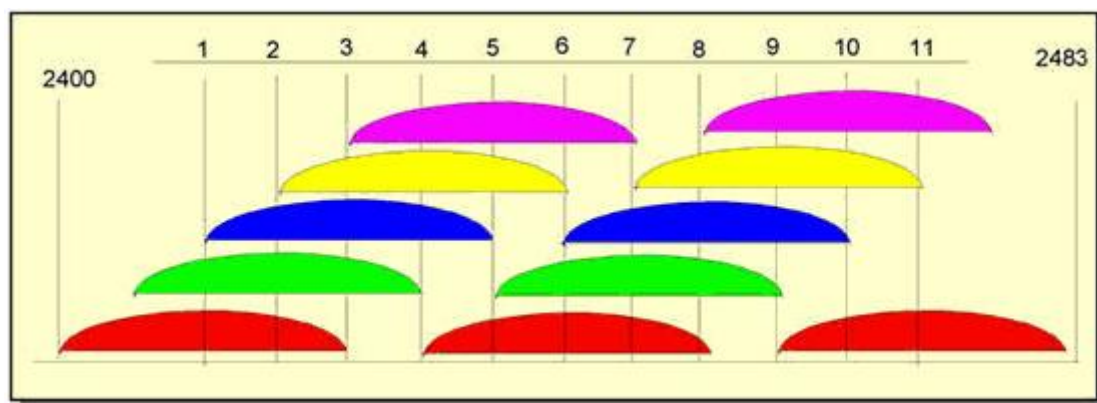
Material	Hosil qiladigan halaqitlari darajasi
Daraxt	Past
Sintetik material	Past
Shisha	Past
Suv	O'rta
G'isht	O'rta
Marmar	O'rta
Gips	Yuqori
Beton	Yuqori
O'q o'tmaydigan shisha	Yuqori
Metall	Juda yuqori

Simsiz tarmoqlarda 2,4 va 5 GGs chastotalar diapazonlari ishlatiladi. 802.11b/g standarti simsiz tarmoqlari 2,4 GGs, 802.11a standarti simsiz tarmoqlari 5 GGs, 802.11n standarti simsiz tarmoqlari esa ham 2,4 GGs, ham 5 GGs chastotalar diapazonlarida ishlaydi.

Ishlatiladigan chastotalar diapazonlari va ishlatishdagi cheklashlar turli davlatlarda turlicha bo'lishi mumkin.

2,4 GGs chastotalar diapazonlarida simsiz tarmoqlar uchun 20 MGs kenglikdagi (802.11b/g/n) yoki ular orasidagi 5 MGs intervallari 40 MGs (IEE 802.11n) kenglikdagi 11 yoki 13 kanallar mumkin bo'ladi. Wi-Fi chastotalar kanallarining birini ishlatadigan simsiz qurilma qo'shni kanallarga halaqitlarni hosil qiladi. Masalan,

agar ulanish nuqtasi 6-kanalni ishlatga, u holda u 5- va 7-kanallarga kuchli halaqitlarni, shuningdek kamroq darajada 4- va 8-kanallarga halaqitlarni hosil qiladi. Kanallar orasidagi o'zaro halaqitlarni yo'qotish uchun ularning tashuvchilari bir-birlaridan 25 MGsga (5ta kanallararo intervallar) ajaralib turishi zarur.



2.27- rasm. 11ta kanallar spektrlari

2.27- rasmda 11ta kanallar spektrlari tasvirlangan. Bitta qamrab olish xizmat ko'rsatish zonasi chegaralaridagi ulanish nuqtalari kanallarni qoplanishini oldini olishi kerak.

Ranglar bilan belgilash kesishmaydigan kanallar guruhlarini belgilaydi, ya'ni [1,6,11], [2,7], [3,8], [4,9], [5,10] bo'ladi. Bitta ishlash zonasi chegaralarida joylashgan turli simsiz tarmoqlarni qoplanmaydigan kanallarga sozlash kerak bo'ladi. Qoplanmaydigan kanallari nomerlari 1, 6 va 11 [15].

2.27- rasmdan ko'rinib turibdiki, 1- 2- kanallar sezilarli darajada qoplanadi. Kanallar nomerlaridan har biri mos kanalning markaziy chastotasi ustida joylashgan. Bitta kanalning markaziy chastotasi qo'shni kanalning markaziy chastotasidan 5 MGsga surilgan, qoplanmaydigan kanallar orasidagi masofa emas 3 MGsni tashkil etadi.

Shunday qilib, bitta yoki qo'shni kanallarda ishlaydigan Wi-Fi-qurilmalar signallari qoplanishi mumkin, bu simsiz ulanish nuqtasiga ulanishga halaqit qilishi mumkin. Bu muammo ulanish nuqtalarining katta zichliklarida, masalan, ko'plab yashovchilar o'z Wi-Fi ulanish nuqtalarini qo'yadigan katta ko'p xonadonli uylarda vujudga kelishi mumkin.

Nazorat savollari

1. 802.11 standartlari to'plamiga qaysi standartlar kiradi?
2. WLAN mahsulotlari uchun birinchi standart qaysi standart?
3. PHY darajaning nimdarajalarini tushuntiring.
4. Skremlirlash va kolliziya nima?
5. IEEE 802.11 tarmoqlarda MAS daraja ajratiladigan muhitga nechta ulanish rejimini ta'minlaydi?
6. DSF ulanish rejimini tushuntiring
7. Yashirin terminal muammosi nima?
8. PLCP freym sarlavhasi nechta maydonchalardan iborat?
9. Ofis tarmog'ini va Ad Hoc rejimini tushuntiring.
10. Aloqa sifatini oshirish uchun qanday bazaviy prinsiplarga rioya qilish kerak bo'ladi?

3- BOB. WiMAX (IEEE 802.16 STANDARTI) SIMSIZ KENG POLOSALI ULANISH TEXNOLOGIYASI

3.1. WiMAX texnologiyasi haqida umumiy tushunchalar

Hozirgi kunda keng polosali simsiz aloqa tizimlari inson hayoti faoliyatining barcha sohalariga kirib bormoqda va butun dunyoda: rivojlangan davlatlarda ham, rivojlanayotgan davlatlarda ham insonlarning yashash sifatini oshirishga xizmat qilmoqda. Ushbu tizimlar yordamida turli xil vazifalarni yechish mumkin: multimediya, interaktiv va personal kontentlarga tezkor va qulay ulanish, an'anaviy nutq aloqasini ta'minlash yoki mahalliy va global jamoalar doirasida axborot almashinuvini amalga oshirish mumkin. IEEE 802.16 (ko'proq, WiMAX sifatida ma'lum bo'lgan) standartlar oilasi deb nomlangan keng polosali simsiz aloqa tizimlari IMS (yangi avlod IP ga asoslangan multimediya nimitizimlari) asosida keng polosali tarmoqlar uchun yaratilgan xizmatlar hamda tezkor Internet kanallarini tashkil etish vositalari bilan birgalikda foydalanuvchilarga (xususan Internetdan) simsiz keng polosali ulanishning prinsipial yangi imkoniyatlarini taklif etadi.

IEEE 802.16 standartini paydo bo'lgunicha Internetga ulanish ancha turg'un bo'lgan, yani foydalanuvchi ish joyidagi kompyuterga yoki juda bo'lmaganda Wi-Fi ulanish nuqtasi doirasidagi noutbukka bog'liq bo'lgan. WiMAX tizimlari keng polosali tarmoqlarga va Internetga ulanishni yanada mobil, yanada ommaviy va yanada keng tarqalgan qilmoqda. Buning uchun turg'un, ko'chma va mobil abonentlarga xizmat ko'rsatadigan simsiz keng polosali tarmoqlar yaratilmoqda. Shunday qilib, Internet va uning barcha ilovalariga, ya'ni axborotlar, xizmatlar va aloqaga har doim va hamma yerda ulanish muhiti shakllantirilmoqda. Bunda WiMAX tizimlariga katta mas'uliyat ajratilmoqda.

3.1.1. WiMAX tizimining tavsifi

WiMAX tizimining Wireless MAN sizziz tarmoqlar tizimiga kiradi. WiMAX atamasi inglizcha "Worldwide Interoperability for Microwave Access" nomini qisqartirishdan kelib chiqadi, bu so'zma so'z tarjima qilganda "Mikroto'lqinli radioaloqa (O'YuCh) asosidagi

tarmoqlarga ulanish uchun butun dunyo o‘zaro ta’sirlashish” ni bildiradi.

Mazkur texnologiya har xil turdagi qurilmalar uchun (avtomatlashtirilgan ishchi stansiyalari va portativ kompyuterlardan tortib mobil telefonlargacha) katta masofalarga yuqori tezlikli simsiz universal aloqani taqdim etish maqsadida ishlab chiqilgan. WiMAX atamasi IEEE 802.16 standartlar atamasini ommalashtirish maqsadida 2001 yil iyunida asos solingan sohaviy forum (WiMAX Forum) tomonidan taklif etilgan [8].

IEEE 802.16 standartlarining ilk versiyalarida 10GGs dan 66GGs gacha bo‘lgan yuqori chastotali diapazonlarda to‘g‘ri ko‘rinish hududida (ingl. *Line of Sight, LOS*) ishlaydigan tizimlar tavsiflangan. Keyinchalik 2GGs dan 11GGs gacha diapazonlarda to‘g‘ri ko‘rinish bo‘lmagan hududlarda ham (ingl. *None Line of Sight, NLOS*) ishlaydigan tizimlarni qo‘llab-quvvatlaydigan standartlar qo‘shimchalarini ishlab chiqishga urg‘u berilgan.

IEEE 802.16-2004 (shuningdek IEEE 802.16d yoki qisqartirib “16d”) nomi bilan ma’lum bo‘lgan standartni yaratishda standartning avvalgi versiyalaridagi barcha ishlanmalardan foydalanilgan. Bu tadbirlar binolar ichida radioqamrovni yaxshilashga imkon berdi va o‘z navbatida, stol ustida ishlatiladigan abonent qurilmalarini yaratishga imkon berdi.

2005 yilning dekabrda IEEE 802.16e (“mobil WiMAX” yoki “16e versiyasi”, ba’zi hollarda “IEEE 802.16-2005”) sifatida ma’lum bo‘lgan standart ustida ishlar yakunlandi va hozirgi kunda u IEEE 802.16 standartlar oilasida eng dolzarb standart bo‘lib qoldi. Hozirda telekommunikatsiyalar bozorida yuqorida ko‘rsatilgan WiMAX standartlarining asosan ikkitasi, yani faqat turg‘un terminallar bilan ishlaydigan IEEE 802.16d standarti va turg‘un, ko‘chma va mobil abonentlar bilan aloqa o‘rnata oladigan IEEE 802.16e standarti namoyon etilgan. 2012 yilda WiMAX ning yangi standarti – IEEE 802.16m tasdiqlanishi kutilmoqda.

3.1.2. WiMAX tizimi va IMT-2000 dasturi

Ma’lumki, Xalqaro telekommunikatsiya ittifoqi (XTI) 3G - uchinchi avlod mobil aloqa tarmoqlarining uyg‘unlashtirish maqsadida, ya’ni mobil aloqa standartlarining ko‘p sonli bo‘lib ketishini oldini olish va ularning global miqyosda o‘zaro ishlay olishi

uchun IMT-2000 dasturini joriy etgan edi. 2006 yilning noyabrida IEEE 802.16 standartlarining asosi hisoblangan yangi IP-OFDMA radiointerfeysining ushbu dasturga qo'shish haqida (ITU-R WP8F/ITU-R Pro.WP/ 1065) IEEE tomonidan taklif kiritilgan [10]. 2007 yilda XTI IMT-2000 dasturi doirasida to'rtta turli ulanish texnologiyalari (FDMA, TDMA, CDMA va OFDMA) ga asoslangan oltita radiointerfeyslarni o'z tarkibida tasdiqlagan. Bularga quyidagi radiointerfeyslar kiradi:

- CDMA-Direct Spread - spektrni to'g'ridan-to'g'ri kengaytirish asosida ishlaydigan CDMA texnologiyasi. UTRA radiointerfeysi, shuningdek, W-CDMA texnologiyasi sifatida ma'lum (yuqorida, 3- Bobda batafsilroq berilgan). UMTS va FOMA standartlarida qo'llaniladi.

- CDMA-Multi Carrier - bir nechta eltuvchilar asosida ishlaydigan CDMA texnologiyasi. CDMA-2000 standartlar oilasida qo'llaniladi.

- CDMA-TDD - vaqt bo'yicha dupleks asosida ishlaydigan CDMA texnologiyasi. UTRA TDD radiointerfeysi. TD-SCDMA standartida qo'llaniladi.

- TDMA-Single Carrier - bir eltuvchi asosida ishlaydigan TDMA texnologiyasi. UWC – IS-136 standarti qo'llanilishi ko'zda tutilgan.

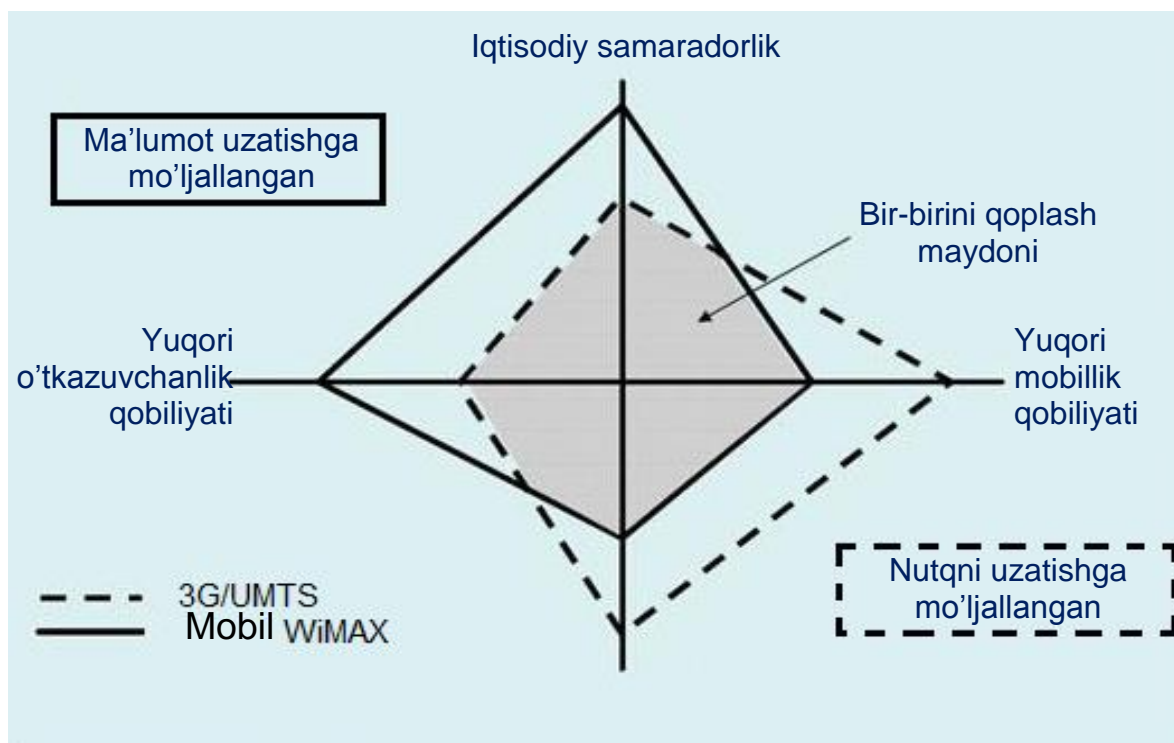
- FDMA-TDMA - FDMA va TDMA texnologiyalarining qo'shilishi. DECT standartida qo'llaniladi.

- IP-OFDMA - IP-protokolini qo'llab-quvvatlaydigan bir necha ortogonal eltuvchilar asosida ko'p sonli ulanish texnologiyasi. FDD chastota bo'yicha dupleks asosidagi OFDMA radiointerfeysi. WiMAX va LTE standartlarida qo'llaniladi.

OFDMA kanallarni ajratish texnologiyasi WiMAX standartini mobil versiyasining asosi sifatida qabul qilingan. OFDMA ning afzalligi yana shundaki, u istiqbolli MIMO, STC va yo'naltirish diagrammalarini shakllantirish kabi samarali antenna texnologiyalarini qo'llab-quvvatlashi tufayli yangi mobil va keng polosali simsiz aloqa tizimlarini yaratish uchun asos hisoblanadi.

Eslatib o'tish kerakki, WiMAX tizimi avvalambor ma'lumot uzatishga asoslangan keng polosali simsiz ulanish texnologiyalarining rivoji hisoblanadi, aksincha, LTE tizimi esa dastlab ovoz uzatishga asoslangan sotali aloqa texnologiyalariga qarashlidir. Lekin bu jarayonda borgan sari keng polosali va mobil aloqa tizimlarining

konvergensiya (bir-biriga yaqinlashishi) yanada yaqqol kuzatilmoqda, xususan, WiMAX texnologiyasi katta mobillikka intilmoqda, LTE tizimi esa o'ta yuqori tezlikda ma'lumot uzatish imkoniyatlari tomon rivojlanmoqda (3.1- rasm).



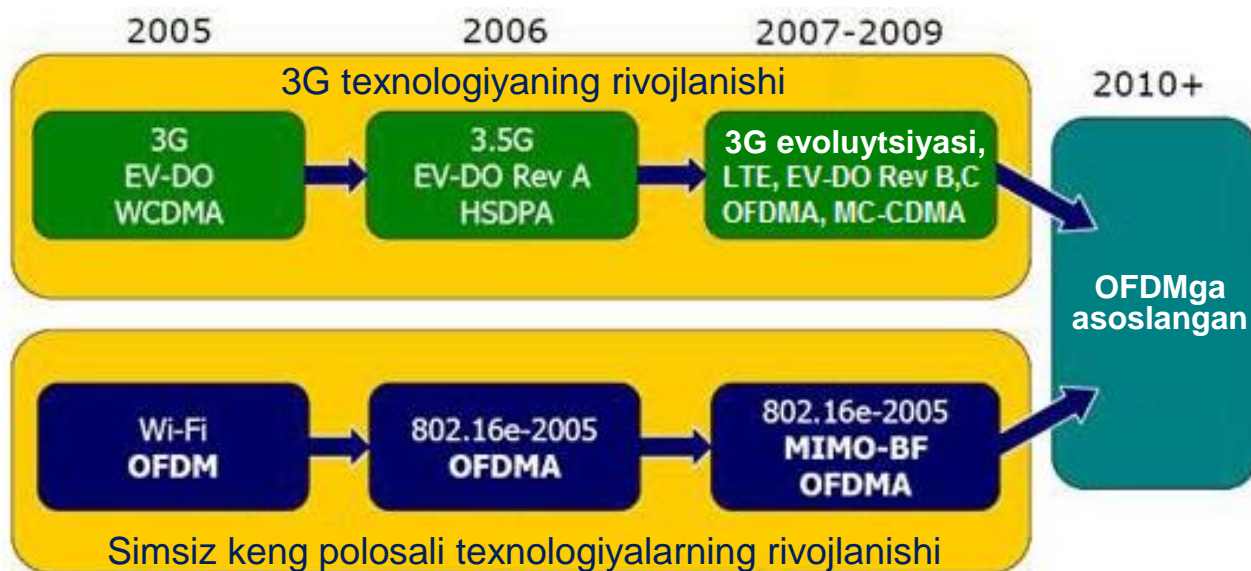
3.1- rasm. Keng polosali va mobil aloqa tizimlarining konvergensiya

WiMAX tizimlarining kelgusi rivoji IEEE 802.16 guruhidagi yangi standartlarning paydo bo'lishi bilan bog'liq deb hisoblanmoqda. IEEE 802.16 ishchi guruhi doirasida standartni takomillashtirish bo'yicha ko'p sonli tadqiqotlar o'tkazilmoqda va hozirgi vaqtda eng istiqbolli deb IEEE 802.16m standarti loyihasi ko'rilmoqda. U ko'zda tutilganidek, IMT Advanced sifatida ma'lum bo'lgan (ya'ni, IMT-2000 dan keyingi) tizimlarni tavsiflaydi. WiMAX forumi IEEE 802.16m standartini WiMAX tizimlarini boshqa mobil texnologiyalar bilan konvergensiya (birlashishining) asosi sifatida baholamoqda. IEEE 802.16m standartining paydo bo'lishi 2012 yilda kutilmoqda.

IMT Advanced dasturi IMT-2000 tizimlarida erishilmagan yanada yuqori ma'lumot uzatish tezligiga, yanada katta mobillikka va funktsionallikka ega tizimlarni yaratishga qaratilgan. Bundan ko'zda tutiladiki, IMT Advanced texnologiyalari yuqori mobillikda 100 Mbit/sek gacha va past mobillikda va turg'unlikda 1 Gbit/sek gacha

tezliklarni ta'minlaydi va shu sabab bu texnologiyalarni mobil aloqa tizimlarining to'rtinchi avlodi - 4G ga kiritish mumkin (3.2- rasm).

Keyinchalik esa mobil va simsiz keng polosali aloqa tizimlarining konvergensiya an'anasi davom etaversa, global miqyosda umumqamrov aloqani ta'minlashga qodir yangi, chinakamiga universal standart paydo bo'lsa ajab emas.



3.2- rasm. Keng polosali va mobil aloqa tizimlari evolyutsiyasi

3.1.3. WiMAX tizimi va “raqamli tengsizlik” muammosi

“Raqamli tengsizlik” (ingl. *Digital Gap*) muammosining ma'nosi nimada? Axborotlarga ega bo'lishlik jamiyatning kengroq iqtisodiy va ijtimoiy rivojlanishiga imkon yaratishi hech kimga sir emas. 1984 yildan boshlab dunyo hamjamiyati rivojlanayotgan mamlakatlarda telekommunikatsiyalar infrotuzilmasi qoloqlili ularning iqtisodiy o'sishi uchun to'siq bo'layotganligini ta'kidlay boshladi. 1996 yilda HTI BMT boshchiligida rivojlanayotgan davlatlarda axborot va kommunikatsion texnologiyalar (AKT) ning asosiy xizmatlariga umumiy ulanishni taqdim etishga va “axborot kambag'alligi” ta'sirini qisqartirishga yo'naltirilgan “Aloqaga huquq” (ingl. “*The Right to Communicate*”) deb nomlangan loyihani olg'a surdi. Ushbu maqsad hozirgi kunda axborot hamjamiyati masalalari bo'yicha Butundunyo sammiti - WSIS (ingl-n *World Summit on the Information Society*) ning barcha rejalarini asosi bo'lib qoldi. 2003 yilning dekabrda Jeneva shaxrida o'tkazilgan WSIS ning birinchi sammitida “Raqamli tengsizlik” deb axborot va kommunikatsion texnologiyalarga noteng

ulanish imkoniyatlari nazarda tutildi. AKTga noteng ulanish deganda, birinchi navbatda davlatlar orasidagi farq (xalqaro raqamli tengsizlik), masalan, rivojlangan va rivojlanayotgan mamlakatlar yoki hududlar orasidagi farq tushuniladi. Shuningdek tengsiz ulanish davlatlar miqyosidagi (milliy raqamli tengsizlik) jarayon sifatida ham aniqlanadi va bunda qishloq va shahar orasidagi, ma'lumotli va kam ma'lumotlilar orasidagi, aholining kambag'al va boy qatlamlari orasidagi farq tushuniladi.

“Raqamli tengsizlik” qanchalik keskin va uning o'zgarish bashoratlari qanday? Provayderlar va Internetdan foydalanuvchilar soni yoki turg'un va mobil telefonlar soni kabi oldindan aniqlangan mezonlar asosida o'tkazilgan tadqiqotlar natijasida, shuningdek, rivojlangan va rivojlanayotgan davlatlarda so'nggi yillarda bo'layotgan o'zgarishlarning tahlili asosida bu masalaning hozirgi ahvoriga turlicha baholar berildi. Bir tarafdin, ham davlatlararo, ham davlatlar miqyosida “Raqamli tengsizlik” o'sib bormoqda, degan fikrlar bo'lsa, boshqa tarafdin, aksincha boy va kambag'al davlatlar orasida “Raqamli tengsizlik” qisqarmoqda, degan fikrlar bo'ldi. Turli xalqaro tashkilotlar (XTI yoki Jahon banki guruhi) e'lon qilgan rasmiy hisob-kitoblarga murojaat qilinsa ma'lum bo'ladiki, rivojlangan va rivojlanayotgan davlatlar orasida AKT ga ulanishdagi tengsizlik mavjud va hali ham jiddiy muammo bo'lib turibdi. Xususan XTI o'z tahlilida quyidagi ma'lumotlarni berdi: hozirgi vaqtda iqtisodiy rivojlangan davlatlarda yashaydigan 942 million aholi kam va nisbatan kam rivojlangan davlatlarda yashaydigan aholiga (yer yuzining qolgan 85% foizi) nisbatan turg'un va mobil aloqa xizmatlaridan 5 marta, Internet xizmatlaridan 9 marta, hamda kompyuterlardan 13 marta ko'proq foydalanish imkoniga egadurlar [14]. Biroq amalda, rasmiy raqamlarga ko'ra, so'nggi o'n yilda “Raqamli tengsizlik” qisqarishining yaqqol belgilari ham namoyon bo'lmoqda. Ammo, shunga qaramay, ahvol sezilarli o'zgarayotgani yo'q, ayniqsa ko'plab aloqa xizmatlariga umuman ega bo'lmagan qishloq joylarda.

O'zicha asosli bo'lgan bunday qarama-qarshi fikrlarning mavjudligiga qaramasdan, ulanish imkoni borligi va uning sifati, ya'ni aloqa infratuzilmasini yaratilishi har xil davlatlarda AKTni tezkor va ishonchli rivojlanishiga asosiy omillar deb hisoblanadi. 2005 yilda XTI “Raqamli tengsizlik” ni qisqartirish uchun hamkorlikni rivojlantirish maqsadida WSIS doirasida global darajada ko'plab

tashkilotlar tomonidan birgalikda o'tkaziladigan "Olamni ulaylik"(ingl. *Connect the World*) deb nomlangan tashabbusni boshladi. Bu tashabbusning maqsadi hozirgi vaqtda hatto oddiy telefon aloqasiga ulanishga ham ega bo'lmagan insonlarga AKT – xizmatlarini taqdim etishdan iboratdir. Shu munosabat bilan WiMAX forumi ming yillik rivojlanish maqsadlariga erishish uchun barcha talablarga javob beradigan yangi simsiz aloqa standartlarini qisqa vaqtda ishlab chiqishga kirishgan. Bu maqsadlar qatoriga "Taraqqiyot uchun global hamkorlikni rivojlantirish" (ingl. *Develop a Global Partnership for Development*) ham kiradi [16]. Ushbu maqsad har bir inson axborotlar va bilimlardan foydalanish, ularni yaratish, ularga ulanish va ular bilan almashish imkoniyatiga ega bo'lishi hisobiga jamoalar va xalqlarning salohiyatini to'liq ro'yobga chiqarish va ularning turmush darajasini oshirishga imkon beradi. Shu munosabat bilan WiMAX texnologiyasi 2015 yilga borib WSIS ning quyidagi vazifalarini bajarishga chaqirilgan:

- **1-sonli masala:** rivojlanayotgan davlatlarda 1,5 million qishloqlar hatto telefon tarmoqlariga ham ulanmaganligini hisobga olgan holda, qishloq hududlarida AKT xizmatlariga ulanishni ta'minlash;

- **10-sonli masala:** 2002 yilda Internet foydalanuvchilarining umumiy soni 600 millionligini yoki dunyo aholisining 10 foizini tashkil etganligini hisobga olgan holda, dunyo aholisining yarmidan ko'piga AKT xizmatlariga ulanishni ta'minlash.

Ko'rinib turganidek, WiMAX texnologiyasining zimmasiga (boshqa simsiz va tarmoq texnologiyalari bilan bir qatorda) "Raqamli tengsizlik" muammosini yechishda o'ta muhim vazifa yuklangan va bu tizim rivojlangan va rivojlanayotgan davlatlarda AKT xizmatlari va infrotuzilmalariga ommaviy, umumqamrovli, teng huquqli va ishonchli ulanishni ta'minlashga chaqirilgan.

3.1.4. WiMAX tizimining asosiy tavsiflari

Yangi IEEE 802.16 standartlarining yaratilishi va WiMAX ning mobil rejimi paydo bo'lishi tufayli ishlab chiqaruvchilar yagona standartlar qabul qilish va qurilmalarni o'zaro ishlash imkoniyatlariga ko'proq qiziqish bildirib boshladilar. Bu qiziqish, shuningdek, WiMAX tizimi kuchli raqobat afzalligiga ega bo'lishi maqsadida Intel (AQSh) korporatsiyasi tomonidan qo'llab-quvvatlanishi bilan yanada

mahkamlanadi. Xususan, WiMAX texnologiyasi jihozlarni (qurilmalarni) standartlashtirish va ularni o‘zaro ishlash imkoniyatlarini ta’minlaydi hamda tarmoqlar tashkil etishda sarf-harajatlarni sezilarli darajada kamaytirishni ko‘zda tutadi. Misol uchun, Intel va Fujitsu kabi chipset (integral sxema) ishlab chiqaruvchilar ularni ko‘p sonda ishlab chiqarishi va yetkazib berishi mumkin, bu esa, o‘z navbatida, abonentlar qurilmalarining narxini pasayishiga olib keladi.

WiMAX tizimlarining ishchi xarakteristikalariga ko‘plab talablar qo‘yiladi va asosan, maksimal ma’lumot uzatish tezligiga va aloqaning uzoq masofalikligi talab qilinadi. Lekin bunda bu ikki parametrlarning maksimal ko‘rsatkichlarini bir vaqtning o‘zida ta’minlash mumkin emasligini ham yoddan chiqarmaslik kerak. Masalan, zamonaviy WiMAX tizimlarida 70 Mbit/sekunddan yuqori tezliklarga erishish mumkin, lekin buning uchun quyidagi shartlar bajarilishi shart: modulyatsiyalash darajasini qo‘llash uchun aloqa kanalining sifati juda yaxshi bo‘lishi kerak (bu to‘g‘ridan-to‘g‘ri ko‘rinish – LOS, yoki shunga yaqin ko‘rinish - nLOS mavjudligida bo‘lishi mumkin), hamda 10 MGs kenglikdagi kanalda 1024 ta subkanallar mavjud bo‘lishi kerak. Aksincha, aloqa masofasini 50 kmdan ortiqqa ta’minlash mumkin, lekin, u holda ma’lumot uzatish tezligi bor yo‘g‘i 2-3 Mbit/sekundni tashkil etadi. Bunda ham kanalning sifati juda yuqori bo‘lishi kerak, ya’ni ob’ektlar orasida to‘siqlar soni juda kam bo‘lishi, tor yo‘naltirilgan antennalardan foydalanish va nLOS sharoiti mavjud bo‘lishi kerak. IEEE 802.16e standartiga asoslangan mobil WiMAX tizimi kanalning 10 MGs kengligi bilan cheklanib qolish ehtimoli bor (har holda boshlanishiga). Shunda ham u 37 Mbit/s tezlikni ta’minlaydi. 5MGs lik polosalarda esa WiMAX tizimi 18,7 Mbit/s maksimal tezlikni taqdim etishi mumkin va bu sotali aloqaning HSDPA texnologiyasidagi maksimal ko‘rsatkichlarga (5 MGs polosada 14,4 Mbit/s) mos keladi.

WiMAX tizimlarining boshqa muhim xarakteristikalari quyidagilardan iborat:

Tarmoqning moslashuvchan arxitekturasi

WiMAX arxitekturasi “nuqta-nuqta”, “nuqta-ko‘p nuqta”, “mesh” va ushbu rejimlarning turli variatsiyalaridan iborat bo‘lgan bir necha konfiguratsiyalarga ega bo‘lishi mumkin. MAS - muhitga ulanishni boshqarish darajasi ko‘p manzilli (multicast) va keng qamrovli (broadcast) aloqa rejimlarini qo‘llab quvvatlaydi.

Tarmoqni tezkor qurish imkoniyati

Simli aloqa tarmoqlaridan farqli ravishda WiMAX tizimlari tashqi inshootlar qurish, kabel yotqizish va shunga o'xshash ishlarni talab qilmaydi. Foydalanuvchi radiochastotalardan foydalanishga ruxsat olish ehtimoli nisbatan yuqori, chunki WiMAX bir necha unchalik yuklanmagan chastotalar diapazonlarida ishlashga mo'ljallangan. Misol uchun, 2004 yilning dekabrda Indoneziyada sodir bo'lgan sunamidandan keyin butun telekommunikatsiya infratuzilmasi va butun region uchun aloqa xizmatlarini tezkor qayta tiklash talab qilingan. Bunda tirik qolgan insonlarga Internetga ulanishni taqdim etish uchun WiMAX texnologiyasidan foydalanilgan.

Qurilmalarning o'zaro moslashuvchanligi

WiMAX texnologiyasi xalqaro ochiq standart asosida (ya'ni, yagona ishlab chiqaruvchiga bog'liq bo'lmagan holda) qurilgan va bu bilan foydalanuvchilarga o'z AQLarini turli joylarda yoki turli provayderlar tarmoqlarida ishlatishga imkon beradi. Bu, shuningdek, operatorlar uchun ham foydali, chunki, ular turli ishlab chiqaruvchilarning qurilmalaridan foydalanishi mumkin. Va nihoyat, bu ishlab chiqaruvchilar orasida sog'lom raqobatni yaratadi va natijada AQLar narxini pasayishiga olib keladi.

Ko'p darajali servis va QoS - xizmatlar sifati

Taqdim etiladigan xizmatlar turi va sifati asosan aloqa provayderi va foydalanuvchi orasida xizmatlar darajasi bo'yicha tuziladigan kelishuvga bog'liq bo'ladi. Bunda provayder turli abonentlarga yoki hatto bir AQning turli foydalanuvchilariga turli servislar darajasini taqdim etishi mumkin. Barcha servislar xilma-xilligini turli darajalarga bo'lish mumkin va bu darajalar chegaralarida servislar bir biriga yaqin xarakteristikalariga ega bo'ladi, masalan, interaktiv o'yinlar, konferensiyalar o'rnatish imkoniyatiga ega tovushli va videoqo'ng'iroqlar, musiqiy dasturlarni eshitish, videokliplar va filmlarni tomosha qilish, Internetda ishlash, elektron pochtdan foydalanish va boshqalar. WiMAX tizimi trafikning har xil turlarini uzatish uchun tezkor ravishda moslashishi va QoS ning 4 ta sinfini qo'llab-quvvatlashi mumkin.

Keng qamrovli zonalar

WiMAX tizimi radiokanal sharoitlariga qarab turli modulyatsiyalash usullarini (BPSK, QPSK, 16-QAM va 64-QAM) tezkor ravishda moslashtirishi (adaptatsiya qilishi) mumkin. Uzatkich

quvvati kuchaytirgichi va past tezlikli modulyatsiyalash usullari ishlatilganda aloqaning uzoqligini (“nuqta-nuqta” rejimida) 56 kmdan oshirish mumkin (ayniqsa, to‘g‘ri ko‘rinish mavjud bo‘lsa).

To‘g‘ri ko‘rinish bo‘lmagan hollarda aloqa o‘rnatish. To‘g‘ri ko‘rinish bo‘lmagan (ingl. *NLOS*) holat deb ob‘ektlar orasida radioto‘lqinning birinchi Frenel zonasi to‘liq yopiq bo‘lgan holat tushuniladi. Ko‘p nurli uzatish sharoitlarida samarali bo‘lgan OFDM texnologiyasidan foydalanish tufayli WiMAX tizimlari to‘g‘ri ko‘rinish bo‘lmagan hollarda ham yuqori ko‘rsatkichlar bilan ishlashi mumkin. Bu qobiliyat WiMAX tizimlarida hatto to‘g‘ri ko‘rinish bo‘lmagan hollarda ham yuqori tezlikdagi aloqani taqdim etish imkonini beradi. Bu narsaga, masalan, 3G tarmoqlarida erishish ancha murakkab.

Mobillik

IEEE 802.16e standarti WiMAX texnologiyasiga mobillikni qo‘llab-quvvatlash uchun asosiy funksional imkoniyatlarni qo‘shdi. Takomillashtirishlar asosan OFDM va OFDMA texnologiyalarining qo‘shilishi hisobiga fizik darajaga tegishli bo‘ldi. Mobil WiMAX tizimi 160 km/soatgacha tezlikda harakatlanuvchi abonent bilan ishonchli aloqani tashkil etishga imkoniyat yaratadi.

Tarmoqqa sozlanish qulayligi

Zamonaviy sotali aloqa tizimlaridagi kabi WiMAX tizimining abonent qurilmasi tarmoqqa ulanganida mustaqil identifikatsiyalanishga qodir. Ya’ni AQ bazaviy stansiyaga ulanganida aloqa kanalining xarakteristikalarini aniqlashi, tarmoqning ma’lumotlar bazasidan ro‘yxatdan o‘tishi va signalni uzatishga mos parametrlarini o‘rnatish mumkin.

Ishchi chastotalarning keng diapazoni

IEEE 802.16 standartlar oilasida 2,5GGs; 3,5GGs va 5,8GGs chastotalar diapazonidan foydalanish ko‘zda tutilgan.

Kuchaytirilgan aloqa xavfsizligi

WiMAX texnologiyasi AES (ingl-n *Advanced Encryption Standard*) va 3DES (ingl-n *Triple Data Encryption Standard*) shifrlash algoritmlarini qo‘llab-quvvatlashi mumkin. Bazaviy stansiya va abonent qurilmasi orasida kanallarni shifrlash hisobiga WiMAX tizimi abonentlar orasida maxfiylikni (boshqalar eshitishidan himoyani) va operator xizmatlariga ruxsat etilmagan ulanishlarni taqiqlash hisobiga butun tarmoq bo‘yicha xavfsizlikni ta’minlaydi. WiMAX tizimi, shuningdek, ichiga o‘rnatilgan VLAN (ingl. *Virtual*

Local Area Network) funksiyasini qo‘llab-quvvatlash hisobiga bir bazaviy stansiya orqali uzatilayotgan turli foydalanuvchilarning ma’lumotlarini himoyasini ta’minlaydi.

3.1.5. WiMAX tizimlarining tarqalishi va qo‘llanish sohalari

SKPU tarmoqlari hozirgi vaqtda turli ilovalar uchun ishlatiladi. Xususan:

- Simli aloqa infratuzilmasi hali ham mavjud bo‘lmagan joylarda (masalan, rivojlanayotgan davlatlarda yoki viloyatlarning chekka qishloq joylarida) an’anaviy telefoniya va ma’lumotlar uzatish xizmatlarini taqdim etishda “oxirgi mil” masalasini yechish uchun;

- Turli foydalanuvchilar, shu jumladan, 2G va 3G sotali operatorlari uchun “nuqta-nuqta” rejimida T1/E1 kommutatsiya liniyalarini o‘rnatish uchun;

- Internet xizmatlariga simsiz ulanishni taqdim etish uchun;

- Uzoqdagi nuqtalarda (masalan, yirik sport va madaniy tadbirlarni o‘tkazishda) vaqtinchalik aloqa o‘rnatish uchun tarmoqlarning tezkorlik bilan qurish uchun;

- 802.16 standartlarining mobil versiyasini qo‘shilishi bilan WiMAX tizimlari qo‘shimcha xizmatlarni taqdim etish uchun ham ishlatiladi. Xususan:

- VoIP protokoli asosida mobil telefoniya uchun;

- IP-protokoliga asoslangan mobil multimediyali xizmatlar uchun;

- Katta hajmdagi ma’lumotlar almashish uchun “nuqta-ko‘p nuqta” rejimida baza stansiyalar orqali mobil ishlash uchun (“xot zonalar” (Hot Zone) deb nomlanadigan);

WiMAX tarmoqlari dunyoda keng tarqalmoqda. WiMAX-Forumining ma’lumotlariga ko‘ra 2010 yilning fevral oyiga qadar dunyoning 147 mamlakatlarida 559 ta faoliyat ko‘rsatayotgan tarmoqlari hisoblangan, ushbu ko‘rsatkich 2009 yilning fevral oyiga qadar esa 139 ta mamlakatda 468 tani tashkil etgan. Mintaqalar kesimida ushbu tarmoqlar 3.1- jadvalda aks ettirilgan.

Hozircha bozorda qayd etilgan WiMAX tarmoqlari yetakchilik qilmoqda (2010 yilning boshlarida 60%). IEEE 802.16.e standarti ko‘payib bormoqda va dunyoda endi uning asosidagi ko‘p sonli tarmoqlar ishlamoqda. Ular orasida AQShning Sprint-Nextel, Clearwire, AT&T va NextWave Broadband, Yevropada Vodofon va

Orange, deyarli davlatning butun hududini qamrab olgan Pokiston milliy Wateen Telekom operatori, Rossiyada Yota va boshqa operatorlar tarmoqlari ishlamoqda.

3.1- jadval

WiMAX tarmoqlarining hududlararo taqsimlanishi

	Mintaqa	Tarmoqlar soni	Mamlakatlar soni
.	Afrika	114	43
.	Markaziy va Lotin Amerikasi	110	32
.	Osiyo-Tinch okeani	102	22
.	Sharqiy Yevropa	84	21
.	G'arbiy Yevropa	70	17
.	Shimoliy Amerika (AQSh, Kanada)	51	2
.	Yaqin Sharq	28	10

Bugungi kunga kelib Pokiston milliy ko'lamdagi jahonda eng katta to'liq funksional WiMAX tarmoqlaridan biriga ega. Wateen Telekom kompaniyasi tarmog'i Motorola (AQSh) jihozlaridan foydalanilgan davlatning 17 ta shaharlarida qurilgan. WiMAX qurilmalarini yirik ishlab chiqaruvchilarga Airspan Networks, Alkatel-Lucent, Alvarion, Cisco Systems, Fujitsu, Huawei Technologies, Intel Corporation, Motorola Solutions, Samsung va ZTE Corporation kabi kompaniyalarni kiritish mumkin [17].

3.1.6. WiMAX tizimining afzalliklari va kamchiliklari

WiMAX tizimining afzalliklariga quyidagilar kiradi:

- IP-protokoliga optimallashtirilgan yuqori samarador 802.16e radiointerfeysi;

- Mobil tizimlarga yaxshi to'g'ri keladigan OFDMA kanallarni ajratish va taqsimlash takomillashtirilgan texnologiyalar turi (OFDM texnologiyasiga nisbatan);

- Noutbuklarga, telefonlarga va maishiy texnikaga WiMAX adapterlarini qulay o'rnatish imkoniyati;

- Sotali aloqa tarmoqlariga o'xshash yirik tarmoqlarni yaratish uchun yetarli bo'lgan keng chastotalar polosasi;

- MIMO va STC antenna-fider qurilmalari sohasida progressiv ishlanmalarni qo'llab-quvvatlash;

- IP-tarmoqlar uchun standart tarmoq qurilmalaridan foydalanish;

- Foydalanuvchilarning ulkan o'ziga xos xususiyatlarini hisobga olinganida QoS xizmati ko'rsatish sifatini boshqarishning universal vositalari;

- Abonentlarga telefoniya xizmatlari, keng polosali ulanish, mobil aloqa va boshqalarni taklif etish imkoniyatini beradigan multiservisli tarmoq platformalari;

WiMAX tizimlarining kamchiliklariga va rivojlanishini saqlab turuvchi omillarga quyidagilar kiradi:

- standart hali ham sinov bosqichida va xizmatlar provayderlari ishlatayotgan qimmat qurilmalarni yangilariga almashtirishga shoshilmayapti yoki bu qurilmalarni ko'tarish va sarflangan vositalar tezda o'zini oqlash imkoniyatisiz sezilarli sarflarni talab qiladi;

- oldin Internetga ulanish imkoni bo'lmagan joylarda WiMAX tarmoqlarini qurishga zarur qurilmalarni yoki uni sotib olishga mablag' vositalariga ega samarali bo'lmagan potensial foydalanuvchilar soni muammosiga duch kelishga to'g'ri keladi;

- ko'p sonli mutaxassislar to'g'ri ko'rinishdagi O'YuCh kanallardan foydalanish inson salomatligi uchun zararli deb hisoblashadi;

- qayd etilgan WiMAX qurilmalari mobil rejimni qo'llab-quvvatlaydi va tarmoqlarning keyingi WiMAX standartiga o'tkazishda qurilmalarning qismlarini yangilash talab qilinadi;

- va nihoyat, WiBro (quyida yoritiladi) radiochastotalarga yaqin diapazonlariga yaqin foydalanadigan keng polosali aloqaning raqobatli standarti shuningdek, mobil aloqaning raqobatli, xususan LTE texnologiyalarining mavjudligi.

Shunday qilib, WiMAX standartining ko'rinib turgan afzalliklarida texnologiyaning total joriy etilishi yoki hatto unga

ommaviy o‘tish va mavjud tarmoqlardan voz kechish imkoniyati haqida hali gapirish erta. IEEE 802.16e standartining litsenziyalangan tijorat maqsadida ishlatilishi natijalarini olish, keyin esa uning rivojlanish istiqbollari baholash zarur. Lekin, shuni ta’kidlash joizki, 802.16 oilasidagi standartlarni takomillashtirish borasida ishlar davom etmoqda. 2009 yilda IEEE 802.16-2009 nomini olgan standartning yangi versiyasi paydo bo‘ldi, lekin u IEEE 802.16m standartining paydo bo‘lgunigacha bo‘lgan oraliq xarakterga ega bo‘ldi. IEEE 802.16m standarti statsionar abonent qurilmasi bilan 1Gbit/sek. gacha, mobil abonentlar qurilmasi bilan esa 100 Mbit/sekundgacha tezlikda ma’lumotlar uzatishga erishishi kerak. Keyin yangi standartlar qo‘llab-quvvatlaydigan qurilmalarni litsenziyalanishi, qurilmalarni ishlab chiqarish bozoridagi raqobat va WiMAX tizimi orqali ulanish xizmatlarini va boshqalarni kutish mumkin. U holda bu texnologiyalarning muqobillariga taqqoslanganda afzalliklari va kamchiliklari haqida aytish mumkin bo‘ladi [18].

3.1.7. WiMAX va Wi-Fi tizimlarini taqqoslash

WiMAX va Wi-Fi tizimlarining taqqoslanishi yangilik emas, shuning uchun atamalarning nomlanishi o‘xshash, bu texnologiyalarga asoslangan standartlarning nomlanishi ham o‘xshash (IEEE standartlari, har ikkalasi 802 dan boshlanadi) shuningdek ikkala texnologiyalar simsiz keng polosali ulanish turkumiga kiradi. Lekin shunga qaramasdan bu texnologiya turli masalalarni yechishga yo‘naltirilgan (3.2- jadvalga qarang).

WiMAX – bu odatda provayderga oxirgi foydalanuvchiga Internet tarmog‘iga “nuqta-nuqta” turi yordamida ulanishni ta’minlash uchun foydalaniladigan bo‘shliq masofalarni qamrab oladigan uzoq masofali ishlaydigan aloqa tizimidir. 802.16 oilasining turli standartlari, qayd etilgan to mobilgacha turli ulanish rejimlarini ta’minlaydi.

Wi-Fi-bu Internetga chiqish va Internetga chiqmasdan qisqa masofalarda lokal tarmoqni tashkil etish uchun foydalaniladigan tizimdir.

WiMAX va Wi-Fi tizimlari umuman turli QoS xizmat ko‘rsatish mexanizmlariga ega, WiMAX tizimi baza stansiya va abonent qurilmasi orasidagi har bir bog‘lanishga yagona QoS darajasini o‘rnatishga asoslangan mexanizmdan foydalanadi.

Keng polosali simsiz aloqa standartlarini taqqoslash jadvali

Texnologiya	Standart	Sinfi	O‘tkazish qobiliyati	Qamrov hududi	Chastota diapazoni
Wi-Fi	802.11 a	WLAN	54 Mbit/sek.	100 m gacha	5 GGs
Wi-Fi	802.11 b	WLAN	11 Mbit/sek.	100 m gacha	2.4 GGs
Wi-Fi	802.11 g	WLAN	54 Mbit/sek.	100 m gacha	2.4 GGs
WiMAX	802.16 d	WMAN	73 Mbit/sek.	6-10 km	1.5-11 GGs
WiMAX	802.16 c	Mobil WMAN	30 Mbit/sek.	1-5 km	2-6 GGs

WiMAX tizimida har bir bog‘lanish uchun yuqori QoS darajasini kafolatlaydigan maxsus rejalashtirish algoritmiga asoslanadi. Wi-Fi o‘z navbatida har bir paket turli QoS darajasini oladigan Ethernet tarmoqlarida ishlatiladigan QoS mexanizmidan foydalanadi. Shunday qilib, Wi-Fi tizimida har bir bog‘lanish uchun bir xil QoS darajasi kafolatlanmaydi. Nisbatan past narxi va o‘rnatishda soddaligi tufayli Wi-G‘i tizimlari mijozlarga Internetga tez ulanishni taqdim etish uchun ishlatiladi, masalan, ko‘plab kafelarda, mexmonxonalarda, vokzallar va aeroportlarda bepul Wi-G‘i ulanish nuqtalarini uchratish mumkin.

3.2. WiMAX (IEEE 802.16) standartlari

3.2.1. WiMAX standartlarining qisqacha rivojlanish tarixi

IEEE 802.16 standartlarini ishlab chiqish ustidan asosiy ishlar 2001 yilda boshlandi. Shu yilning iyunida 802.16 oilasidagi standartlar asosida jihozlarni ishlab chiqarish bo‘yicha tavsiyalarni ishlab chiqish uchun sohaviy konsorsium WiMAX forumiga asos solindi. 2001 yilning dekabridayoq yangi simsiz keng polosali aloqa tizimi IEEE 802.16-2001 standarti paydo bo‘ldi [18].

Standart shahar “megapolis” (ingl. *Metropolitan Area Network, MAN*) ko‘lamida statsionar simsiz tarmoqlarni tavsifladi, shunday qilib, standartning dastlabki nomi Wireless MAN (WiMAN) bo‘ldi.

Yangi standartning topologiyasi faqat “nuqta-ko‘p nuqta” rejimini taqdim etdi, fizik darajada esa bir eltuvchi chastotadan foydalanish ko‘zda tutildi (ingl. *Single-Carrier, SC*). Shuning uchun protokolning nomlanishiga SC ni qo‘shiladigan bo‘ldi. (Wireless MAN-SC). Ishchi chastotalar sifatida 10GGs dan 66GGs gacha diapazondan foydalanish ko‘zda tutildi. Bunda standart faqat to‘g‘ri ko‘rinish sharoitlarida ishlashi ko‘zda tutildi. Natijada bu, 802.16-2001 standarti qurilmalari keng tarqalishiga olib keldi. Shuningdek, ushlab turuvchi omil yuqori chastotalar diapazonida ishlash uchun yetarli apparatura bazasining ta‘minlanmaganligi hisoblanadi. Bu omillarni hisobga olib 2003 yilning yanvarida yangi 2 GGsdan 11GGsgacha chastota diapazonidan foydalanish ko‘zda tutilgan. IEEE 802.16 standartini IEEE 802.16-2003 kengaytirilgan standarti qabul qilindi. Mazkur standart ham megapolis ko‘lamida statsionar simsiz tarmoqlarni yaratishga yo‘naltirildi. U “so‘nggi mil” kabelli modemlar, xDSL va T1/E1kanallar uchun keng polosali ulanishning alternativ an‘anaviy yechimi bo‘ldi. Bundan tashqari, IEEE 802.16a tarmoqlari 802.16 b/g/a standartlarining ulanish nuqtalarini Internetga ulash uchun qo‘shimcha texnologiya sifatida foydalanish uchun rejalashtirdi. Lekin “16a” standartning zaif joyi bino ichida yomon radio qamrab olish bo‘lib qoldi.

IEEE 802.16a standartining mantiqiy davomi IEEE 802.16d standarti bo‘ldi. U bino ichida qayd etilgan ulanishni ishlatish imkoniyatini ko‘zda tutdi. Tamomila IEEE 802.16.a standarti 2004 yilning iyulida qabul qilindi va IEEE 802.16 -2004 nomini oldi. “D” versiyasining paydo bo‘lishi bilan IEEE 802.16a va IEEE 802.16d standartlarining alohida rivojlantirilishi zaruriyati dolzarb bo‘lmay qoldi, chunki IEEE 802.16d standartining yakuniy versiyasi oldingi standartlarning barcha imkoniyatlarini qamrab oldi. Lekin standartlarni ishlab chiqish bo‘yicha ishlar to‘xtab qolmadi, chunki SKPU tizimlariga mobillikni berish bo‘yicha bosh maqsadga hali erishilmadi. 2005 yilning dekabrda IEEE 802.16e standarti (shuning IEEE 802.16d-2005 nomlanadigan), lekin ko‘proq “mobil WiMAX” sifatida ma‘lum standart qabul qilindi. Shu yilning o‘zida Setekom (Ispaniya) kompaniyasi asosida WiMAX jihozlarini sertifikatlashtirish uchun birinchi laboratoriya ochildi.

Ta‘kidlash kerakki, ETSI Evropa instituti BRAN (ingl. *Broadband Radio Access Networks*) texnik qo‘mitasining parallel ishlanmasi Hiper Man standarti ham 2005 yilda yaratildi [41].

Standart 2GGs -11GGs chastotalar diapazonidan foydalanish bilan Yevropa davlatlarida ishlatish va foydalanuvchilarning qayd etilgan va ko'chma ish rejimlarida umumiy qamrab olish zonasida Internetga simsiz keng polosali ulanishni taqdim etish uchun mo'ljallangan. Shunday qilib, Hiper Man standarti WiMAX tizimlariga (yoki IEEE 802.16 standartlariga), shuningdek, WiBro Koreya ishlanmalariga alternativ hisoblanadi.

Shu bilan birga standart IEEE 802.16 ishchi guruhi bilan uzviy hamkorlikda ishlab chiqildi va shuning uchun Hiper MAN va IEEE 802.16a-2003 standartlari orasida "cheksiz rouming" qo'llab quvvatlanadi, Bunda Hiper MAN va IEEE 802.16 standartlari orasida o'zaro ta'sirlashishni ta'minlash ustida ish olib borilmoqda [15].

2006 yil IEEE 802.16 standarti bazasidagi jihozlarning birinchi namunalarning paydo bo'lishi bilan o'ziga xos bo'ldi va bu bilan qayd etilgan WiMAX ni aktiv (joriy) etilishi boshlandi. Chunki WiMAX ning qayd etilgan va mobil versiyalari o'zaro moslashmaydigan bo'lib qoldi, ya'ni raqobatchilarga aylandi, unda qayd etilgan WiMAX jihozlarini ishlab chiqaruvchilari va operatorlarining strategik vazifasi mobil WiMAX mahsulotlari paydo bo'lguncha SKPU bozorlarini tezroq va kengroq o'zlashtirish bo'lib qoldi. Shu 2006 yilning o'zida Koreyada birinchi WiBro tarmoqlarining ishga tushirilganligini yoddan chiqarmaslik kerak, bu Janubiy Koreya telekommunikatsion va AT industriyasining bosh vakillari Samsung, Korean Telecom kompaniyalarining davlat qatnashuvidagi ko'p yillik aktiv (faol) ishlarining natijasi bo'ldi. 2002 fevralida Janubiy Koreya koordinatori WiBroni rivojlantirish uchun 2.3-2.4GGs diapazonda 100 MGs radiochastota polosasini ajratdi. 2004 yilning oxirida birinchi WiBro fazasi davlat standartlashtirishidan o'tdi va 2005 yilning oxirida XTI WiBro texnologiyasini IEEE 802.16e standarti sifatida tan oldi. Nihoyat, 2006 yilning iyunida ikki Korea Telecom va South Korean Telecom operatorlari WiBro tarmoqlarini tijoriy ishga tushirdi. Shunday qilib, WiBro IEEE 802.16e (mobil WiMAX) standartiga mos keladigan SKPU texnologiyasini tushunish zarur. WiBro tizimi 8,75 MGGs polosali OFDMA radio ulanish texnologiyasidan va TDD vaqtli dupleksni qo'llab-quvvatlashdan foydalanadi.

Abonent qurilmalari bazaviy stansiya bilan 1dan 5kmgacha masofalarda 30-50M bit/sekund ma'lumotlarni uzatish tezliklarida bog'lanishlari mumkin. Binobarin, tarmoq abonentning 120 km/soat

tezliklardagi mobilligini qo‘llab quvvatlaydi. Shu bilan birga, mobil WiMAX ishlab chiqaruvchilari orqada qolmadi. 2007 yilda IEEE 802.16e standarti bazasidagi birinchi qurilmani sertifikatlashtirish muvaffaqiyatli o‘tdi va WiMAX bozorida ikkita raqobat qiladigan lagerlar standartning qayd etilgan va mobil versiyalari tarafdorlari paydo bo‘ldi. Shu munosabat bilan WiMAX standartining bu versiyalarini atroflicha ko‘rib chiqish va ularning xarakteristikalarini taqqoslash maqsadga muvofiq bo‘ladi.

3.2.2. IEEE 802.16 standartlari oilasining tavsifi

Standartlar bo‘yicha IEEE institutining qo‘mitasi simli va simsiz keng polosali aloqa standartlarini ishlab chiqish bilan shug‘ullanadi. Ethernet (802.3) va Wi-Fi kabi tarmoq texnologiyalari sohasidagi standartlarning ishlab chiqaruvchisi hisoblangan 802 qo‘mita WiMAX (802.16) texnologiyasining tavsiflaydigan standartlar to‘plamini chiqardi.

Yuqorida ta’kidlanganidek, WiMAX Forumi ularning o‘zaro moslashuvchanligini ta’minlash maqsadida 802.16 oilasidagi standartlar (WiMAX profillari deyiladigan) asosida jihozlarni ishlab chiqarish bo‘yicha tavsiyalarni ishlab chiqarishdan iborat vazifasini sohaviy konsorsium, ya’ni standartlarni ishlab chiqishda ko‘plab infokommunikatsion jihozlarni ishlab chiqaruvchilar qatnashmoqda. WiMAX forumi hozirgi vaqtda servis provayderlar (50% atrofida) jihozlar va komponentlar ishlab chiqaruvchilari, shuningdek, kontent provayderlardan iborat 500 tadan ortiq a’zolari birlashtiradi [15].

Yuqorida ta’kidlanganidek, hozirgi vaqtda WiMAX nomidagi ikkita simsiz keng polosali aloqa standarti rivojlanmoqda:

- “16d” versiya (standartning rasmiy nomi - IEEE 802.16-2004) faqat qayd etilgan terminallarda ishlash uchun mo‘ljallangan;
- “16e” versiya (standartning rasmiy nomi - IEEE 802.16-2005) ham qayd etilgan, portativ va mobil aloqa uchun mo‘ljallangan va takomillashtirilgan radiointerfeysni qo‘llab-quvvatlaydi.

Umuman olganda bu ikki WiMAX versiyalarining tizimiy jihozlari o‘zaro moslashmaydi, shuningdek, “16d” versiyaning abonent qurilmalari “16e” versiyadagi tarmoqlarda ishlay olmaydi. Bu moslashmaslik va “16d” versiyaga vaqt sarflamasada “16e” versiyani qo‘llab-quvvatlashga qaror qabul qilmoqdalar.

3.2.3. IEEE 802.16 standartining qayd etilgan va mobil versiyalari

Butun WiMAX oilasiga ma'lum xarakteristikalar to'plami xarakterli bo'lsada, uning versiyalari bir-birlaridan sezilarli farq qiladi. Standartni ishlab chiqaruvchilar ham qayd etilgan, ham mobil qo'llanilishi uchun optimal yechimlarni qidirdilar, lekin bir standart doirasida barcha talablarni moslashtirishga erishilmadi.

Shu bilan birga IEEE 802.16d va IEEE 802.16e standartlari umumiy xususiyatlarga ega.

Avvalo bu butun dunyoda ochiq spetsifikatsiyali standartlashtirilgan va yagona IP–platformada qurilgan texnologiyalardir. Har ikkala standart BS katta xizmat ko'rsatish hududini qo'shganda tarmoqning yuqori o'tkazish qobiliyatiga ega. Texnologiyalar talab qiladigan xizmat ko'rsatish sifatini qo'llab-quvvatlash va radiokanal bo'yicha axborotlarni uzatishda javobni qisqa ushlanish vaqti bilan bazaviy stansiyalar va abonent qurilmalari orasidagi to'g'ri ko'rinish bo'lganda (LOS) ham, bo'lmaganida ham (NLOS) shunday oladi. Standartlar yuqori spektral samaradorlikni qo'shganda keng chastotalar diapazonidek foydalanishi mumkin. Qator bazaviy talablar mos kelsada, turli bozor munosabatlariga texnologiyaning yo'naltirilganligi standartning ikkita alohida versiyalarining yaratilishiga olib keldi (to'g'rirog'i, ularni ikki turli standartlar deb hisoblash) mumkin. WiMAX har bir spetsifikatsiyalari o'zining ishchi chastotalar diapazonini, polosasining kengligi nurlanish quvvatini, uzatish va ulanish usullarini signalni modulyatsiyalash va kodlash usullarini, radiochastotalardan qayta foydalanish prinsiplarini va boshqa ko'rsatkichlarni aniqlaydi. Shuning uchun IEEE 802.16e va IEEE 802.16d standartlari versiyalariga asoslangan WiMAX tizimi deyarli moslashmaydi. Bu standartlarni atroflicha ko'rib chiqamiz.

IEEE 802.16-2004 (shuningdek IEEE 802.16d va turg'un WiMAX) standarti

Standartda ortogonal chastotaviy multiplekslash (OFDM) ishlatiladi va to'g'ri ko'rinish bo'lganida yoki bo'lmagan hududlarga qayd etilgan ulanish qo'llab-quvvatlanadi. Foydalanuvchi qurilmalari binolarning ham ichida ham tashqarisida o'rnatish uchun statsionar modemlar, shuningdek noutbuklar uchun RSMSIA–kartalar hisoblanadi. Ko'p davlatlarda bu texnologiyalarga 3,5 GGs yoki 5 GGs chastotalar diapazoni ajratilgan. WiMAX Forumi ma'lumotlariga

ko'ra, qayd etilgan versiyada 175 tani tashkil qiladi [16]. Ko'plab tahlilchilar (analitiklar) uni DSL simli keng polosali ulanish texnologiyasiga raqobat qiladigan texnologiya sifatida ko'rishmoqda.

IEEE 802.16-2005 (shuningdek, IEEE 802.16e va mobil WiMAX) standarti

Mobil foydalanuvchilarni qo'llab-quvvatlash uchun optimallashtirilgan "16e" versiya "xendover" yoki rouming kabi qator maxsus (spetsifik) funksiyalarni qo'llab-quvvatlaydi. OFDMA asosidagi (S -OFDMA) ko'lamlashtirilgan ulanish qo'llaniladi, to'g'ri ko'rinish bo'lganida ham bo'lmaganida ham ishlashi mumkin. Mobile WiMAX tarmoqlari uchun 2,3 GGs; 2,5 GGs; va 3,4 - 3,8 GGs chastotalar diapazonlari rejalashtirilgan. Dunyoda IEEE 802.16e standarti asosidagi bir necha loyihalar, shu jumladan, milliy ko'lamdagi o'nga yaqin tarmoqlar ishlamoqda 802.16e ning raqobatchilari barcha uchinchi va to'rtinchi avlod mobil texnologiyalari (masalan, EV-DO, HSPA va LTE) hisoblanadi [10].

IEEE 802.16-2004 va IEEE 802.16.2005 standartlarini taqqoslash

WiMAX standartlarining paydo bo'lishi yuqori ishlatilishi xarakteristikalari va maqbul narxli simsiz keng polosali tarmoqlarni ishlatilishi imkoniyatlarini ko'rib chiqadigan operatorlar tomonidan katta qiziqish uyg'otdi. Biroq, ikkita o'zaro moslashmaydigan WiMAX standartlarining (IEEE 802.16e va IEEE 802.16d) mavjudligi bu tekisliklarda investitsiyalar haqida yechimlarni qabul qilishda jarayonlarni murakkablashtirdi. Ma'lumki, IEEE 802.16d standarti "qayd etilgan", IEEE 802.16de standarti "mobil" deyiladi. O'z yo'lida IEEE 802.16e standarti ham qayd etilgan, ham portativ, ham mobil abonentlarga to'liq xizmatlar spektrini taqdim etishga imkoniyat beradi. Biz yuqorida ko'rdikki, IEEE 802.16d standarti qo'llab-quvvatlanadigan birinchi mahsulotlar 2006 yilda IEEE 802.16e standarti qo'llab-quvvatlanadigan birinchi mahsulotlar 2007 yilning boshida bozorda paydo bo'ldi. Shunday qilib, bu mahsulotlarning chiqishi orasidagi vaqt oralig'i umuman kam bo'ldi va avvalroq paydo bo'lgan mos mahsulotlariga bog'liq IEEE 802.16d standartining afzalliklari minimumga keldi. Natijada vositalarni investitsiyalashda qarorlarda qabul qiladigan operatorlar jiddiy tanlash qarshisida bo'lib qoldi va bu standartlarning har birining sifatini tortib ko'rishi va ko'p muddatli istiqbolda ularning roliga e'tibor qaratishi kerak bo'ldi. Qayd etilgan va mobil WiMAX orasida qanday farq bor?

Ko‘rinib turibdiki, ikkala texnologiyalardagi asosiy farq shundan iboratki, qayd etilgan WiMAX faqat statik abonentlarga emas, balki 120 km/soat tezliklarda harakatlanadigan mobil foydalanuvchilarga xizmat ko‘rsatish imkoniyatiga yo‘naltirilgan. Bunda mobil roaming va "xendover" funksiyalarining mavjudligini, ya'ni abonent harakatlanganda bazaviy stansiyalar orasida cheksiz qayta ulanishni (sotali aloqa tizimlarida amalga oshadigandek) bildiradi. Ko‘rinib turibdiki, mobil WiMAX qayd etilgan foydalanuvchilarga xizmat ko‘rsatish uchun ham qo‘llanilishi mumkin.

Ikkinchi farq, shundaki IEEE 802.16e standarti IEEE 802.16d standarti bilan moslashuvchanlikka ega emas. IEEE 802.16d standarti jihozlarni bir necha ishlab chiqaruvchilari IEEE 802.16e ga o‘tishga imkon beradigan qo‘shimcha apparat yoki dasturiy vositalar bilan jihozlangan bazaviy stansiyalarni taklif etsada, bunday o‘tish ishlatilayotgan IEEE 802.16d standarti abonent terminallariga hech qanday ta'sir etmaydi. Bazaviy stansiyalarning jihozlarni modernizatsiyalash imkoniyatlarini ta'minlash ham sezilarli qo‘shimcha harakatlarga olib kelishi mumkin. Kutilmoqdaki, ko‘plab ko‘rilgan IEEE 802.16d standarti tizimlarida FDD kanallarni chastotaviy ajratish ishlatiladi. IEEE 802.16e standartining istiqbolli profillari uchun TDD kanallarni vaqtli ajratishning qo‘llanilishi kutilmoqda. Bu kanalga bir standartdan boshqasiga o‘tish turini murakkablashtiradi, chunki TDD va FDD ning bir chastota diapazonida bir vaqtda ishlatilishi halaqitlarning paydo bo‘lishiga olib kelishi mumkin. Bundan tashqari IEEE 802.16d standartidagi apparaturani ishlatadigan va qandaydir vaqtdan keyin IEEE 802.16e jihozlarni o‘rnatishga harakat qiladigan operatorga ikki standartlar tizimlari orasidagi mavjud chastotasini bo‘lishga yoki chastotalarga yangi litsenziyalar olishga to‘g‘ri keladi.

Standartlar orasidagi sezilarli farq radiointerfeyslarini ishlatilishida ham bor. "16d" versiyada dastlab ham 256 elementlardan iborat Fure tezkor o‘zgartirishli OFDM multiplekslash (256 FFT), ham 2048 nimeltuvchili (ya'ni 2048 ta FFT elementli OFDMA radio ulanish texnologiyasi qo‘llab-quvvatlandi. Natijada IEEE 802.16d standartining fizik darajasi profilida WiMAX Forumi 2048 FTTli OFDMA dan emas 256 FTTli OFDM dan foydalanishga qaror qildi. IEEE 802.16e standartini ishlab chiqishda S-OFDMA (ingl. *Scalable -OFDMA*) usulini qo‘llab-quvvatlash ko‘rinishida fizik darajada takomillashtirish kiritish qabul qilingan. IEEE 802.16e

standarti doirasida qo'llanilgan OFDMA texnologiyasining afzalliklaridan biri shundaki, kanalning kengligi o'zgaruvchan hisoblanadi, lekin kanalning kengligi va OFDM simvollarini diskretlashtirish chastotasi orasidagi o'zgarish munosabat mavjud. FTT massivlarining bir necha 128, 512, 1024 va 2048 o'lchamlari ko'zda tutilgan va bu turli qiymatlardagi kengliklardagi (5, 7, 8,75; 10 MGs) radiokanallarni ishlatishga imkon beradi. Bundan tashqari IEEE 802.16e standartidagi OFDMA texnologiyasi uning aloqasining uzoqligi va tarmoqning sig'imi bo'yicha u va bu talablarga mosligini ta'minlash maqsadida tarmoqning ishchi xarakteristikalarini optimallashtirish uchun subkanallarni bir necha tashkil etish usullarini ishlatishga imkoniyat beradi. Fizik darajada OFDM-simvollar va nimeltuvchilar chastotaviy rejalashtirish yordamida alohida mantiqiy va fizik subkanallarga ajratiladi.

Chastotaviy rejalashtirish chastotaviy –ajratishli yoki chastotaviy–tanlovchanlik asoslarida amalga oshirilishi mumkin. Chastotaviy–ajratishli usul har bir subkanalga mo'ljallangan nimeltuvchilar psevdotasodifiy holda mavjud subkanallar orasida taqsimlanadigan holdagi sxemani ko'zda tutadi. Bu usuldan foydalanish turli aloqa sharoitlarida kanal resursini optimal ishlatishga imkon beradigan chastotalar xilma–xilligini shuningdek, BSning ta'sir etishi ishlash hududini kengaytirishni va tarmoqning sig'imini oshirishni ta'minlaydi. Chastotaviy tanlovchanlikli chastotaviy rejalashtirish usuli AMS adaptiv modulyatsiya va kodlash rejimida qo'llab- quvvatlanadi va bevosita bir–birlari bilan yaqin joylashgan nimeltuvchilarning qo'llanilishi orqali subkanallarni tashkil etishga imkon beradi. Bu usul tarmoqning sig'imini 30% gacha oshirishiga olib kelishi mumkin. Usulning teskari tomoni xizmat axborotlari hajmining ortishi hisoblanadi.

OFDM texnologiyasi (IEEE 802.16d standartlarida foydalanilgan) abonentlar orasida kanal resurslarining taqsimlanishi qismida kam erkinlikka ega, chunki unda taqsimlash faqat bir abonentga bir simvolga amalga oshirilishi mumkin.

OFDMA texnologiyasi esa katta erkinlikka ega va resurslarni bir necha abonentlari orasida bir simvolga taqsimlashga imkoniyat beradi. Shunday qilib, kanalni kengaytirish imkoniyati va subkanallarini turli tashkil etish usullaridan foydalanish IEEE 802.16e standartidagi OFDMA fizik interfeysga IEEE 802.16d standartidagi OFDM ga qaraganda sezilarli afzalliklarni beradi.

Har ikkala standartlarda radiointerfeyslarni tashkil etishga turli talablar aniqlangan bo'lsada, IEEE 802.16e standartda bu talablar qo'shimcha kengaytirildi va ishlab chiqaruvchilarga tarmoqning sig'imini, aloqaning uzoqligini, terminallarning energiya iste'molini va xizmat ko'rsatish sifatini keyingi yaxshilash, shuningdek, IP-protokol asosida ishlaydigan multimediyali va boshqa hujumlarni qo'llash imkoniyati taqdim etildi. IEEE 802.16d va IEEE 802.16e standartlari aloqaning ishonchliligini oshirishga chaqirilgan turli FEC xatoliklarni to'g'ri korreksiyalash algoritmlarini qo'llaydi. Oddiy o'ramli kodlardan va ARQ mexanizmidan foydalanish majburiy qo'shimcha vositalar sifatida esa o'rama turbokod va HARQ ixcham teskari aloqa kabi samarador yo'llar qo'llanilishi mumkin hisoblanadi. Biroq, bu xatoliklarni to'g'rilashning yuqori samarador vositalaridan IEEE 802.16d standarti birinchi avlodi qurilmalarida foydalanish ehtimolligi kam. IEEE 802.16e standartida birinchi mahsulotlardayoq LDPC (ingl. *Low Density Parity Check*) kamchilik sirtlilikka tekshirish va STS kabi takomillashgan kodlash usullar qo'llanilmoqda.

Tarmoqning ta'sir etish (ishlash) hududini oshirishga chaqirilgan qo'shimcha yechimlar ham IEEE 802.16d standartida, ham IEEE 802.16d standartida ko'zda tutilgan. Ular antennalarni fazoviy ajratish (STS) qo'llaniladigan MIMO texnologiyalari yordamida ishlatiladi. Bu mexanizmlar IEEE 802.16e standartida keyingi rivojlanish oldi, bu yerda antennalarni ajratish usuliga va adaptiv antennalarni ishlatishga katta e'tibor qaratildi. BS uzatkichlarida ko'p antennali konfiguratsiyalarni qo'llash, shu jumladan, takomillashtirilgan antenna nimitzimi rejimi AAS, teskari aloqasiz fazoviy-vaqtli kodlash rejimlari (2-4 uzatuvchi antennalar uchun va teskari aloqali MIMO rejimlari) ishlatilgan.

IEEE 802.16e standartida elektr energiyasini tejashni va AQni avtonom uzoqroq ishlash vaqtini ta'minlaydigan energiya istemolini boshqarishning qator funksiyalari ("uyqu" va "kutish" rejimlari) tavsiflanadi. AQning mobillik qismiga IEEE 802.16e standartiga kiritilgan yangi qo'shimchalar hatto yuqori tezliklarda harakatlanganda ham jihoz ishlashi sifatini keyingi oshirilishiga olib keladi. Bunga yaxshilangan "xendover" protsedurasi, qo'shni sotalar signallari parametrlarini nazorat qilish, shuningdek "uxlash" rejimida mobillikni qo'llab-quvvatlash hisobiga erishiladi, bu abonent qurilmasining energiya iste'molining kamayishini ta'minlaydi.

IEEE 802.16e standartida real vaqtda kanalni ilg'or taqdim etilishining takomillashtirilgan algoritmi (ingl. *Extended Real Time Polling Service, ERTPS*) kiritilmoqda. Bu algoritmdan foydalanish aniqlikning ushlanishi va uning notekisligi (djitter) ko'rsatkichlarini yaxshilash imkoniyatini beradi. Shu sababli IEEE 802.16e standarti tizimi trafikni uzatish tizimini va boshqa uning parametrlarini samarali boshqarishga qodir. QoS ta'minlash vositalaridan foydalanish, ayniqsa, IP protokoli bo'yicha (VoIP) nutq uzatilgan holda muhimdir [18].

Shuningdek, IEEE 802.16e standarti guruhli (ko'p manzilli) va keng uzatishli uzatish imkoniyatini ko'zda tutadi. OFDMA dan foydalanish hatto sotalar chegaralarida ham ma'lumotlarini yuqori uzatish tezligida guruhli va keng uzatishli uzatish imkoniyati multimediya tizimlariga (videoni paketli uzatish qo'llaniladigan, masalan IP-TV, IP-protokoli bo'yicha katta trafik hajmi bilan xarakterlanadigan) o'tkazish polosasidan foydalanishni va kontentning yetkazilishini sezilarli optimallashtirishga imkon beradi.

Va nihoyat, u yoki bu standartning mahsulotlari narxlarining o'zgarishlariga taxminlarda farqlar mavjud. SKPU tizimlari bozori o'sishda davom etmoqda va shuning uchun ularning narxi ommaviy joriy etilishi va ishlab chiqarish ko'lamlari hisobiga iqtisod qilish natijasida kelajakda kamayishi kerak. AKT induksiyasidagi tajribalarning ko'rsatishicha, portativ va mobil qurilmalarning tarqalishi ko'pincha ham abonent, ham infratuzilma jihozlari ishlab chiqarish hajmlarini tez o'sishiga olib keladi. Shuning uchun IEEE 802.16e standarti mobil qurilmalarining rivojlanishi IEEE 802.16d standartidagiga qaraganda arzon bo'lishiga imkon beradi. Shu bilan birga yirik chipsetlar ishlab chiqaruvchilari (Intel, FUJITSU kabi) rasman bildirishdiki, IEEE 802.16e standarti WiMAX tizimlarining asosiy standarti bo'lib qoladi. Lekin agar qayd etilgan WiMAX ham afzalliklari keltirilmasa taqqoslash to'liq bo'lmaydi. Bu avvalo foydalaniladigan signalni modulyatsiyalash va kodlash turlari hisobiga yuqori o'tkazish qobiliyati hisoblanadi.

Bu o'tkazish polosasiga qat'iy talablarni qo'yadigan va qayd etilgan modemni o'rnatish imkoniyatiga ega bo'lgan korporativ foydalanuvchilar uchun muhim. Qayd etilgan WiMAX uchun standartning avvalroq paydo bo'lishi hisobiga tayyor jihozlarni yetkazib beruvchilarning katta tanlash mavjud va bu jihozlar endi

o‘zaro moslashishga testlangan va WiMAX Forumi sertifikatlari bilan tasdiqlangan.

IEEE 802.16d va IEEE 802.16e standartlarini ko‘rib chiqishni yakunlash bilan 3.3–jadvalga kiritilgan bu standartlarning xarakteristikalarini umumlashtirilgan taqqoslashni shuningdek 3.4–jadvalda bu standartlar taqdim etiladigan xizmatlar klassifikatsiyasini keltiramiz.

3.3– jadval

IEEE 802.16d va IEEE 802.16e standartlarini taqqoslash

	IEEE 802.16 -2004(d)	802.16e
Ko‘plab ulanish usuli	OFDM/OFDMA	S-OFDMA
O‘tkazish polosasining kengligi (MGs)	1,75/3/3,5/5,5/7 (OFDM) 1,25/3,5/7/14/28 (OFDMA)	1,25/2,5/5/10/20 1,75/3/3,5/5,5/7
FFT massivning o‘lchami	256 (OFDM) /2048 (OFDMA)	128; 256; 512; 1024; 2048
Nimeltuvchilar orasidagi surilish (kGs)	22,5 (OFDM 5MGs) 2,8 (OFDMA 5MGs)	Istalgan o‘tkazish oraliq‘i kengligi uchun 11.2
Dupleksirlash usuli	FDD/TDD/FDD2 yarim dupleks	FDD/TDD/FDD yarim dupleks
Kadrning uzunligi (ms)	2,5; 4; 5; 8; 10; 12,5; 20	2; 2,5; 4; 5; 8; 10; 12,5; 20
Kanal koderi	Sistematik kaskadli o‘rama rekursiv kod (RSCCC), Block TS, STSZ	Sistematik kaskadli o‘rama rekursiv kod (RSCCC), Block TS, STS, LDPC
Nimkanallar («pastga»)	FUSC/PUSC/Band AMS	FUSC/PUSC/Band AMS
Nimkanallar («yuqoriga»)	PUSC/Optional PUSC	PUSC/Optional PUSC
HARQ ni qo‘llab – quvvatlash	Bor (faqat 2048 OFDMA)	bor
SQI tezkor	Bor (faqat 2048)	bor

aks aloqa	OFDMA)	
AAS	bor	bor
STC ni qo‘llab – quvvatlash	bor	bor
Chastotalarni ko‘p marta ishlatilishi	2/4 antennalar	2/3/4 antennalar
Mobillik/ aloqa seansini uzatish	1 sota doirasida ishlatilmaydi	1 sota doirasida ishlatish mumkin
“Uyqu ” rejimi	yo‘q	bor
Zondlash kanali	yo‘q	bor
Guruhli / keng qamrovli uzatish	yo‘q	bor

3.4 – jadval

Mavjud va paydo bo‘ladigan servislarning misoliy klassifikatsiyasi

Uzatiladigan ma‘lumotlar turi	Xizmatlar toifasi	Qayd etilgan WiMAX	Mobil WiMAX
Axborotlar	Internet –ulanish, e –mail	++	++
	VPN	++	++
	Ma‘lumotlar bazasiga portallarga ulanish	+	++
	Ma‘lumotlarni to‘plash	+	++
	Telemetriya	++	+
	Aktivlar ustidan nazorat	-	+
Tovush	VoIP	++	++
	PTT (guruhli chaqirish)	-	++

	FMC	-	++
Video	Radiochaqiruv Videokonferensiya	+	++
	Videokuzatuv	++	+
Joylashgan o‘rin	Axborot xizmatlari	-	++
	Xodimlar va texnikani boshqaruv	-	+
	Chaqiruvlarni adaptiv marshrutlashtirish	-	++

++ xizmatlar yaxshi qo‘llanilgan; + xizmatlar o‘rtacha qo‘llanilgan;
- qo‘llanilmagan.

3.3. WIMAX tizimining arxitekturasi

3.3.1. WIMAX tizimi arxitekturasi asosiy prinsiplari

WIMAX tizimining arxitekturasi nisbatan IEEE instituti PHY fizik va MAC darajalardagi asosiy talablarni aniqladi. O‘z vaqtida bunday yondashuv Ethernet va WI-FI texnologiyalarga qo‘llanishda o‘z samaradorligini ko‘rsatdi. Ularda TCP/IP, SIP, VoIP va IP-SEC turdagi yuqori darajalardagi protokollar va boshqa sohaviy tuzilmalar, bu holda IETF (ingl. *Internet Engineering Task Force* – Internet tarmog‘ini loyihalashtirish bo‘yicha maqsadli guruh) guruhi tomonidan qabul qilingan. Lekin, PHY va MAC darajalarda radiointerfeysga umumiy talablar ishlanmasidan tashqari, xalqaro darajada moslashtirish zarur bo‘lgan masofalar to‘plami mavjud. Xususan, turli xil bir jinsli, ham “turli jinsli”(ya’ni boshqa texnologiyalarga kiradigan) tarmoqlar bilan WIMAX tizimlarining o‘zaro ta’sirlashishini ta’minlash bo‘yicha talablarni aniqlash zarur. Misol uchun mobil aloqalar uchun bu masalalar bilan 3GPP va 3GPP-2 dasturlari shug‘ullanadi. Ular interfeyslar va protokollar keng to‘plam bo‘yicha standartlarni o‘rnatadi. Chunki bu faqat umumiy radiointerfeys bo‘yicha o‘zaro ta’sirlashish uchun emas, balki turli ishlab chiqaruvchilar jihozlarida qurilgan turli tarmoqlar orasida

o‘zaro ta’sirlashish va rouming uchun zarur bo‘ladi. Shunga o‘xshash IEEE 802.16 oilasidagi standartlar uchun protokollar va interfeyslarni ishlab chiqish bilan WIMAX forumi shug‘ullanadi. Xususan, forum doirasida ikki ishchi guruh tashkil etildi. Statsionar, ko‘chma, portativ va mobil ish rejimlari uchun yuqori darajalar spetsifikatsiyalarini tayyorlash maxsuslashtirilgan tarmoqlarni tashkil etish bo‘yicha guruh (ingl. *Network Working Group*) tarmoqqa ulanishni taqdim etish bo‘yicha talablarni aniqlagan va ularni ishlatishga tarmoqlarni tashkil etish bo‘yicha guruhga yordam bergan xizmatlarni tashkil etish bo‘yicha guruh (ingl. *Service Network Working Group*) tashkil etildi. Bu guruhlar o‘z ishida quyidagi asosiy tarmoqlarni qurish prinsiplariga asoslandi [8]:

1. WIMAX tizimi arxitekturasi bevosita IEEE 802.16 standarti, shuningdek, IETF va Ethernet standartlari aniqlagan kommutatsiya protsedurasi qo‘shilganda paketni kommutatsiya asosida qurilishi kerak.

2. Arxitektura kommutatsiya darajasidan ulanish darajasini ajratish kerak. Ya’ni, tarmoqning kommutatsiya darajasi elementlari IEEE standartlarining qo‘llanilgan radioulanish texnologiyalariga bog‘liq bo‘lmasligi kerak.

3. Tizimning arxitekturasi tarmoqlarni qurish va kengaytirishning turli variantlarini qo‘llab-quvvatlash uchun modulli va ixcham bo‘lishi kerak. Xususan, ularga quyidagilar kiradi:

- Kichik o‘lchamlardagi tarmoqlardan katta o‘lchamli tarmoqlarga o‘tish;

- Shahar, shahar atrofi va qishloq sharoitlaridagi radioto‘lqinlarni tarqalishida ishlash;

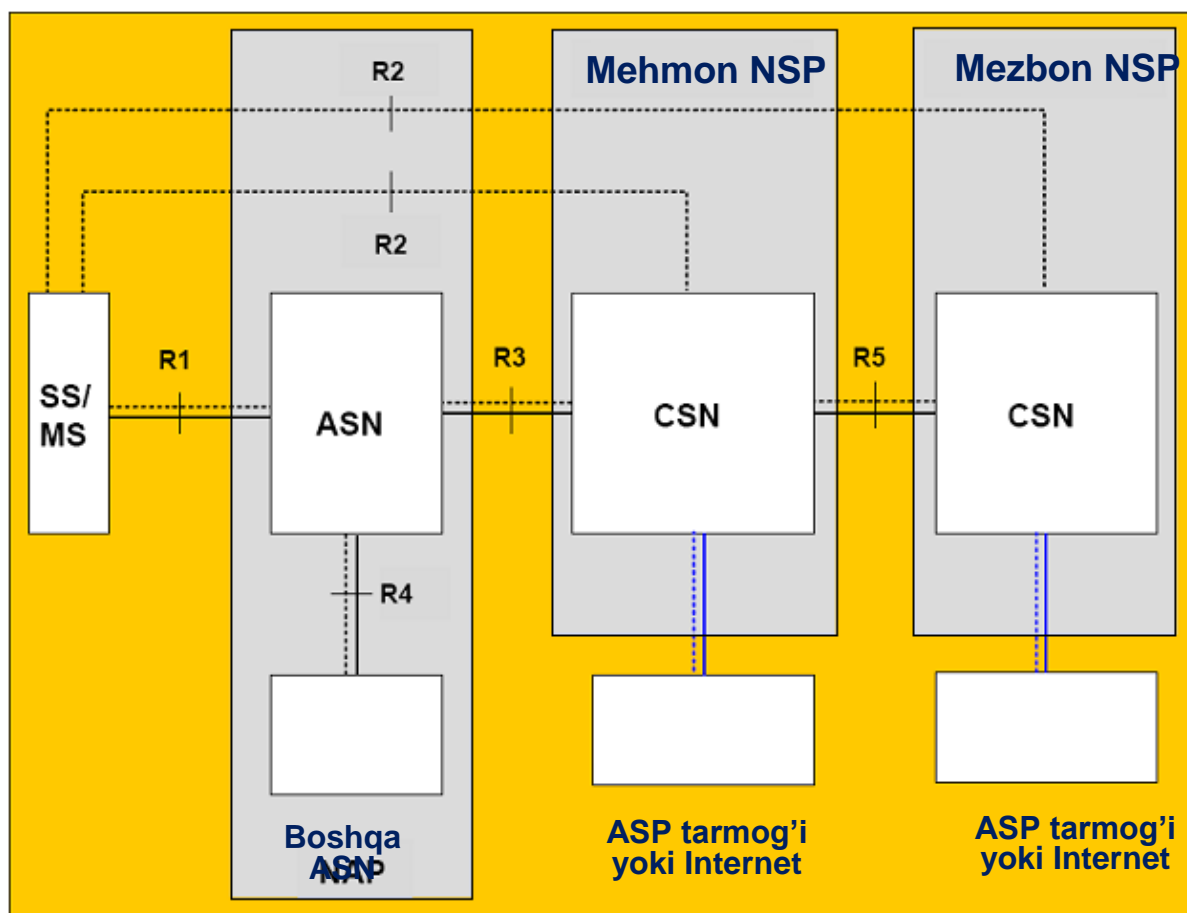
- Litsenziyalangan hamda litsenziyalanmagan ishchi chastotalardan foydalanish;

- Ierarxik, bir darajali va o‘zi shakllanadigan tarmoqlar topologiyalari va ularning kombinatsiyalari;

- Qayd etilgan ko‘chma, portativ va mobil terminallarda birgalikda ishlash.

WIMAX Forumi qatnashchilari tizim arxitekturasiining mantiqiy taqdim etilishi hisoblangan NRM (ingl. *Network Reference Model*) WIMAX tarmog‘ining tayanch modelini aniqladi [10]. NRM modeli funksional tizimlar orasida o‘zaro ta’sirlashishi amalga oshiriladigan va tayanch nuqtalar (ingl. *Reference Points*) deyiladigan tarmoqning

funksional tugunlarini tavsiflaydi. WIMAX tarmog'ining tayanch modeli umumiy ko'rinishda 3.3-rasmda keltirilgan.



3.3- rasm. WIMAX tarmog'ining tayanch modeli (NRM)

Tizimning bunday arxitekturasi turli tarmoqlarni qurish modullarini va terminallarning ish rejimlarini qoniqtiradigan funkcionallikni ta'minlash maqsadida taklif etilgan. WIMAX Forumi WIMAX tarmoqlar ishlashining ko'plab aspektlarini aniqlaydigan arxitekturani ishlab chiqdi:

- Boshqa tarmoqlar bilan o'zaro ta'sirlashish;
- Tarmoq manzillarini taqsimlash;
- Mobillikni boshqarish;
- Autentifikatsiya va ko'plab boshqalar.

WIMAX tarmog'i arxitekturasi bosh o'ziga xos xususiyati shundan iboratki, u qandaydir ma'lum konfiguratsiya bog'lanmagan va yuqori ko'lamlikka va ixchamlikka ega. Masalan, WIMAX tarmog'i turli funkcionallik imkoniyati AQ larni va mikrosotalarni va makrosotalardan boshlangan hamda pikosotalar va femsotalarda

tugagan o‘zgaruvchan qamrash hududli BS larni qo‘llab-quvvatlashi mumkin.

WIMAX Forumi R1-R5 (asosiy) va R6-R8 (yordamchi) belgilanishlarni olgan tayanch nuqtalari bo‘lgan bir necha tugunlararo ulanishlar bilan birga tarmoqning tugunlar tarkibini aniqladi.

3.3- rasmdan ko‘rinib turibdiki, WIMAX tarmog‘ining asosiy tugunlari quyidagilar hisoblanadi:

- SS/MS (ingl. *Subscriber Station/Mobile Station*) – abonent qurilmasi/mobil stansiya;

- ASN (ingl. *Access Service Network*)-ulanishni taqdim etish;

- BS (ingl. *Base Station*)-bazaviy stansiya (ya’ni “ulanish nuqtasi nomiga ega”), ASN tuzilmasiga kiradi;

- ASN-GW (ingl. *ASN Gateway*)- ASN shlyuzi, u ham ASN tuzilmasiga kiradi;

- CSN (ingl. *Connectivity Service Network*)-kommutatsiya tarmog‘i;

- HA (ingl. *Home Agent*)-uy agenti, CSN tuzilmasiga kiradi;

- AAA Server (ingl. *Authentication, Authorization and Accounting Server*)-Autentifikatsiyalashtirish, mualliflashtirish va qayd etish serveri, u ham GSN tarkibiga kiradi;

- NAP (ingl. *Network Access Provider*)-tarmoqqa ulanish provayderi;

- NSR (ingl. *Network Service Provider*)- tarmoq xizmatlari provayderi.

Tarmoq tugunlariga bo‘lish mantiqiy darajada va har bir mantiqiy tugunlarda amalga oshirilgan. MS, ASN va CSN guruhli funkcionallikdan iborat bo‘lishi mumkin. Bunda tarmoq funksiyalari funksiyalar bo‘lingan ham bir, ham bir necha apparatlarida ishlatilishi mumkin. Uskunada funksiyalarni bo‘lish yoki birlashtirish tizimni integratsiya modeli bilan aniqlanadigan yoki tizimning xarakteristikalariga qo‘yiladigan talablarni tanlash hisoblanadi. Tizim ichida o‘zaro ta’sirlashish tarmoqning funkcionallik tugunlari orasidagi o‘zaro ta’sirlashish protokollarini aniqlashda quriladi.

3.3.2. WIMAX tarmog‘i tugunlarining funkcionalligi

Abonent qurilmalari

Abonent qurilmalari WIMAX tarmog‘iga va tashqi IP-tarmoqlarga bazaviy stansiyalarga radiokanal bo‘yicha ulanish orqali

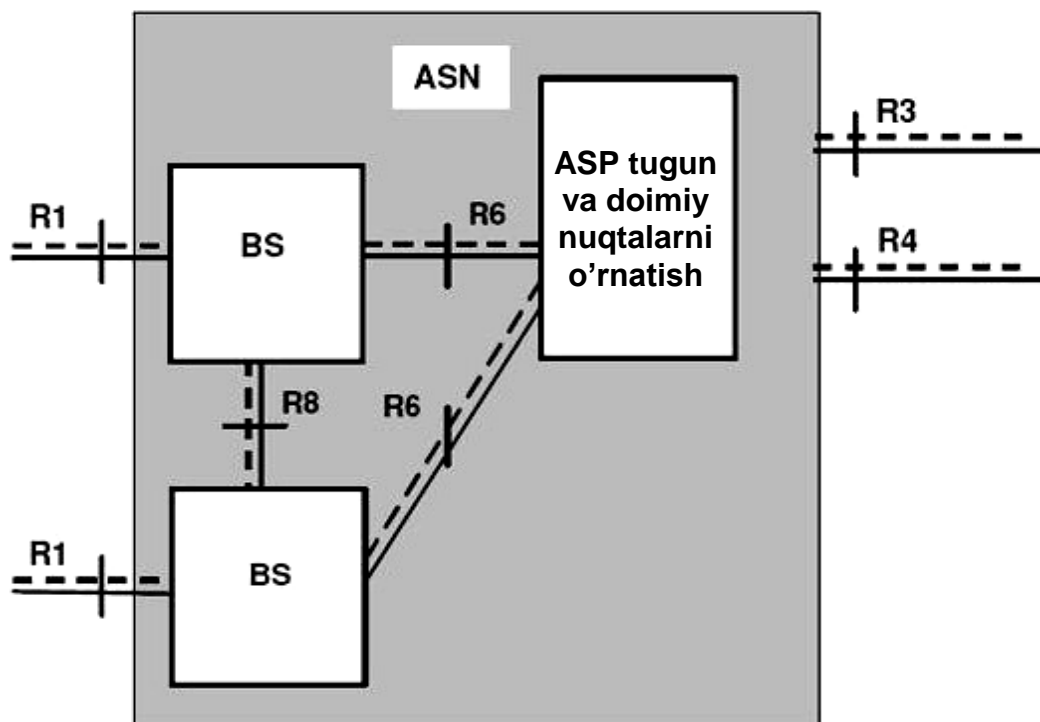
ulana oladi. Ular statsionar, ko'chma va mobil rejimlarda ishlatilishi mumkin va mos ravishda ham bino ichida, ham bino tashqarisida ishlatish uchun mo'ljallangan. Bino ichida foydalanishga mo'ljallangan AQLar tashqi qurilmalarga qaraganda BS dan sezilarli kichik masofalarda ishlashga qodir va shuning uchun tarmoq infratuzilmasida ko'p sonli BSlardan foydalanishni ko'zda tutadi. Mobil WIMAX paydo bo'lishi bilan yo'nalish (urg'u) mobil smartfonlar, USB-modullar va PC-kartalar ko'rinishida mobil AQLarni ishlab chiqarishga qaratiladi.

ASN ruxsat olishni taqdim etish tarmog'i

ASN tuguni kommutatsiya darajasi va ulanishni taqdim etish darajasini mantiqiy chegarasini aniqlaydi va ulanishni taqdim etishga javob beradigan funksional tugunlar orasida o'zaro ta'sirlashish va xabarlarni almashtirishning qulay usulini taklif qiladi. ASN bir yoki bir necha mijozlar bilan bir yoki bir necha BS lardan iborat. ASN mijozlar CSN kommutatsiya tarmog'i bilan u orqali boshqa transport IP-tarmoqlar bilan aloqani ta'minlaydi. Faktik bu tugun IEEE 802.16 radio ulanish tarmog'ini tashqi IP-tarmoqlar bilan bog'laydi. NRM modelida o'rnatilishlarga muvofiq ASN tarmoqlari chegaralarida funksional va mantiqiy kommutatsiya turli usullarda amalga oshirilishi mumkin. Xususan ASN - shlyuz bir necha BS lar ishini boshqarishi mumkin, lekin har bir BS ham bir emas, bir necha ASN-shlyuzlarga bog'langan bo'lishi mumkin.

Bundan tashqari, BS ham, ASN-shlyuzlar ham to'g'ridan-to'g'ri bir-birlariga bog'langan bo'lishi mumkin. WIMAX Forumi ishlab chiqaruvchilar jihozlarning xilma-xilligini qo'llab-quvvatlash va ularni o'zaro ta'sirlashish imkoniyatlarini hisobga olganda tarmoqning spetsifikatsiyasini aniqlaydi. ASN tuzilmasi 3.4-rasmda keltirilgan.

ASN tuguni AQLari bilan ulanish uchun R1 tayanch nuqtasidan, CSN tugun bilan ulanish uchun R3 tayanch nuqtasidan, boshqa ASN tugunlar bilan ulanish uchun R4 tayanch nuqtasidan foydalanadi. Bevosita ASN tuguni BS lar va ularga ulangan ASN-shlyuzlardan iborat (3.5-rasm).



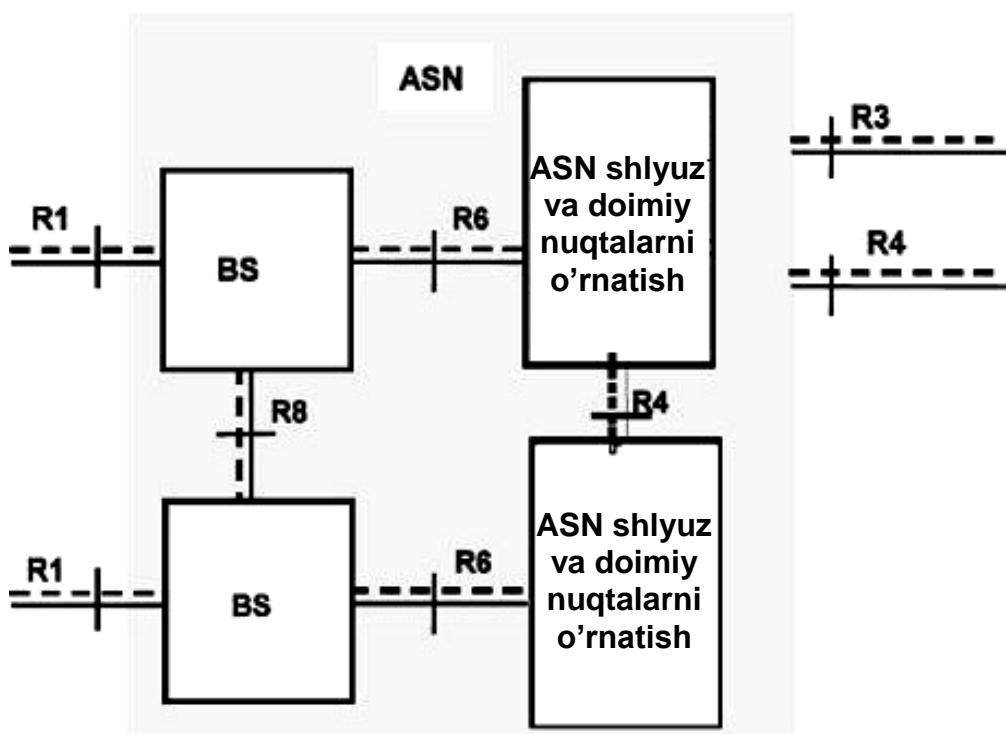
3.4- rasm. ASN tuzilmasi

ASN tuguni elementlarining o‘zaro ta’sirlashishi R6, R7, va R8 maxsus interfeyslarini tayanch nuqtalarini sifatida ishlatishi hisobiga amalga oshiriladi. Agar ASN tuguni bir necha ASN – shlyuzlarni ishlatgan holda, unda boshqarish signallarini almashtirish R4 tayanch nuqtasidan orqali amalga oshiriladi.

BS IEEE spetsifikatsiyalarida aniqlangan parametrlar bo‘yicha mos hisoblanadigan abonent qurilmalariga Internetga simsiz ruxsat etishni ta’minlaydi. BS AQ va Internet tarmog‘i orasida IP-trafikni WIMAX standarti radiointerfeysli orqali marshrutlashtiradi.

Bazaviy ctansiya tavsifi

WIMAX Bazaviy Stansiyasi (ba’zan “ulanish nuqtasi” sifatida belgilanadi) bu IEEE 802.16 standartga muvofiq PHY va MAC darajalariga munosabatga ega mantiqiy uskunadir. Bu shuni bildiradiki, turli BSlar turli funksiyalarga ega bo‘lishi mumkin. WIMAX tarmog‘idan mantiqiy BS o‘z chastota resursini bir ma’lum sektor hisoblanadi. Ya’ni real BS bir nechta mantiqiy BSlar bilan birlashmasidan iborat. Yuklamani bir tekis taqsimlash yoki BS tizimining to‘lib qolishi uchun BS bir necha ASN – shlyuzlar orqali ulanishi mumkin.



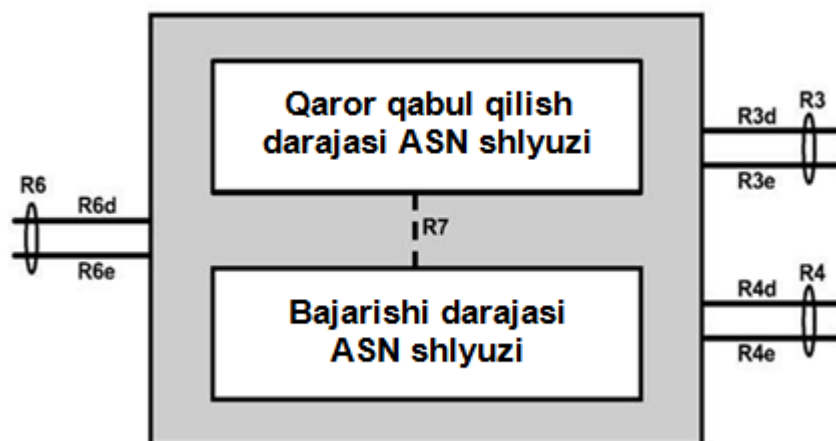
3.5- rasm. ASN tayanch nuqtalari

ASN–shlyuz tavsifi

ASN–shlyuz mazkur mantiqiy qurilmalarning qismini o‘ziga olish bilan ASN va CSN tugunlar orasida o‘zaro ta’sirlashishi bo‘yicha funksiyalarni bajaradigan mantiqiy uskuna hisoblanadi. Shuningdek, ASN – shlyuz bir ASN tuguni BS ini boshqa ASN tugunlar va CSN tugun bilan bog‘laydi. Bunda aloqa ham trafik kanallari darajasida ta’minlanadi. Yuklamani bir tekis taqsimlash va tarmoqning ishonchliligini ta’minlash uchun ASN tugunda bir necha ASN – shlyuzlar bo‘lishi mumkin.

ASN–shlyuzning funkcionalligi

ASNning funkcionallik imkoniyatlari asosan ASN–shlyuzga qo‘yilgan, u opsional jihatdan ikkita DP (ingl. *Decision Point*) qarorni qabul qilish va EP (ingl. *Enforcement Point*) bajarish darajasiga bo‘linishi mumkin. Bunday bo‘linish tarmoqqa ASN – shlyuzlarni qulay joriy etish uchun maxsus qilingan. DP va EP darajalar R7 tayanch nuqtasidan orqali bir-birlari bilan ta’sirlashadi. Bunda DP daraja bittadan ortiq EP darajalar bilan (ya’ni ASN–shlyuz bilan) o‘zaro ta’sirlashishi mumkin. EP daraja trafikni uzatish funksiyasini, DP daraja esa boshqarish funksiyasini bajaradi. R3, R4, R6 tayanch nuqtalarga qo‘yilgan ASN – shlyuzlar funksiyalari 3.6-rasmda keltirilgan.



3.6- rasm. ASN – shlyuzining tayanch nuqtalari

Misol uchun, R6 d va R6 c tayanch nuqtalari BS va ASN – shlyuzining DP va EP darajalari orasidagi interfeys hisoblanadi. BS va ASN – shlyuzlar orasida funksiyalarni taqsimlanishi ASN profillar (A, B va C profillar) tomonidan aniqlanadi.

CSN kommutatsiya tarmog‘i

CSN tuguni ham WIMAX tarmog‘i ichida, ham tashqi IP-tarmoqlar bilan abonentlarga aloqa xizmatlarini taqdim etadigan bevosita WIMAX operatori tarmog‘i hisoblanadi. CSN da IP-marshrutlashtirish, RCRF va abonentlar prodgillarini saqlash, ASN tugunlar bilan trafikni almashtirish AIS ASN hududi chegaralaridan chiqqanda mobillikni boshqarish, roumingda turli CSN tugunlari orasida trafikni tunnellashtirish, billing va rouming hisoblari, multimediya servislari, qonuniy ushlab va boshqalar kabi ko‘p sonli funksiyalar ishlatiladi. CSN tugun marshrutizatorlar, AAA proksi-serverlar, abonentlar ma’lumotlari bazasi va o‘zaro ta’sirlashish shlyuzlari kabi tarmoq elementlarini o‘z ichiga olishi mumkin. CSN tuguni yana yaratiladigan tarmoq yoki mavjud WIMAX xizmatlari provayderi tarmoqlari qismi sifatida ishlatilishi mumkin [11].

IEEE 802.16 standartiga mobillikni kiritilishi bilan NRM bazaviy modelga NSP(ingl. *Home NSP* va *Visited NSP*) tarmoq xizmatlari provayderining uy va mehmon tugunlari kiritildi. Uy HSP bu AQga aloqa xizmatlarini taqdim etadigan operator, mehmon HSP esa AQga rouming xizmatlarini taqdim etadigan operatoridir. Buning uchun uy va mehmon HSP o‘zaro rouming haqida shartnoma imzolaydi. Ham uy va ham mehmon HSP AAA funksiyalarini bajaradi. AQga tarmoqning yozilgan xizmatlariga taqdim etishni taqdim etadi, lekin

billing va abonent to'lovini hisob-kitobi uy NSP orqali amalga oshiriladi. Roumingda AQ uchun trafikni marshrutlashtirish ham uy NSP orqali, ham to'g'ridan-to'g'ri mehmon NSP orqali amalga oshirilishi mumkin.

Tayanch nuqtalarining funksiyalari

Tayanch nuqtasi ikki turli tarmoqlar guruhlarida joylashgan ikkita funksional tugunlar orasida o'zaro ta'sirlashish nuqtasi hisoblanadi.

Bunda quyidagi shartlar to'g'ri:

- mazkur tayanch nuqtasining protokollari doim ham bir funksional guruhga birlashtirilmagan;
- tayanch nuqtasi orqali birlashtirilgan ikkita tugun turli funksional guruhlarda bo'ladi.

R1 tayanch nuqtasi

R1 tayanch nuqtasi IEEE 802.16 standarti spetsifikatsiyasi bo'yicha radiointerfeys orqali AQ va ASN tuguni orasidagi protokollar va protseduralardan tashkil topgan R1 tayanch nuqtasi boshqarish rejasiga muvofiq qo'shimcha protokollarni o'z ichiga olishi mumkin.

R2 tayanch nuqtasi

R2 tayanch nuqtasi NSP uy tarmog'i bilan ta'sirlashadigan AQ va SSN tuguni orasidagi protokollar va protseduralardan tashkil topgan R2 Autentifikatsiyalash, mualliflashtirish va IP-konfiguratsiyalash funksiyalarini bajaradigan mantiqiy inerfeys hisoblanadi.

R3 tayanch nuqtasi

R3 tayanch nuqtasi AAA xizmatlarni, boshqarish siyosati va mobillikni boshqarish qo'llab-quvvatlash uchun ASN va SSN tuguni orasidagi nazorat protokoli to'plamidan iborat. U shuningdek, ASN va SSN tugunlar orasida trafikni uzatish funksiyasini bajaradi.

R4 tayanch nuqtasi

R4 tayanch nuqtasi nazorat va xizmat protokollari hamda ASN ishiga bog'liq turli funksional protseduralardan tashkil topgan va ASN mijozlar orqali ASN tugunlar orasida o'zaro ta'sirlashishni ta'minlaydi. Binobarin R4 tayanch nuqtasi orqali bir jinsli (geterogin) ASN tugunlar orasidagi o'zaro ta'sirlashish protokolini ta'minlaydi.

R5 tayanch nuqtasi

R5 tayanch nuqtasi uy va mehmon NSP provayder tarmoqlariga kiradigan SSN tugunlar orasidan nazorat protokollari to'plamidan iborat.

ASN tayanch nuqtalari

R6 tayanch nuqtasi

R6 tayanch nuqtasi BS va ASN - shlyuz orasida o'zaro ta'sirlashishi uchun nazorat va bir tomonga yo'nalgan kanallardan tashkil topgan [9]. Teskari aloqa kanali BS va ASN - shlyuz orasida ASN tuguni kanali ichidagi axborotni kanali hisoblanadi. Nazorat matritsasi axborot kanalini tashkil etish protokollari, mobil abonentlar AQLari uchun nazorat kanalini taqdim etish va o'zgartirishni o'z ichiga oladi. **R6 R4** bilan kombinatsiyada **R8** nuqta orqali almashtirish imkoniyatiga ega bo'lmagan bazaviy stansiyalar orasida MAS-holatlarni almashtirish uchun "tunnel bo'lib" xizmat qilishi mumkin.

R7 tayanch nuqtasi

R7 tayanch nuqtasi ASN-shlyuzdagi boshqarish siyosati va AAA funksiyalar uchun nazorat protokollari opsional matritsasidan tashkil topgan.

R8 tayanch nuqtasi

R8 tayanch nuqtasi AQ xizmat ko'rsatishni tez va sezilarsiz uzatilishi bo'lgan "xendover" uchun BS orasida trafikni uzatish opsional interfeysi va boshqaruvchi xabarlar va oqimlar interfeyslaridan tashkil topgan.

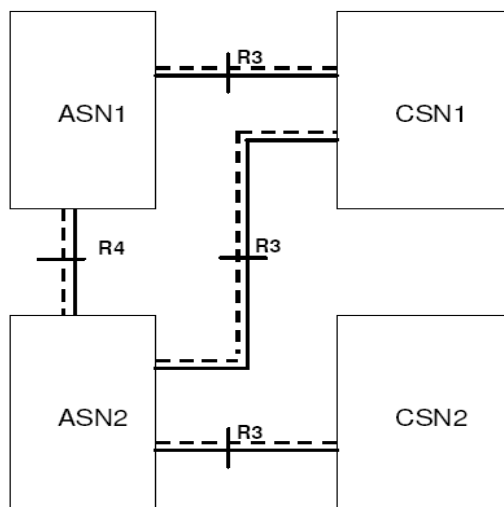
Radiulanish tarmog'i va kommutatsiya tarmog'ining o'zaro ta'sirlashishi. WIMAX tizimi arxitekturasining boshqa o'ziga xos xususiyatlari

3.7-rasmda ASN va CSN tugunlar bir operatorga tegishli bo'lmagan holda ularning o'zaro ta'sirlashishi mumkin va aksincha, bir nechta CSN tugunlari bitta ASN tuguniga ko'rinadigan bo'lishi mumkin.

WIMAX tizimi arxitekturasi bir tarmoq platformasida IP va Ethernet xizmatlarini taqdim etishga imkoniyat beradi. WIMAX tarmoq komponentlarini ixchamligi va moslashuvchanligi operatorlarga, shuningdek, aralash tarmoqlarda ham tashkil etish uchun turli ishlab chiqaruvchilarning foydalanish qulayligini beradi. WIMAX arxitekturasining universalligi quyidagi turli xizmatlar va ilovalarni qo'llab-quvvatlashga imkon beradi:

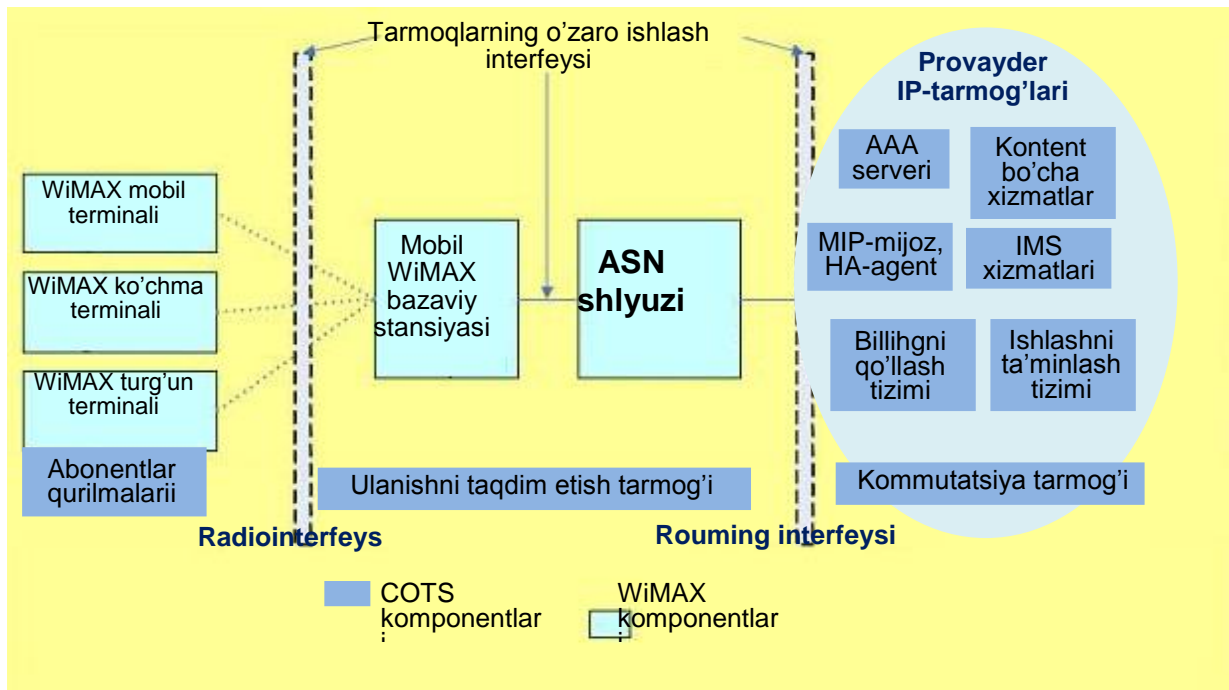
- Tovush va multimediya ilovalari, shuningdek, avariya chaqiruvlari va qonuniy ushlaridagi majburiy xizmatlar;
- Turli xizmat ko'rsatish tarmoqlariga mustaqil ulanish;
- IP bo'yicha tovushga asoslangan mobil tovushli aloqa (VoIP);

- IP bo'yicha SMS, IP bo'yicha MMS va boshqa xizmatlar;
- Guruhli va keng uzatishli aloqa.



3.7- rasm. WiMAX tayanch tarmog‘i tugunlarining o‘zaro ta’sirlashishi

O‘zaro ta’sirlashish va rouming xizmatlari WIMAX tarmoqlarining muhim funkcionalligi hisoblanadi. Xususan, WIMAX tarmoqlari 3GPP va 3GPP-2 simsiz tarmoqlar, shuningdek, IETF protokollari asosidagi DSL va MSO simli tarmoqlar bilan o‘zaro ta’sirlashishi mumkin. WIMAX tarmoqlari bilan global rouming xizmatlari o‘sha bir AQ identifikatorlaridan foydalanish imkoniyatlarini AAA va billing yagona funksiyalarini, “nom/parol” birlashmasi, raqamli sertifikatlar, SIM-kartalar, universal USIM-kartalar va RUIM (ingl. *Removable User Identify Module*) abonentni identifikatsiyalashning olinadigan modullari kabi turli Autentifikatsiyalash formatlarini qo‘llab-quvvatlash imkoniyatlarini o‘z ichiga oladi. Ko‘p darajali tuzilmali WIMAX tizimi arxitekturasining modeli 3.8-rasmda keltirilgan.



3.8- rasm. IP asosidagi WIMAX tarmog'i arxitekturasi

3.3.3. IEEE 802.16 standartidagi ish rejimlari

Avval ta'kidlaganimizdek, IEEE 802.16 standarti WIMAX tarmoqlari uchun fizik va MAC darajalarni tavsiflaydi. Bu sathlarda radiointerfeyslar texnologiyalari, kanallarga ulanish va modulyatsiya usullari, oqimlarni bajarish tizimlari, uzatiladigan axborotlar tuzilmasi, yuqori darajalar ma'lumotlarni uzatish protokollarini (avvalo ATM va IR) WIMAX tarmoqlarining pastki (fizik) darajalari protokollari uyg'unlashtirish mexanizmlari aniqlanadi. IEEE 802.16 standarti 3.5-jadvalda keltirilgan.

Jadvaldan ko'rinib turibdiki, faqat bitta eltuvchidan foydalanadigan WirelessMAN-SC (ingl. *Wireless Metropolitan Area Network-Single Carrier*) rejimi 10-66 GGs diapazonda ishlash uchun mo'ljallangan va 25 MGs kanal kengligida va 120Mbit/sek. ma'lumotlarni uzatish tezlikli to'g'ri ko'rinish sohasida ishlaydigan magistral tarmoqlarga yo'naltirilgan (mo'ljallangan). Qolgan rejimlar 11 GGs dan past diapazonlar uchun ishlab chiqilgan. WirelessMAN-SCa bu WirelessMAN-SC rejimining "past chastotali" versiyasidir (qator qo'shimcha mexanizmlari, xususan, 256-QAM kvadraturali-amplitudaviy modulyatsiyaga ruxsat etiladi).

WirelessHUMAN (ingl. *High Speed Unlicensed Metropolitan Area Network*) rejimi litsenziyasiz diapazonlarda ishlash uchun mo'ljallangan (bunday diapazonlar AQShda va qator Yevropa

davlatlarida ko‘zda tutilgan). WirelessHUMAN rejimining o‘ziga xos xususiyatlari faqat TDD, DFS (ingl. *Dynamic Frequency Selection*) chastotalarni dinamik taqsimlash funksiyasidan va chastota kanallarini nashrlashtirish mexanizmidan foydalanish hisoblanadi [8].

3.5- jadval

IEEE 802.16 standartining asosiy rejimlar

Rejim	Chastota diapazoni, GGs	Opsiyalar	Duplekslash usuli
WirelessMAN-SC	10-66		TDD/FDD
WirelessMAN-SCa	< 11	AAS/ARQ/STC	TDD/FDD
WirelessMAN-OFDM	< 11	AAS/ARQ/STC/ Mesh	TDD/FDD
WirelessMAN-OFDMA	< 11	AAS/ARQ/STC	TDD/FDD
WirelessHUMAN	<11, litsenziyalashtirilmaydigan diapazon *	DFS/AAS/ARQ/ Mesh/STC	TDD/FDD
* AQSh va Evropada			

WirelessMAN-OFDM va WirelessMAN-OFDMA kanallarni ortogonal bo‘lishga asoslangan va IEEE 802.16-2001 standartga nisbatan prinsipial yangi usullardir. Oldin bu rejimlar IEEE 802.16a standartiga kirgan, lekin qator o‘zgartirishlarga uchradi va natijada IEEE 802.16d standart IEEE 802.16e standartlariga kirdi.

11 GGsdan past diapazonlardagi barcha rejimlarda o‘ta takomillashtirilgan signalni qayta ishlash texnologiyalari qo‘llaniladi:

- ARQ-takroriy uzatishni avtomatik so‘rov mexanizmi;
- AAS - adaptiv antenna tizimlari bilan ishlashni qo‘llab-quvvatlash;
- AAS tizimlari bilan ishlashda STC-Fazoviy-vaqtli kodlash.

Shuningdek, WirelessMAN-OFDM rejimida “nuqta-ko‘p nuqta” markazlash turiga topologiyasiga qo‘shimcha rejimda mesh–tarmoq arxitekturasini qo‘llab-quvvatlash ko‘zda tutilgan (tarmoq terminallari

faqat AQ funksiyalarini bajarishdan tashqari, trafikni retranslyasiyanishi mumkin bo'lgan markazlashtirilmagan topologiya).

3.3.4. IEEE 802.16 standarti tarmog'i fizik darajasining tavsifi

IEEE 802.16 standartining fizik darajasi WIMAX tizimlari turli ish rejimlarining qo'llab-quvvatlashini hisobga olib ishlab chiqilgan va shu maqsadda uchiga prinsipial farqli signallarni qayta ishlash usullarini ko'zda tutadi:

- SC-FDMA bir eltuvchili modulyatsiya usuli (WirelessMAN-SC va WirelessMAN-SCa rejimlari);
- OFDM ortogonal eltuvchilar orqali multipleksorlash usuli (WirelessMAN-OFDM va WirelessHUMAN rejimlari);
- OFDMa ortogonal eltuvchilar orqali ko'plab ulanish usuli.

Bu usullarni atroflicha ko'rib chiqamiz.

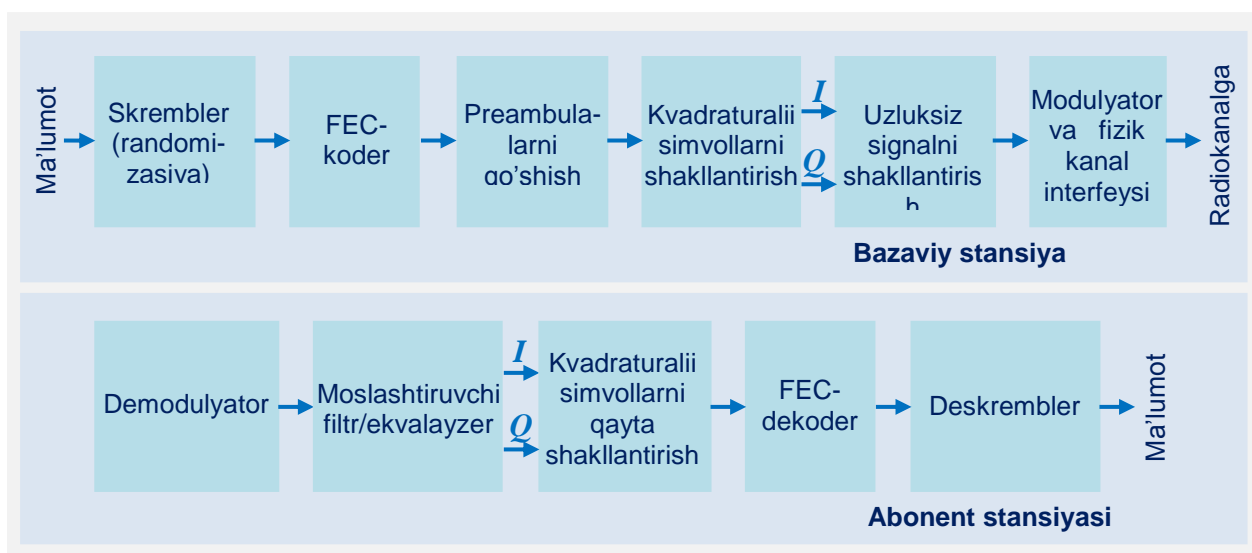
SC-FDMA bir eltuvchili modulyatsiya usuli

SC-FDMA usuli WirelessMAN-SC va WirelessMAN-SCa rejimlari qo'llanilgan. "Yuqoriga" va «pastga» liniyalar uchun WirelessMAN-SC rejimida signalni qayta ishlash protsedurasi bir necha operatsiyalardan tashkil topgan va 5.9-rasmda ko'rsatilganidek, ko'rinishda bo'ladi.

Kirish ma'lumotlari oqimi dastlab randomizatsiyaga uchraydi. Randomizatsiya (shuningdek, "skremblirovanie" atamasi qo'llaniladi) –bu usul orqali qabul qilingan ma'lumotlar tasodifiyga o'xshaganga o'zgartiriladi. Bunga ma'lum matematik mexanizm bo'yicha PTK generatori ishlab chiqaradigan qandaydir psevdo tasodifiy ketma-ketlikka ma'lumotlar oqimini kengaytirish hisobiga erishiladi.

Keyin skremblangan ma'lumotlar FEC (ingl. *Forward Error Correction*) xatoliklar tuzatish usulidan foydalanib halaqitbardosh kodlar yordamida himoya qilinadi. WirelessMAN-SC rejimida ikkita FEC kodlash algoritmi majburiy algoritmi hisoblanadi:

Galua FEC GF(256) maydonidagi simvollarni Rida-Solomon kodlashli va Rid-Solomon tashqi kodli kaskadli kod va ichki o'rama kod ($k = 7$ kodli cheklashli, $2/3$ kodlash tezligili) va Viterbi algoritmi bo'yicha dekodlash. Opsional ravishda boshqa ikkita algoritim qo'llanilishi mumkin: Rida-Solomon tashqi kodli va juftlikka tekshirilishi ichki kodli kaskadli kod (8,6,2) va blokli turbo kod.



3.9- rasm. WirelessMAN-SC rejimida signalni qayta ishlash trakt

Skremblash mexanizmlari va kaskadlash algoritmlari haqida axborotlar kadr preambulasiga kiritiladi va keyin modulyatsiya uchun yo'naltiriladi. WirelessMAN-SC usulida uch turdagi QPSK va 16-QAM (majburiy), shuningdek, 64-QAM (opsional) kvadraturali modulyatsiyadan foydalaniladi. Kodlangan bitli ketma-ketlik modulyatsion simvollariga o'zgartiriladi. (har bir 2/4/6 bit QPSK/16-QAM/64-QAM bir simvolini aniqlaydi). 2/4/6 bitdan iborat har bir guruhga mos ravishda sinfaz (I) va kvadraturali (Q) koordinatalar qo'yiladi. Keyin I va Q kanallardagi diskret qiymatlar ketma-ketligi SQRT-filtr (ingl. *Square-root Raised Cosine Filter*-ACHX kosinisoidal silliqilinishli filtr) yordamida uzluksiz signallarga o'zgartiriladi. $I(t)$ va $Q(t)$ filtrlangan oqimlar to'g'ridan-to'g'ri kvadraturali modulyatorga beriladi. Uning chiqishida quyidagi chiqish signali shakllanadi:

$$S(t) = I(t) \cos(2\pi f_c t) - Q(t) \sin(2\pi f_c t),$$

bu yerda, f_c –eltuvchi chastota.

Keyin signal kuchaytiriladi va efirga uzatiladi. Qabul qilish tomonida barcha jarayonlar teskari tartibda bo'lib o'tadi. Natijada, kanalning kengligiga va modulyatsiyalash usuliga bog'liq ravishda ma'lumotlarni turli uzatish tezliklari shakllanadi (3.6-jadval).

WirelessMAN-SC rejimida kanalning kengligi va modulyatsiya turiga bog‘liq ravishda ma’lumotlarni uzatish tezliklari

Kanalning kengligi, MGs	Simvollar tezligi, Mbod	Fizik ma’lumotlar oqimi tezligi, Mbit/sek.		
		QPSK	16-QAM	64-QAM
20	16	32	64	96
25	20	40	80	120
28	22,4	44,8	89,6	134,4

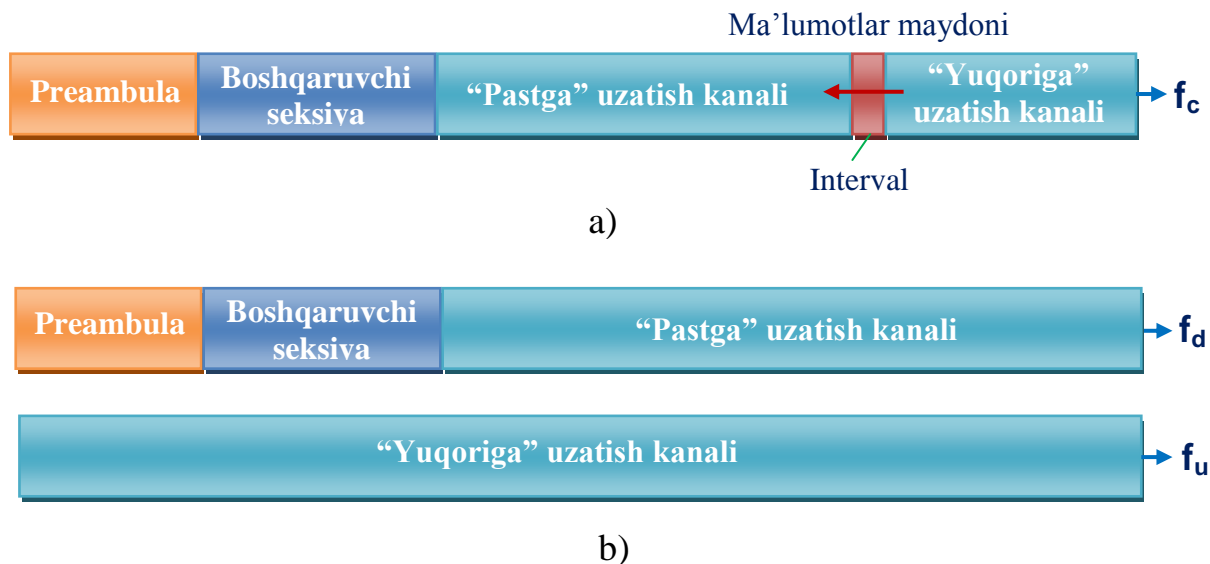
WirelessMAN-SC rejimidagi fizik kanalda kadrning tuzilmasi

WirelessMAN-SC rejimida fizik darajada ma’lumotlarni uzatish uzluksiz ketma-ketlikdagi kadrlar yordamida amalga oshiriladi. Kadrlar 0,5; 1 va 2 ms qayd etilgan uzunliklarga ega bo‘lishi mumkin. Kadrning preambulasi (32 QPSK–simvollaridagi sinxron ketma-ketlikdagi uzunlikda), boshqaruvchi seksiya va ma’lumotlar maydonidan iborat. Preambula va boshqaruvchi seksiyalar xabarlarini har doim QPSK-modulyatsiya yordamida uzatiladi, ma’lumotlar maydoni uchun esa yuqorida ko‘rsatilgan uchta modulyatsiya usullaridan biri qo‘llanilishi mumkin. Vaqtli va chastotaviy dubleksirlash usullarida kadrning tuzilmasi sezilarsiz farq qiladi.

TDD rejimida kadr “pastga” va «yuqoriga» subkadrlarga bo‘linadi, ular orasida esa maxsus interval qoldiriladi. “Pastga” va «yuqoriga» subkadrlar orasidagi munosabat zarur o‘tkazish polosasi bog‘liq ravishda ixcham o‘zgarishi mumkin. FDD rejimida «pastga» va «yuqoriga» kanallar bir-birlaridan ajratilgan eltuvchi chastotalardan foydalaniladi (3.10-rasm.)

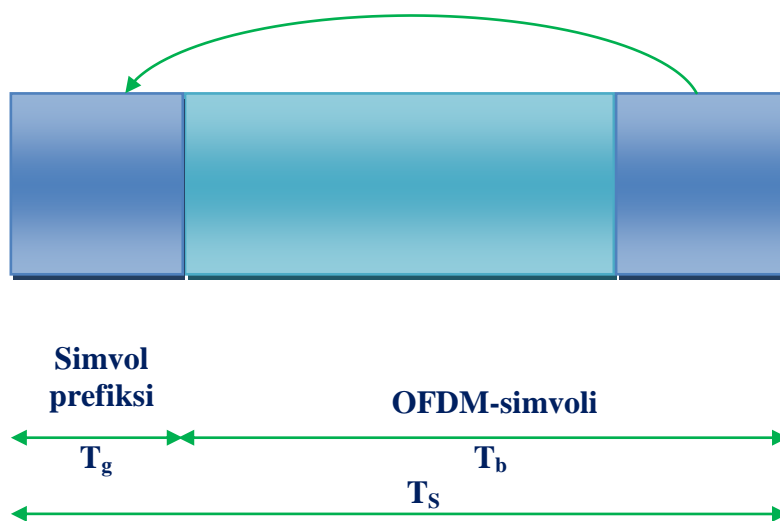
OFDM ortogonal eltuvchilar yordamida multiplekslash usuli

OFDM bu ko‘p sonli ortogonal qisqa polosali nimeltuvchi chastotalarga bo‘lingan bir keng polosali chastotaviy kanalda ma’lumotlar oqimini multiplekslash texnologiyasidir. Ortogonal eltuvchilar orasidagi masofa OFDM–simvolning T_s uzunligi hisoblanadi. OFDM–simvolga shuningdek, T_d uzunlikdagi SR (siklik prefiks) himoya intervali qo‘shiladi, unda OFDM –simvolning umumiy uzunligi $T_s = T_b + T_d$ ni tashkil etadi (3.11-rasm). SR himoya intervali simvolning oxirgi fragmenti nusxasi hisoblanadi va uning T_d uzunligi T_b dan 1/4, 1/8, 1/16, 1/32 qismini tashkil etishi mumkin.



3.10- rasm. Kanallarni vaqtli (a) va chastotaviy (b) dublekslashli tizimlar uchun IEEE 802.16a standartidagi kadrlar tuzilmasi

Har bir nimeltuvchi mustaqil ravishda fazaviy yoki kvadraturali amplitudaviy modulyatsiya yordamida modulyatsiyalanadi va umumiy signal teskari Fure tezkor o'zgartirish usuli bilan hisoblanadi. IEEE 802.16d standartida OFDM rejimi uchun $N=200$ nimeltuvchilar soni va mos ravishda $N_{OBPF}=256$ ga teng bo'lgan razryadlar soni ko'zda tutilgan. Ulardan 55 tasi ($k = -128 \dots -101$ va $101 \dots 127$) chastota kanali chegaralarida himoya intervallarini tashkil etadi. Kanalning markaziy chastotasi ($k = 0$) va himoya intervallari chastotalari signalni uzatish uchun ishlatilmaydi (ya'ni, ularga mos signallar amplitudalari nolga teng). Qolgan 200 ta nimeltuvchilarda sakkizta chastota pilot ($\pm 88, \pm 63 \pm 38, \pm 13$ indeksli) qolganlari 12 ta nimeltuvchilardan iborat 16 ta subkanallarga bo'linadi, ularning har birida chastotalar bir tartibda joylashmagan. Masalan, 1-subkanalni $-100, -99, -98, -37, -36, -35, 1, 2, 3, 64, 65, 66$ indeksli nimeltuvchilar tashkil etadi. Subkanallarga bo'lish zarur, chunki WirelessMAN-OFDM rejimida (opsional) barcha 16 ta subkanallarda emas, balki 1, 2, 4, 8 subkanallarda ishlash imkoniyati ko'zda tutilgan. Buning uchun har subkanal va har bir subkanallar guruhi o'z indekslariga ega bo'ladi (0 dan 31 gacha). OFDM-simvolning foydali qismini T_b uzunligi kanal polosasining uzunligiga va tizimiy takt chastotasiga (diskretlashtirish chastotasi) bog'liq [11].



3.11- rasm. OFDM–simvolning tuzilmasi

OFDM-multiplekslashda SR himoya intervalidan foydalanish shahar sharoitlaridagi qayta jipslanishlar va signalning ko‘p nurli tarqalishi natijasida vujudga keladigan SAI (simvollararo interferensiyadan) qutqaradi. Biroq, bu mexanizm OFDM-simvol T_b foydali qismi uzunligining chegaralarida fazaviy kechikish bilan keladigan o‘sha bir simvoldagi signallarning ustma-ust tushishi bo‘lgan ichki simvolli interferensiyani (ISI) oldini ololmaydi. Natijada axborot to‘liq buziladi. Yoki butunlay yo‘qoladi (masalan, 180^0 ga fazaviy surilishda). ISI ga qarshi turish va alohida simvollar yoki ularning fragmentlari yo‘qotilganda ma‘lumotlarni yo‘qotilishining oldini olish uchun IEEE 802.16 standartida kanalli kodlashning samarador vositalari qo‘llaniladi. Fizik darajada ma‘lumotlarni kodlash uchta randomizatsiya, halaqitbardosh kodlash va o‘rin almashtirish bosqichlarini o‘z ichiga oladi.

Randomizatsiya ma‘lumotlar blokini PTKK generatori shakllantiradigan psevd tasodifiy ketma-ketlikka ko‘paytirish yo‘li bilan amalga oshiriladi. Bu protsedura bilan “ma‘lumotlar oqimini oqartirish” deyiladi.

Qabullash tomonida keyin dastlabki tuzilmalashtirilgan ketma-ketlikni olish maqsadida bu tasodifiy ketma-ketlikni teskari o‘zgartirish bajariladi.

Ma‘lumotlarni kodlash Rid-Solomon tashqi koderi va ichki o‘rama koderdan iborat ikkita bosqichdagi kaskadli kodlarning qo‘llanilishini ko‘zda tutadi. Rid-Solomon koderi BPSK ikki pozitsiyali modulyatsiya bilan va OFDM subkanallari ishlatiladigan hollarda qo‘llanilmaydi. Tavsiflangan kodlash mexanizmidan tashqari,

standart blokli turbokodlarni (Xemming kodlariga va juftlikni nazorat qilishga asoslangan) va o‘rama turbokodlarni opsional qo‘llanilishini ko‘zda tutadi.

Kodlashdan keyin o‘rin almashtirish protsedurasi (shuningdek, “interliving” atamasi qo‘llaniladi) keladi. Bu OFDM simvolga mos keladigan ma’lumotlarni kodlash bloki chegaralarida bitlarni o‘rin almashtirishi hisoblanadi. Bu operatsiya ikkita bosqichda amalga oshiriladi. Dastlab qo‘shni bitlar qo‘shni bo‘lmagan eltuvchilarga tarqatiladi, keyin esa qo‘shni bitlar turli yarim ketma-ketliklarga tarqatiladi. O‘rin almashtirishdan maqsad shundaki, simvoldagi guruhli xatoliklarda qo‘shni bo‘lmagan bitlar zararlansin va shunday qilib, bitlarni qayta tiklanish darajasi ortsin.

O‘rin almashtirishdan keyin modulyatsiya bosqichi boshlanadi. Tanlangan modulyatsiya sxemasidan (BPSK, QPSK, 16-QAM, 64-QAM) kelib chiqib, blok modulyatsion simvollarga mos ravishda bitlar guruhlari ketma-ketligidan (1/2/4/6 bitlar) iborat bo‘ladi.

3.7- jadval

Qo‘llab-quvvatlanadigan kodlash va modulyatsiya usullari

		«Pastga»	«Yuqoriga»
Modulyatsiya		QPSK, 16-QAM, 64-QAM	QPSK, 16-QAM, 64-QAM
Kodlash tezligi	CC	1/2, 2/3, 3/4, 5/6	1/2, 2/3, 5/6
	CTC	1/2, 2/3, 3/4, 5/6	1/2, 2/3, 5/6
	Qaytarilish	x2, x4, x6	x2, x4, x6

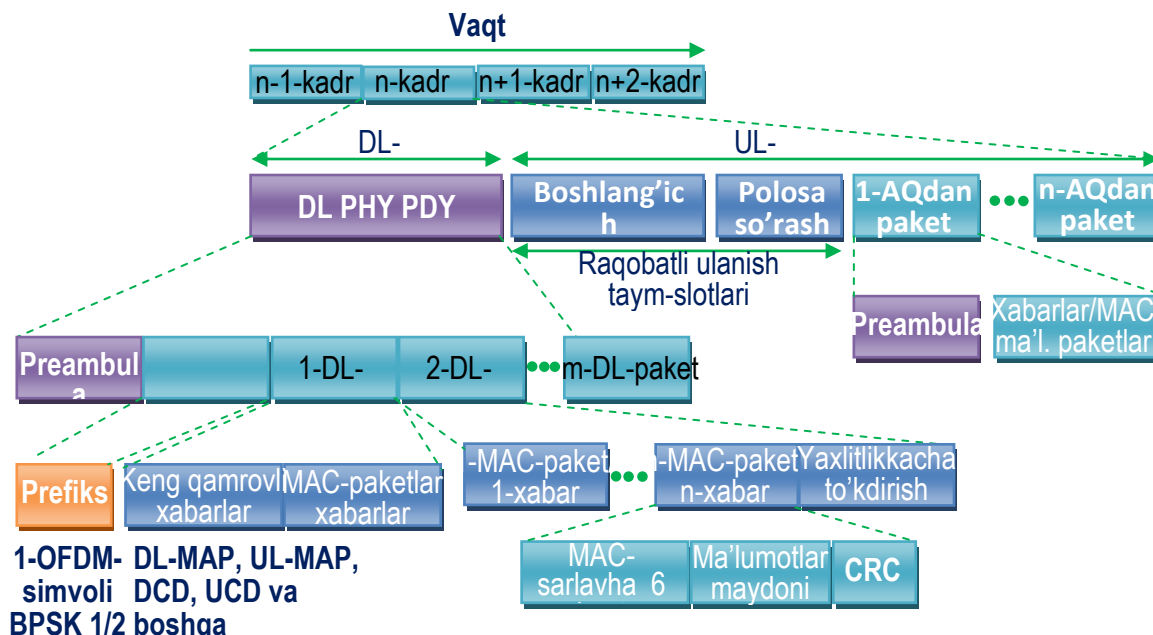
Har bir guruhga keyinchalik ular eltuvchini bevosita modulyatsiyalashda ishlatiladigan Grey vektor diagrammalaridan mos ravishdagi Q va I qiymatlar qo‘yiladi. Kvadraturali simvollar amplitudalarini o‘rtachalashtirish uchun Q va I me‘yorlashtirilgan qiymatlar ishlatiladi. (ya’ni, s koeffitsientlarga ko‘paytirilgan: QPSK uchun $s = 1/\sqrt{2}$, 16-QAM uchun $s = 1/\sqrt{10}$, 64-QAM uchun $s = 1/\sqrt{42}$).

TFTO‘ mexanizmidan foydalanib modulyatsion simvollar aniqlanganidan keyin radiosignalning o‘zi hisoblanadi va uzatkichga uzatiladi. Qabullashda barcha protseduralar teskari tartibda amalga oshiriladi.

WirelessMAN-OFDM rejimidagi kadrning tuzilmasi

OFDM rejimida fizik darajada “nuqta-ko‘p nuqta” arxitekturali tarmoqlar uchun kadrli uzatish tuzilmasi WirelessMAN-SC

rejimidagidan prinsipial kam farq qiladi. Axborotlarni almashtirish ham FDD yoki TDD asosida «pastga» va «yuqoriga» subkadrarga bo‘linadigan kadrlar ketma-ketligi yordamida amalga oshiriladi (3.12-rasm).



3.12- rasm. TDDli OFDM–kadrning tuzilmasi

«Pastga» subkadr preambula, kadr sarlavhasini boshqaruvchi (ingl. *Frame Control Header, FCH*) va ma’lumotlar paketlari ketma-ketligini o‘z ichiga oladi. Preambula «pastga» kanalda ikki OFDM-simvoldan iborat (uzun preambula), kadrlarni sinxronlashtirishga mo‘ljallangan va QPSK yordamida modulyatsiyalanadi. Preambuladan keyin standart kodlash sxemasini BPSK yordamida modulyatsiyalanadigan va bitta OFDM-simvoldan iborat kadr sarlavhasini boshqaruvchi keladi. Sarlavha DL–subkadrda birinchi paket (yoki bir necha boshlang‘ich) uzunligini va profilini tavsiflaydigan «pastga» kanal kadrining prefiksida (ingl. *Downlink Frame Rrefix, DLFP*) iborat. Birinchi paketga keng uzatishli xabarlar, “pastga” va «yuqoriga» liniyalarda paketlarning joylashish xaritasi (DL-MAP/UL-MAP) «pastga»/«yuqoriga» kanallar diskriptorlari va boshqa xizmat axborotlari kiradi.

«Pastga» subkadr AQ boshlang‘ich initsializatsiyalash uchun (tarmoqqa ulanishni olish uchun) va uzatishga kanal so‘rov uchun davrlarni o‘z ichiga oladigan raqobatli ruxsat intervalidan iborat. Keyin BS ma’lum AQ larga uzatish uchun tayinlangan vaqt

intervallari keladi. Bu intervallarning taqsimlanishi haqida axborotlar (boshlanish nuqtalari haqida) UL-MAP xabarlarida joylashadi. AQ o'z vaqt intervalida qisqa preambulani (bitta OFDM-simvol) uzatish bilan translyatsiyani boshlaydi, undan keyin MAC-darajada shakllantirilgan axborot paketi uzatiladi. OFDM-kadrlarining uzunliklari 2,5; 4; 5; 8; 10; 12,5; va 20 ms larni tashkil etishi mumkin. BS belgilangan kadrlarni qurish davrini o'zgartirib bo'lmaydi, chunki bu holda barcha AQLarni resinxronlashtirish talab qilinadi. Ulanishlarni o'rnatilishiga so'rov umumiy qabul qilingan IEEE 802.16d standartidan farq qilmaydi. Lekin, OFDM rejimida kanal resursi faqat vaqt sohasida emas, balki chastota sohasida ham, ya'ni alohida kubkanalarda taqdim etilishi mumkin. BS va AQ bunday imkoniyatlarni qo'llab-quvvatlaydigan sharoitlarda.

OFDMA - ortogonal eltuvchilar yordamida ko'plab ulanish usuli

Modulyatsiya simvollarining shakllanishi nuqtai nazaridan WirelessMAN-OFDM va Wireless MAN-OFDMA rejimlari bir xil. Farq kanallarni ajratish mexanizmlaridan iborat (ko'p sonli ulanish). OFDMAda mantiqiy kanal fizik kanalning barcha ruxsat etiladigan chastotalar diapazoniga taqsimlangan eltuvchilarni tanlash (to'plami) bilan tashkil qilinadi. OFDM rejimida esa bu mexanizm soddalashtirilgan ko'rinishlarda opsional foydalaniladi, unda kanalli 16 ta subkanallarga bo'lish amalga oshiriladi.

OFDMA da fizik kanalning kengligi me'yorlashtirilmagan bo'lsada, real tarmoqlarda 5 MGs dan past chastotali kanallar samarador bo'lmaydi. OFDMAda eltuvchilar soni 2048 tagacha bo'lishi mumkin, mos ravishda subkanallar soni tarmoqning ishini tashkil etishi uchun yetarli bo'lib qoladi. Turli rejimlarda ular 32 tadan 70 tagacha, har birida esa 24 yoki 48 tadan nimeltuvchilar bo'lishi mumkin. Bunda tizim takt chastotasi kanal kengligining $8/7$ qismini tashkil etadi. Signalni shakllantirish usuli, OFDM-simvollar tuzilmasi va kanalni kodlash mexanizmi OFDM va OFDMA rejimlarida deyarli bir xil. Randomizatsiyalash usuli faqat PTK generatorining initsializatsiyalovchi vektorini shakllantirish usuli bilan farqlanadi. Va OFDMA dagi halaqitbardoshli kodlar majburiy sifatda faqat bitta kodlash bosqichini o'rama koddan foydalanishni ko'zda tutadi (OFDM dagi kabi kodlash tezliklari to'plami bilan).

OFDM va OFDMA rejimlaridagi modulyatsiya sxemalari deyarli mos tushadi, farq shundaki, OFDMA da ko'zda tutilgan usullar

to'plami $\frac{1}{2}$ va $\frac{3}{4}$ kodlash tezliklari QPSK va 16-QAM, opsional esa $\frac{1}{2}$, $\frac{2}{3}$ va $\frac{3}{4}$ kodlash tezlikli 64-QAM usullarini o'z ichiga oladi. Shuningdek, OFDMA rejimida kvadraturali modulyatsiya simvollarini shakllantiradigan va ularning amplitudalari o'rtachalashtirilganidan keyin har bir eltuvchidagi simvollar ketma-ketligi OFDM rejimida generatsiyalanganidek, binar PTK ga W_k ga ko'payadi. Har bir k-nchi nimeltuvchi $1-2W_k$ qiymatga ko'payadi (ya'ni, agar $W_k=0$) u holda $1-2W_k=1$, va simvol o'zgarmaydi; agar $W_k=1$, u holda simvol -1 ga ko'payadi. Pilot nimeltuvchilar simvollarini VPSK usulida modulyatsiyalanadi, ularning qiymatlari ham $S_k=1-2W_k$ orqali hisoblanadi, lekin pilot nimeltuvchilar signallari quvvati, axborotlar nimeltuvchilari o'rtacha quvvatidan 2,5 dB ga ortiq bo'lishi kerak, u holda S_k qiymat qo'shimcha $\frac{4}{3}$ ga ko'paytiriladi.

Wireless MAN-OFDMA rejimidagi kadrning tuzilmasi

WirelessMAN-OFDMA rejimidagi kadrning tuzilmasi ko'p jihatdan yuqorida ko'rib chiqilgan kadrlar tuzilmalariga o'xshash, lekin o'zining farqlariga ham ega. Kadrning uzunliklari 2; 2,5; 4; 5; 8; 10; 12,5; va 20 ms larni tashkil etishi mumkin. OFDMA kadri subkanallar to'plamini o'z ichiga oladigan OFDMA-simvollar ketma-ketligidan iborat. OFDMA-simvollaridan iborat ma'lumotlar paketlari turli subkanallarda bir vaqtda uzatilishi mumkin. Subkanallar bo'yicha nimeltuvchilarni taqsimlash (ya'ni bir subkanalga nimeltuvchilarni taqsimlash) uzatish yo'nalishga va nimeltuvchilarni taqsimlash usuliga bog'liq. IEEE 802.16 standarti ham «pastga», ham «yuqoriga» kanalda nimeltuvchilarni taqsimlashning bir necha usullarini tavsiflaydi.

Prinsipial jihatdan ular FUSC (ingl. *Full Usage of the Subchannels*) BS uzatkichi tomonidan tomonidan to'liq ishlatiladigan va RUSC (ingl. *Portial Vsage of the Subchannels*) subkanallar qisman, ya'ni butun ruxsat etiladigan diapazon to'liqsiz ishlatiladigan turlarga ajratiladi. RUSC va FUSC usullarida (va ularning variatsiyalarida) har bir subkanalga barcha ruxsat etiladigan fizik kanal bo'yicha bir tekis taqsimlangan nimeltuvchilar taqdim etiladi. Lekin boshqa yondashuv subkanallarda ketma-ket (qo'shni) nimeltuvchi chastotalar to'plamidan foydalaniladi. Bunday yondashuv adaptiv antenna tizimlarida ishlash uchun mo'ljallangan AMS (ingl. *Adaptive Modulation and Coding*) uslubida ishlatilgan. AMS usulida ham 2048 ta nimeltuvchi ishlatiladi, ulardan 160 tasi pastki va 159 tasi himoya intervallarini tashkil etadi, markaziy chastota esa ishlatilmaydi.

Qolgan nimeltuvchilar har biri 9 ta nimeltuvchidan bo‘lgan 192 ta chastota guruhlariga (ingl. *bin*) ketma-ket bo‘lib chiqiladi. Har bir guruhdagi markaziy (beshinchi) nimeltuvchi pilot hisoblanadi. AMS rejimida subkanal bir chastota guruhini vaqt bo‘yicha oltita ketma-ket OFDM-simvollarini yoki ikki chastota guruhini va uchta OFDMA-simvollarini ishlatadi. AMS-subkanallarning tuzilmasi «pastga» va «yuqoriga» subkadrda bir xil. Bunda nimeltuvchilarni qayta o‘rnatish subkanal chegaralarida amalga oshiriladi.

Ta’kidlaymizki, bitta subkadr chegaralarida subkanallar bo‘yicha nimeltuvchilarni taqsimlash turli RUSC, FUSC, AMS va boshqa taqsimlash mexanizmlaridan foydalanish mumkin. Standartda “qayta o‘rnatish hududlari” chegaralari (ingl. *Permutation Zone*) DL-MAP va UL-MAP subkadr kartalarida aniqlanadi.

OFDMA-rejimida ma’lumotlarni uzatish uchun minimal resurs “slot” hisoblanadi. Slot bir subkanalni va bittadan o‘rtacha OFDMA-simvollar ketma-ketligini egallaydi. «pastga» subkadrda slotning uzunligi FUSC rejimda bir simvolga RUSC rejimda esa ikkita simvolga teng. «Yuqoriga» subkadrda slotning uzunligi doimo uchta OFDMA-simvollariga teng. WirelessMAN-OFDMA rejimi uchun RNY darajasining asosiy ko‘rsatkichlari 3.8-jadvalda keltirilgan.

“Mobil WIMAX” boshlang‘ich versiyalarida faqat TDD vaqtli dupleks qo‘llab-quvvatlaydi. WIMAX Forumi IEEE 802.16 standartining versiyalarida TDD dan foydalanish ta’qiqlangan yoki FDD ning qo‘llanilishi afzalroq bo‘lgan bozorlarni o‘zlashtirish maqsadida FDD uslubini kiritish istaldi.

3.8- jadval

WirelessMAN-OFDMA rejimi uchun RNY darajasining asosiy ko‘rsatkichlari

Parametrlar	“Pastga”	“Yuqoriga”	“Pastga”	“Yuqoriga”
Kanal kengligi	5 MGs		10 MGs	
FFT soni	512		1024	
Nol nimeltuvchilari	92	104	184	184
Pilot nimeltuvchilari	60	136	120	180
Ma’lumot nimeltuvchilari	360	272	720	560
Subkanallar	15	17	30	35

Simvol davri, T_s		102,9 mikrosekund			
Kadr vaqti		5 millisekund			
OFDM simvollar/kadrda		48			
Ma'lumot OFDM simvollari		44			
Modulyat siya turi	Kodlash tezligi	5MGs li kanal		10MGs li kanal	
		“Pastga” uzatish tezligi, Mbit/sek	“Yuqoriga” uzatish tezligi, Mbit/sek	”Pastga” uzatish tezligi, Mbit/sek	“Yuqoriga” uzatish tezligi, Mbit/sek
QPSK	1/2 CTC, 6x	0,53	0,38	1,06	0,78
	1/2 CTC, 4x	0,79	0,57	1,58	1,18
	1/2 CTC, 2x	1,58	1,14	3,17	2,35
	1/2 CTC, 1x	3,17	2,28	6,34	4,70
	3/4 CTC	4,75	3,43	9,50	7,06
16-QAM	1/2 CTC	6,34	4,57	12,67	9,41
	3/4 CTC	9,50	6,85	19,01	14,11
64-QAM	1/2 CTC	9,50	6,85	19,01	14,11
	2/3 CTC	12,67	9,14	25,34	18,82
	3/4 CTC	14,26	10,28	28,51	21,17
	5/6 CTC	15,84	11,42	31,68	23,52

TDD usuli ishlatishda murakkab hisoblansada, (chunki u barcha tizim chegaralarida vaqtli sinxronlashtirishni talab qiladi), baribir u quyidagi sabablar bo'yicha afzal bo'lib qoladi:

- TDD «pastga» va «yuqoriga» kanallar munosabatlarini dinamik boshqarish imkoniyatini beradi va buning hisobiga assimetrik trafikni samarali qo'llab-quvvatlaydi. FDD esa “pastga” va “yuqoriga” qayd etilgan kanallar bilan ishlaydi, shunga ko'ra simmetrik trafikka ega.

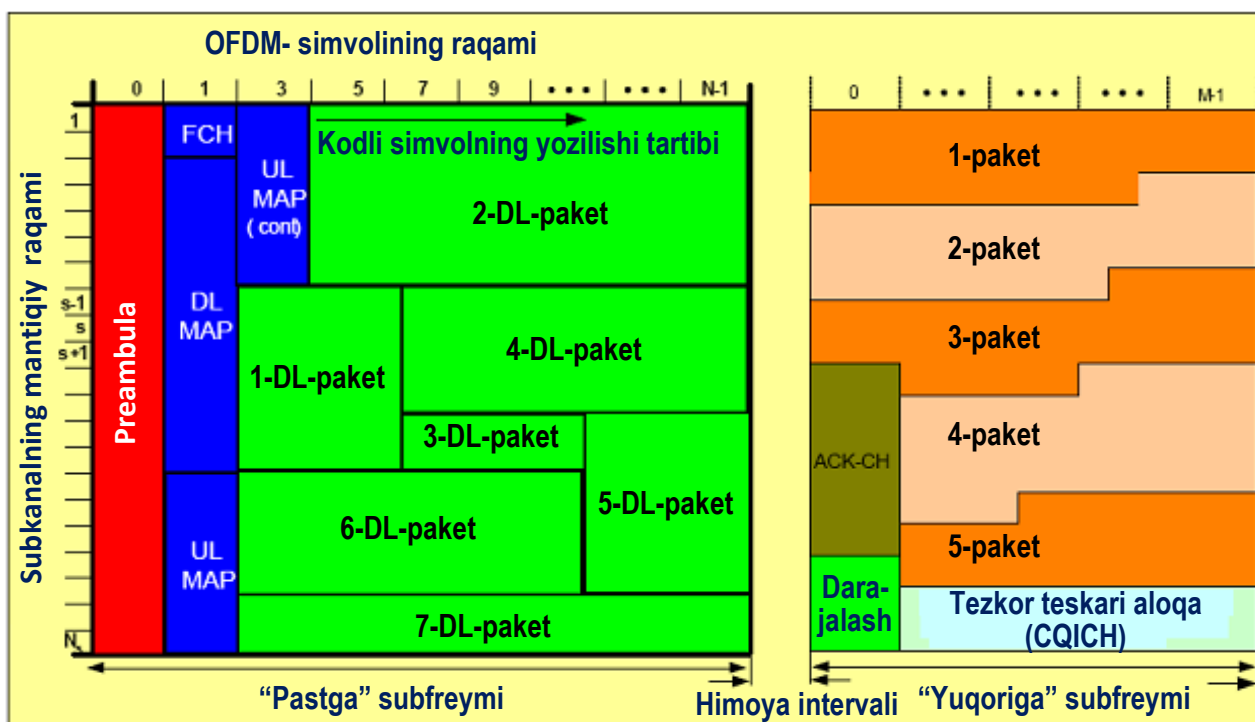
- TDD teskari aloqani talab qiladigan MIMO va boshqa takomillash antenna texnologiyalari, kanallar moslashishini qo'llab-

quvvatlash uchun kanalning parametrlari bo'yicha eng yaxshi teskari aloqani ta'minlaydi.

- Juft chastota kanallari talab qilinadigan FDD dan farqli ravishda TDD usuli "pastga" va "yuqoriga" kanallari uchun bir chastota kanalidan foydalanadi, mos ravishda ega bo'lgan radiochastota resursiga nisbatan ixcham hisoblanadi.

- TDD usuli uchun bazaviy stansiya konstruktiv jihatdan kamroq murakkab va mos ravishda arzon turadi.

3.13-rasmda TDD usuli ishlatilgan OFDM kadrining tuzilmasi keltirilgan.



3.13- rasmda TDD usuli ishlatilgan OFDM kadrining tuzilmasi

Har bir kadr "pastga" va "yuqoriga" liniyalari orasida kolliziyalarning oldini olish uchun bir-birlari bilan himoyaviy vaqt intervallari bilan ajratilgan «pastga» va «yuqoriga» subkanallarga (uzatish va qabullash rejimlarining belgilanishi uchun mos ravishda TTG va RTG).

Kadrda tizimning optimal ishlashini ta'minlash uchun quyidagi boshqarish maydonlari ishlatiladi:

- Preamble-OFDM kadrining birinchi simvoli hisoblanadi va kadrlarni sinxronlashtirish uchun ishlatiladi.

- FSN kadrni boshqarish sarlavhasidan keyin keladi va o'zida MAR xabarining uzunligi, kodlash sxemasi va bo'sh subkanallar

nomerlari va boshqalar kabi kadr konfiguratsiyasi haqida axborotni tashiydi.

- DL-MAP “pastga” va UL-MAR “yuqoriga” kanallar subkadrleri kartalarining xabarleri-mos subkadrler uchun DL-MAP, UL-MAR subkanallarini va boshqa nazorat axborotlarining taqsimlanishini ta’minlaydi.

- «yuqoriga» signali ishlov berish maydoni (ingl. *UL Ranging*). UL Ranging maydoni vaqt, chastota va signal quvvati bo’yicha o’rnatishlarni bajarish, shuningdek, berk aloqa rejimida o’tkazish polosasiga so’rov uchun AQga ajratiladi.

- Kanal sifati indikator “yuqoriga” kanal (ingl. *ULSQICH*)-radiokanalning holatini baholash bo’yicha BS bilan teskari aloqa uchun AQga ajratilgan.

- “Yuqoriga” kanalni taqsimlash maydoni (ingl. *UL ASK*)-paketning olinganligini tasdiqlash uchun AQga ajratilgan.

IEEE 802.16-2005 standarti ko’lamlashtirilgan OFDMA(S-OFDMA) texnologiyalariga asoslangan. Bunday tanlash S-OFDMA texnologiyasi turli o’tkazish polosalarini qo’llab-quvvatlash mumkinligi tufayli amalga oshirilgan, bu AQning turli ish rejimlariga ixcham xizmat ko’rsatish va mavjud chastota resurslariga mos kelishi uchun zarur bo’ladi. Texnologiyaning ko’lamligiga nimeltuvchi chastota kengligi qayd etilgan va 10,94 kGs teng qolganda massivni FTTO o’zgartirilishi hisobiga erishiladi [2].

Nimeltuvchi kengligi va OFDM-simvol davomiyligi o’zgarmay qolishi hisobiga kanalni o’tkazish polosasining ko’lamlashtirishida yuqoriroq darajalarga ta’sir etishi minimal bo’lib qoldi. S-OFDMA parametrlari 3.9-jadvalida keltirilgan.

3.9- jadval

Ko’lamlashtirilgan OFDMA parametrlari

Parametrlar	Qiyamatlar			
Kanal kengligi (MGs)	1,25	5	10	20
Diskretizatsiya chastotasi (F_p , MGs da)	1,4	5,6	11,2	22,4
FFT soni (N_{FFT})	128	512	1024	2048
Subkanallar soni	2	8	16	32
Nim eltuvtchilarning polosa kengligi	10,94 kGs			
Simvolning foydali vaqti ($T_b=1/f$)	91,4 mikrosekund			

Himoya intervali ($T_g = T_b/8$)	11,4 mikrosekund
OFDMA simvolining vaqti ($T_s = T_b + T_g$)	102,9 mikrosekund
Kadrdagi OFDMA simvollar soni	48

3.3.5. MAC darajasining ishlatilishi

Yuqorida ko'rganimizdek, IEEE 802.16 standartining fizik darajasi radiokanal bo'yicha BS va AQ orasida ma'lumotlarni almashtirish vazifasini bajaradi. MAC-darajada bu ma'lumotlarning tuzilmasini shakllantirishga bog'liq funksiyalar, shuningdek, WIMAX tizimi ishini boshqarish ishlatiladi. IEEE 802.16 standarti jihozi turli ilovalar (servislar) uchun transport muhitini shakllantirishga chaqirilgan, shuning uchun standartdagi birinchi yechiladigan masala bu yuqori darajalar xilma-xil servislarini qo'llab-quvvatlash mexanizmi bo'ldi. Shuning uchun standartni ishlab chiquvchilar vazifasi barcha ilovalar uchun fizik darajaning qurilishini o'ziga xos bo'lgan xususiyatlariga bog'liq bo'lmagan MAC darajasining yagona protokolini yaratish bo'ldi.

O'z navbatida IEEE 802.16 standartining MAC-darajasi uchta nimdarajaga bo'linadi (chiquvchi bo'yicha):

- SS (ingl. *Convergence Sublayer*) - servisni o'zgartirish nimdarajasi;
- CPS (ingl. *Common Part Sublayer*) - asosiy nimdaraja;
- PS (ingl. *Privacy Sublayer*) - himoya nimdarajasi.

SS nimdarajada IEEE 802.16 tarmog'i orqali uzatish uchun yuqori darajadan ma'lumotlar oqimlarini transformatsiyalash amalga oshiriladi. IEEE 802.16 standartida hozircha ikkita servis pultlari turlari ATM va paketli uzatish (IP, Ethernet, virtual-VLAN) tavsiflangan. SS nimdarajaning maqsadi bu xususiyatlari hisobga olinganda yuqori daraja ilovalarini uzatishni optimallashtirishdir. Shuning uchun SS nimdarajasining muhim vazifasi paketlarni tasniflash hisoblanadi. SRS asosiy nimdarajaning asosiy vazifasi yagona uzatish muhiti-radioefirga ko'plab foydalanuvchilarga ulanishni ta'minlash hisoblanadi. Bunda 2 ta topologiya ishlatilishi mumkin:

- faqat BS-AQ aloqasi mavjud bo'lgan "nuqta-ko'p nuqta topologiyasi";

- BS-AQ aloqasidan tashqari, AQ-AQ to‘g‘ridan-to‘g‘ri aloqa mavjud bo‘lgan “mesh-topologiya” topologiyasi”.

PS himoya nimdarajasida ma’lumotlarni kripto himoyalash funksiyasi va sanksiyalanmagan ulanishni autentifikatsiyalash/oldini olish mexanizmlari ishlatiladi.

IEEE 802.16 standartida “servis oqimi” tushunchasi va unga bog‘liq bo‘lgan “ulanish”, “ulanish identifikatori” va “servis sinfi” tushunchalari ishlatiladi. IEEE 802.16 standartida servis oqimi deganda ma’lum ilovaga (servisga) bog‘liq bo‘lgan ma’lumotlar oqimi tushuniladi. Mos ravishda servis oqimiga QoS bo‘yicha ya’ni kanalning talab etiladigan o‘tkazish qobiliyatiga, ilg‘orlik darajasiga (1 dan 7 gacha), javob ta’sirining ulanish vaqtiga va djitter darajasiga talablar qo‘yiladi. Tarmoqdagi har bir servis oqimi maxsus servis oqimiga bog‘liq bo‘lgan zarur ulanish parametrlarini BS-AQ o‘rnatishiga asoslanib o‘z SFID (ingl. *Service Flow ID*) 32 razryadli identifikatoriga ega bo‘ladi.

IEEE 802.16 terminologiyasida “ulanish” tushunchasi (shuningdek, “transport ulanish” atamasini ishlatiladi) servis oqimini uzatish uchun MAS-darajada mantiqiy aloqaning o‘rnatilishini bildiradi. Har bir ulanish turi va xarakteristikasiga bog‘liq bo‘lgan o‘z SID (ingl. *Connection ID*) 16 razryadli identifikatoriga ega bo‘ladi. Har bir AQga tarmoqdagi boshlang‘ich initsializatsiyada uchta darajadagi xizmat xabarlar uchun uchtadan SID tayinlanadi. Shunday qilib AQ turli ilovalar uchun (masalan, telefoniya, televideniya, Internetga ulanish yoki korporativ tarmoq uchun) ko‘plab turli ulanishlarni o‘rnatish mumkin. Bu ilovalardan har birini QoS ma’lumotlarini uzatish tezligiga SID orqali o‘z talablarini qo‘yadi va BS mos SFID tarmoq oqimini tashkil etadi.

Tarmoqdagi ishini umumiy standartlashtirish uchun “servis sinfi” tushunchasidan, standart ilovalar, masalan, E1 telefon kanallarini translyatsiyalash uchun parametrlar barqaror foydalaniladi.

Servis oqimining parametrlarini ularning ma’lum servis sinfiga tegishlilikini ko‘rsatish bilan berish mumkin.

IEEE 802.16 standarti to‘lig‘icha paketli kommutatsiyaga asoslangan. CPS asosiy nimdarajada MAC PDU (ingl. *MAC Protocol Data Unit* – MAC protokoli ma’lumotlari bloki) ma’lumotlar paketlari shakllantiriladi. Keyin ular fizik darajaga uzatiladi, fizik paketlarga inkapsulyasiyalanadi va radiokanal orqali translyatsiyalanadi (uzatiladi). MAC PDU paketi (keyinchalik PDU) umumiy sarlavha va

ma'lumotlar maydonini (u bo'lmasligi ham mumkin) o'z ichiga oladi, ulardan keyin CRC nazorat yig'indisi kelishi mumkin (3.14- rasm).

Umumiy MAS sarlavha	Ma'lumotlar maydoni	CRC nazorat yig'indisi
---------------------	---------------------	------------------------

3.14- rasm. IEEE 802.16 ning MAC-darajali paketi

PDU sarlavha 6 baytni egallaydi va ikki turda umumiy va o'tkazish oraliq'ini so'rov sarlavhasi (O'OSS) bo'lishi mumkin. Umumiy sarlavha ma'lumotlar maydoni bo'lgan paketlarda ishlatiladi. Bu sarlavha CID ulanish identifikatori, sarlavhaning turi va nazorat yig'indisi ko'rsatiladi, shuningdek, ma'lumotlar maydonida nimsarlavhalar va ARQ teskari aloqa xabarlar mavjudligi haqida axborotlar keltiriladi [1].

O'OSS AQ BSdan "yuqoriga" kanalda o'tkazish polosasini ajratish yoki oshirish haqida so'ragan hollarda qo'llaniladi. Bunda sarlavha CID va talab qilinadigan polosaning o'lchami (fizik paketlar sarlavhalarini hisobga olmasdan, baytlarda) ko'rsatiladi.

Ma'lumotlar maydoni MAS nimsarlavhalari, boshqaruvchi xabarlar va CS nimdarajada o'zgartirilgan yuqori darajalar ilovalari ma'lumotlaridan iborat. MAS nimdarajalari beshta turda qadoqlash, fragmentatsiya, kanalning taqdim etilishini boshqarish, shuningdek Mesh – tarmoq nimsarlavhalari va tez teskari aloqa kanali (ingl. *Fast Feedback*) bo'lishi mumkin. Boshqaruvchi xabarlar bu IEEE 802.16 tizimini asosiy boshqarish mexanizmi hisoblanadi. Ular orqali barcha boshqarish, ruxsat etishni taqdim etish, so'rov va tasdiqlash (masalan, paketlar trafiklari tavsifi, ruxsat etishni boshqarish, kripto himoya mexanizmlari, tizim ishini dinamik o'zgartirish va boshqalar) ishlatiladi. «pastga»/"yuqoriga" kanallar kartalari ham (UL-MAP/DL-MAP) boshqaruvchi xabarlar hisoblanadi. Umuman 256 turdagi boshqaruvchi xabarlar zaxiralangan, ulardan 48 tasi ishlatiladi. Boshqaruvchi xabarlar formati oddiy bo'lib, u xabar turi maydoni (1 bayt) va ixtiyoriy uzunlikdagi ma'lumotlar (parametrlar) maydonidan iborat.

IEEE 802.16 standartida so'rov bo'yicha kanalga ruxsat etishni taqdim etish uslubi ishlatiladi (ingl. *Demand Assigned Multiple Access, DAMA*). Bunda kanalga ruxsat etish AQ dan oldindan so'rov bo'yicha faqat bazaviy stansiya tomonidan taqdim etildi. Bunda BS

AAQ ga «yuqoriga» kanalda vaqt intervalini ajratadi va uning UL-MAP kartadagi joylashishini ko'rsatadi, AQ ning boshlang'ich initsializatsiyasi va kanalga so'rov aniq ruxsat etish mexanizmi asosida ular uchun maxsus ajratilgan vaqt intervallarida amalga oshadi. BS AQ ga SFID servis oqimi turiga bog'liq ravishda kanalga ruxsat etish vaqtini va davomiyligini tayinlaydi. AQ ham kanaldagi ma'lum polosa o'lchamini so'rashi, ham unga berilgan kanal resursini o'zgartilishi haqida so'rashi mumkin. Aniq AQning kanal resursi AQ tomonidan maxsus boshqaruvchi xabarlar yordamida yoki kanal resurslariga barcha AQLardagi zarurat borligiga BS tomonidan so'rovlar (ingl. *polling*) orqali navbatdagi ulanishda o'zgarishi mumkin.

Standartda ikkita har bir alohida bog'lanish uchun va ma'lum AQning barcha ulanishlar uchun ruxsat etish rejimlari ko'zda tutilgan. Birinchi rejimda kanal resurslaridan foydalanishda katta ixchamlik va tejamkorlik ta'minlanadi. Ikkinchi rejim xizmat axborotlari sig'imini sezilarli kamaytiradi va alohida AQ uchun QoS yagona darajasini kafolatlaydi.

3.3.6. QoS - xizmat ko'rsatish sifati

IEEE 802.16 standartida QoS parametrlari ma'lumotlarni uzatish bo'yicha ma'lum xizmat ko'rsatish darajalari bilan (ingl. *Data Delivery Service, DDS*) asoslanadi. DDS darajalari quyidagilarga bo'linadi [4]:

- Servisni so'zsiz taqdim etish (ingl. *Unsolicited Grant Service, UGS*) ma'lum davriylik shakllantirilgan qayd etilgan o'lchamlardagi paketlardan iborat ma'lumotlar paketlarini real vaqt rejimida uzatish uchun mo'ljallangan (masalan T1/E1 tovush kanallari yoki "IP bo'yicha tovushlar" (VoIP) kanallari);

- Real vaqt ko'lamida servisni taqdim etish (ingl. *Real Time Variable Rate, RT-VR*) ma'lum davriylikda shakllantirilgan o'zgaruvchan o'lchamli paketlarning uzatilishini ko'zda tutadi;

- Shuningdek, "Real vaqt qo'lamida servislarni kengaytirib taqdim etish" (ingl. *Extended Real-Time Variable-Rate, ERT - VR*) qo'shimcha darajasi mavjud. ERT – VR darajasi UGS va RT-VR xizmatlarning kombinatsiyasi hisoblanadi. Uning vazifasi kafolatlangan uzatish tezliklari va kechikish vaqti qiymatlarini talab

qiladigan, lekin o'zgaruvchan tezlik bilan xarakterlanadigan yuqori ilg'or ilovalar hisoblanadi (masalan, IP–telefoniya);

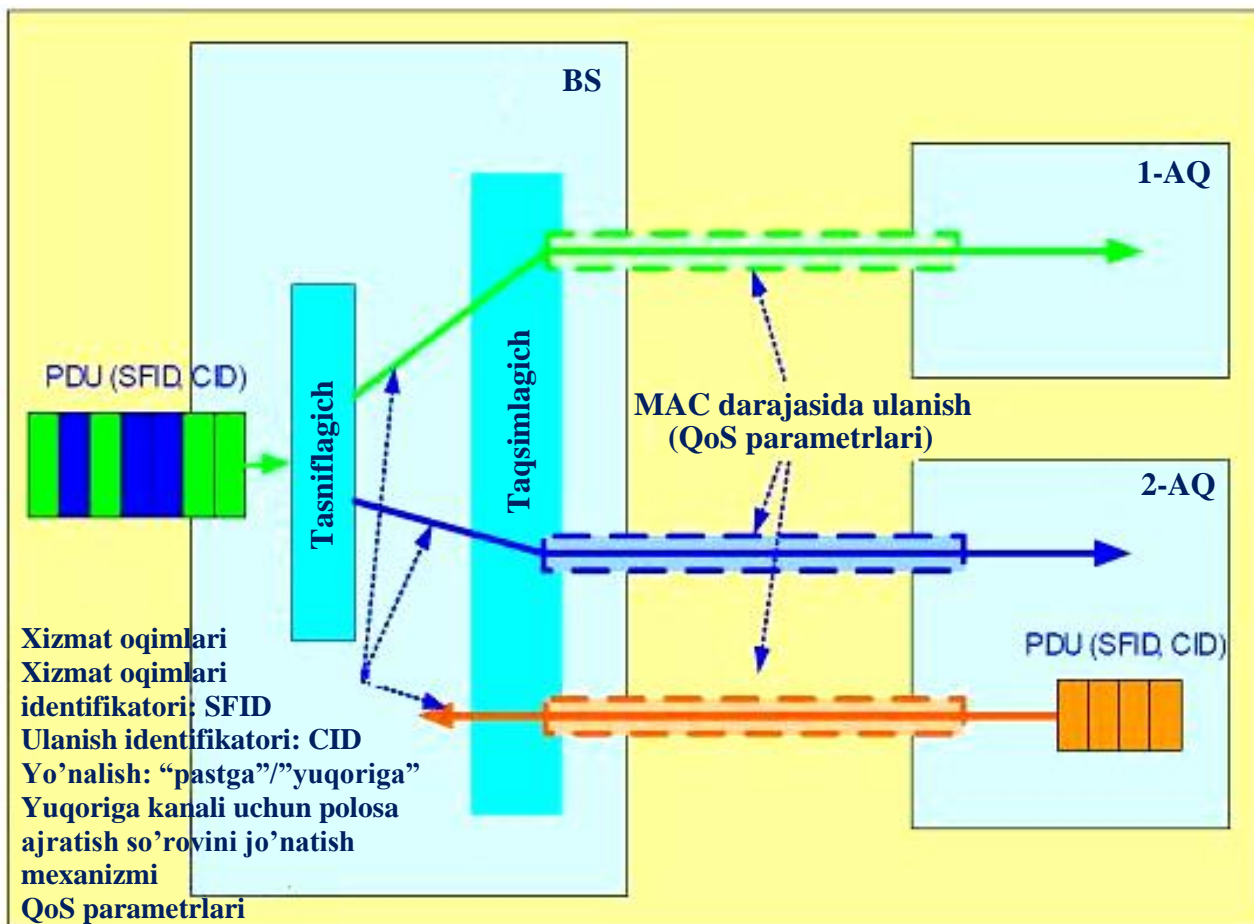
– Real bo'lmagan vaqt qo'lamida servisni taqdim etish (ingl. *Non Real-Time Variable-Rate*) minimal uzatish tezliklarini talab qiladigan va o'zgaruvchan o'lchamlarni paketlarga ega bo'lgan, vaqt kechiktirishlariga kritik bo'lmagan ma'lumotlarni uzatish uchun foydalaniladi (masalan, FTP fayllari);

– “Imkoniyat bo'yicha” servis (ingl. *Best Effort, BE*) kafolatlangan uzatish kanallarini talab qilmaydigan va ularni bo'sh slotlar paydo bo'lishi bo'yicha uzatish mumkin bo'lgan ma'lumotlar oqimini uzatish uchun mo'ljallangan.

IEEE 802.16 standarti “mobil” versiyasining paydo bo'lishi WiMAX tarmoqlarida o'z talablarini va QoS xizmat ko'rsatish sifatiga talablarni aniqlashtirdi. Radioruxsat etish tarmog'i yuqori o'tkazish qobiliyati, assimetrik «pastga»/»yuqoriga» trafik xizmat ko'rsatish imkoniyati, kanallarni kasrlashtirilgan tuzilmasi va kanal resurslarini taqsimlashning ixcham mexanizmi turli ilovali va servisli mobil WiMAX ning samarali ishlashini ta'minlaydi.

IEEE 802.16e standartida QoS xizmat ko'rsatish sifati MAS darajadagi servis oqimlari hisobiga ham ta'minlanadi. Bu 3.15-rasmda keltirilgan [4].

Mobillik va rouming imkoniyatlarining paydo bo'lishi bilan IEEE 802.16e standartida “global servis sinfi” tushunchasi kiritildi. Mavjud servis sinfi tushunchasidan u shunday farqlanadiki, global servis sinfi nomi barcha BS lar uchun yagona va o'zgarmas bo'lib qoldi va hech qanday alohida BS uni o'zgartira olmaydi. Shunday qilib, global servis sinfi bu global tarmoq doirasidagi QoSni boshqarish quroli yoki bir necha tarmoqlarni birlashtirilishda hisoblanadi. Global servis sinfi nomi 32 bit uzunlikdagi sakkizta parametrlar (yana bitta zahirada) to'plami hisoblanadi.



3.15- rasm. IEEE standartida QoSni qo'llash

3.3.7. Mobillikni boshqarish

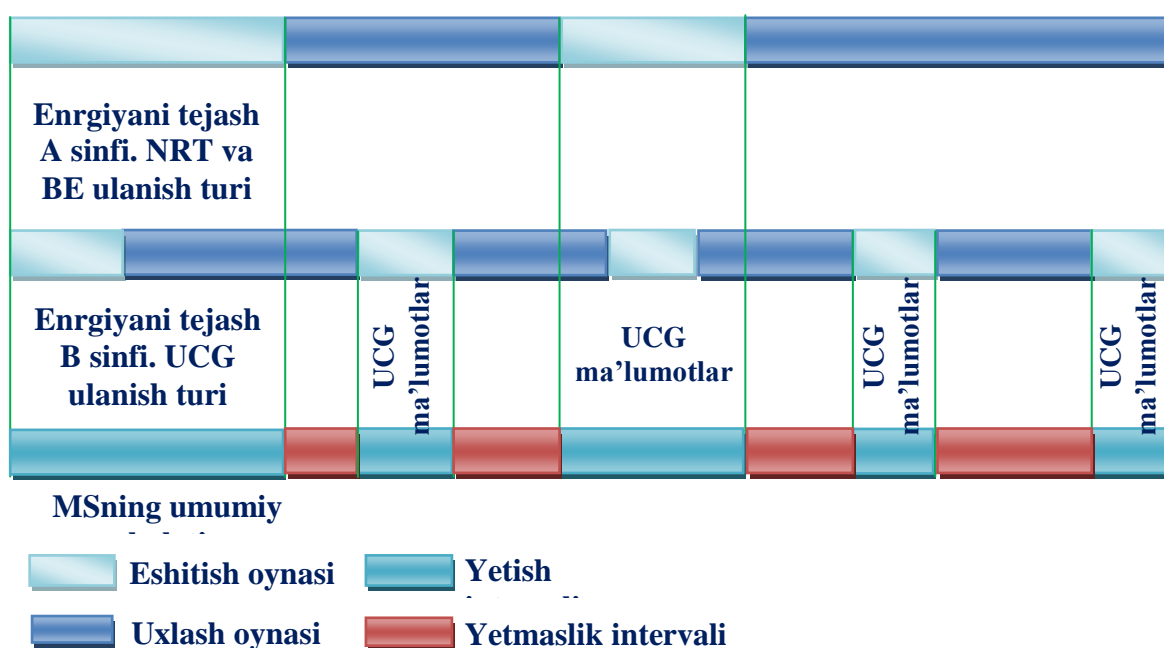
Ko'rinib turibdiki, mobillikni boshqarish funksiyasi faqat IEEE 802.16e standarti uchun dolzarb emas. Abonent qurilmalarining mobillik deganda ko'pincha "xendover"ni tashkil etish bo'yicha choralar va AQ batareyalarining xizmat muddatini oshirish tushuniladi.

"Mobil" WiMAX da energiyani tejash nuqtai nazaridan ikkita uxlash (ingl. *Sleep Mode*) va kutish (ingl. *Idle Mode*) rejimlarini qo'llab-quvatlaydi.

1) **Uyqu rejimi** har bir BS ni qo'llab-quvatlash uchun majburiy va AQ uchun opsional. Uyqu rejimida BS bilan moslashtirilgan AQ vaqt intervalida BSdan uziladi (bunda BS da ro'yxatdan o'tgan holda qoladi), bu radiointerfeys resurslarini va AQ batareyasi energiyasini tejashga imkon beradi. Bunda AQda ma'lum davriy protseduralarga ruxsat etiladi, masalan, ishlov berish (aloqa kanalidagi sharoitlarni va

mos parametrlar bo‘lgan kechikish vaqti, nurlanish quvvati va boshqalarni aniqlash). Uyqu rejimida etish (ingl. *Unavailability Interval*) etmaslik interval bilan (*Availability Interval*) va bu intervallarda AQning o‘zini tutishi uning ishlashi oddiy rejimdan hech qanday farq qilmaydi (3.16- rasm).

Yetmaslik intervalida AQ BSdan hech qanday ma’lumotlarni olmaydi, bu davrda kelgan ma’lumotlar esa o‘chiriladi yoki AQning yetish davrigacha keyingi uzatish uchun BSda o‘zgartiriladi. Yetmaslik intervali o‘z navbatida navbat almashadigan eshitish (ingl. *Listen Window*) va uyqu (ingl. *Sleep Window*) oynalaridan iborat.



3.16- rasm. Ikkita energiyani tejash sinflarini AQ ni ishlashiga misol

Listen va Sleep oynalarining navbat almashishi parametrlari PSC (ingl. *Power Saving Class*) energiyani tejash sinflari bilan xarakterlanadi. Har bir aktiv ulanish uchun o‘z PSC sinfi tayinlanadi. Quyidagi uchta PSC sinfi qo‘llaniladi:

- **1 sinf** BE, NRT-VR QoS darajalar bilan ulanish uchun tavsiya qilinadi. 1 sinfda Sleep oynasi har bir bilan oshadi (masalan, ikkilanadi), lekin ma’lum chegaradan ortmaydi. Listen oynasi vaqtida BS AQga uzatishni kutayotgan unga manzillashtirilgan ma’lumotlarning mavjudligi xabar qiladi. AQ bunday xabarni qabul

qilib BSGa BR (ingl. *Bandwidth Request*) kanalini ajratilishiga so‘rovni yuboradi.

•**2 sinf** UGS, RT-VR QoS darajalar bilan ulanish uchun tavsiya qilinadi. Unda ketma-ket navbat almashadigan Sleep va Listen oynalari doimo bir xil uzunlikka ega. 1 sinfdan farqli ravishda bu sinfdan AQ Listen oynasi vaqtida ma’lumotlarni olishi va uzatishi mumkin.

•**3 sinf.** Guruhli uzatish uchun (multicast), shuningdek, davriy ishlov berish boshqaruvchi xabarlarini va xizmatlarni dinamik o‘zgartirish va boshqalar uchun tavsiya qilinadi. Masalan, agar BS guruhli ko‘rsatish uchun ma’lumotlarni kelish davriyligini bilsa, u holda butun bu davr mobaynida BS AQga 3 sinfdagi uxlash rejimini tayinlaydi.

Har bir AQ bir necha PSC sinflari bilan bir vaqtda ulanishni qo‘llab- quvatlaydi. Agar AQda o‘rnatilgan ulanish hech qanday PSC sinfiga tegishli bo‘lmasa, u holda bu ulanish doimo aktiv hisoblanadi (ya’ni, unda Sleep oynasi bo‘lmaydi). Uxlash rejimini aktivlashtirish (shuningdek, noaktivlashtirish) PSC sinfi va uning parametrlari ko‘rsatilgan AQdan xabar orqali amalga oshiriladi. Javob xabarida BS uxlash rejimini aktivlashtirish haqida xabarga (manfiy va salbiy javob bilan) javob beradi va shuningdek, uning parametrlarini aniqlaydi. Uxlash rejimidan chiqish ma’lum hodisalar (masalan, BS dan signalni maksimal qiymatini detektorlash) yoki jadval bo‘yicha maxsus boshqarish xabari orqali bo‘lishi mumkin.

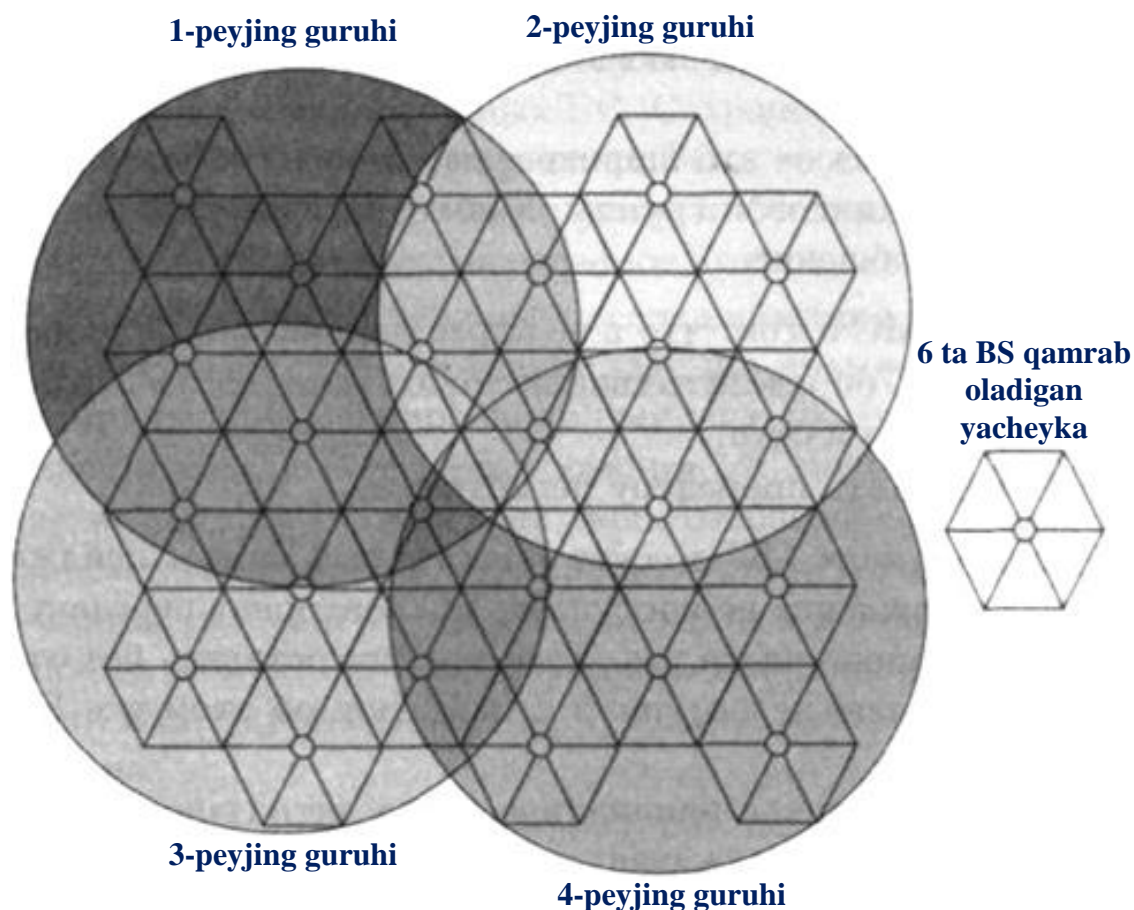
2) Ma’lumotlarni almashtirish bo‘lmaganida AQ kutish rejimiga o‘tishi mumkin (AQni bu rejimni qo‘llab-quvatlashi majburiy bo‘lmasada). Bu rejimda AQ faqat keng uzatishli kanaldan BS dan keladigan axborotlarni davriy ravishda eshitadi. Bunda AQ uchun u joylashgan ta’sir etish (ishlash) zonasida (hududida) BSda ro‘yxatdan o‘tkazishga zarurat yo‘q. Masalan, AQ ko‘p sonli BSlarni uzun hududda harakatlanganida axborotlarni uzatmasligi va BS uning manziliga trafik kelgan haqida maxsus xabar bilan uni chaqirmaguncha massiv kelishi mumkin.

Bu “xendover” protsedurasini bo‘lmasligini va aktiv bo‘lmagan rejimda joylashgan abonent qurilmalarining radioresurslarni ishlatishini kamaytirish imkoniyatini beradi. AQ uchun ma’lumotlar kelganida BS “peydjing” (ingl. *Paging*) keng uzatishli kanal bo‘yicha xabar yuboradi. Kutish rejimini ishlatish uchun barcha BS lar ma’lum mintaqani radio qamrab olishni ta’minlaydigan o‘z IOlarli (LTE

tizimidagi *Tracking Area* kabi) peydjing guruhlarga mantiqiy birlashtiriladi (3.17- rasm).

Bunda AQni chaqirish peydjing guruhga kiradigan barcha BSlarda amalga oshiriladi. Peydjing guruh AQ uning chegaralarida qanchalik uzoq qolishi uchun yetarlicha katta va guruhlarni o‘zaro qoplashi ortiqcha bo‘lmasligi uchun yetarlicha kichik bo‘lishi kerak. Kutish rejimida bo‘lgan AQ davriy ravishda Bsdan peydjing uchun intervalni eshitadi.

Peydjing intervallari peydjing uchun yetarli bo‘lmagan intervallar bilan almashadi. U davomida AQ ta‘minotni kamaytirishi yoki qo‘shni BSlarni skanerlashi yoki ishlov berishni amalga oshirishi mumkin.



3.17-rasm. BSni peydjing guruhlarga bo‘linishi

AQ harakatlanganida radiokanalning yaqin RSCI, CINF xarakteristikalarini BS ni tanlashni amalga oshiradi. AQ kutish rejimida bo‘lganida o‘zi joylashgan o‘rni haqida xabar qiladi (ingl. *Location Update*) yoki o‘z xohishiga ko‘ra, yoki quyidagi hollarda:

- AQ joylashgan BS ta'sir etish (ishlash) hududi yangi peydjning guruhiga tegishliligi aniqlansa;
- kutish rejimining tugashi bo'yicha (4096 sekund);
- chaqiruvlar guruhidan AQ haqida axborotlar o'chirilganda AQning o'chirilishida;
- bu AQga tegishli bo'lmagan BS tomonida peydjning chaqiruvlari soni bo'yicha chegaralarga yetganida (inglizcha, "*MAC hash skip threshold*" deb nomlangan protsedurasi).

IEEE 802.16e standartida AQ joylashgan o'rni haqida ma'lumotlarni ikkita yangilanishi turini qo'llaydi (ingl. *Location Update, LU*):

- himoyalangan – BS va AQ orasidagi xizmat axborotlarini himoyalash aktivlashtirilgan;
- himoyalanganmagan – BS va AQ kontekstni aktiv himoyalashga ega emas yoki BS u yoki bu sabablarga ko'ra LU himoyalangan turni tanlaydi.

Tarmoqda kutish rejimini qo'llab-quvvatlashning barcha funksiyalarini maxsus tugun bo'lgan peydjning nazoratchisi bajaradi. Nazoratchi (kontroller) barcha BS larga kutish rejimida bo'lgan AQLar ro'yxati bo'lgan maxsus xabarlarini yuboradi, uni aktiv rejimga tez qaytarish uchun ma'lum vaqt intervalida AQLar haqida ma'lumotlarni saqlaydi, shuningdek, tarmoqning boshqa nuqtasida AQni qayta ro'yxatdan o'tgani haqida BSga xabar qiladi.

IEEE 802.16e standartida tarmoqning tayanch modeli mobillikni boshqarishni ikki turini qo'llab-quvvatlaydi:

- ASN (ingl. *ASN anchored mobility*) boshqaradigan mobillik;
- CSN (ingl. *CSN anchored mobility*) boshqaradigan mobillik.

ASN boshqaradigan mobillik bitta ASN shlyuz bilan boshqariladigan AQ BS lar chegaralarida harakatlanadigan hollarda qo'llaniladi (ya'ni "mikromobillik"). Bunda "xendoverni" ta'minlash bo'yicha funksiya ikkita BS orasida ma'lumotlarni marshrutlashtirish, "xendover" protsedurasini boshqarish, kontekstni uzatish/yangilash, ma'lumotlarni buferlashtirish va boshqalarni qo'shganda ASN darajada bajariladi. CSN tuguni bu protsedurada hech qanday ishtirok etmaydi va AQ IP manzili o'zgarmasdan qoladi. Qoidaga ko'ra, mobillikni bunday boshqarish turi ko'pincha bo'lib o'tadi [4].

CSN boshqaradigan mobillik turli ASN shlyuzlar bilan boshqariladigan BS lar orasida AQ harakatlanganida ishlatiladi. Bu turning ma'nosi bir R3 tayanch nuqtasidan boshqasiga ma'lumotlarni

marshrutlashtirishdan iborat. Bunda MIP (ingl. *Mobile IP*) protokoli qo‘llaniladi. U IP manzillar o‘zgartirilishsiz tarmoqlar orasida AQni harakatlanishini qo‘llab-quvvatlaydi. Bunda AQ axborotlarni almashtiradigan qurilmalar uning harakatini payqamaydi. MIP protokoli quyidagi funksional komponentlardan foydalanadi:

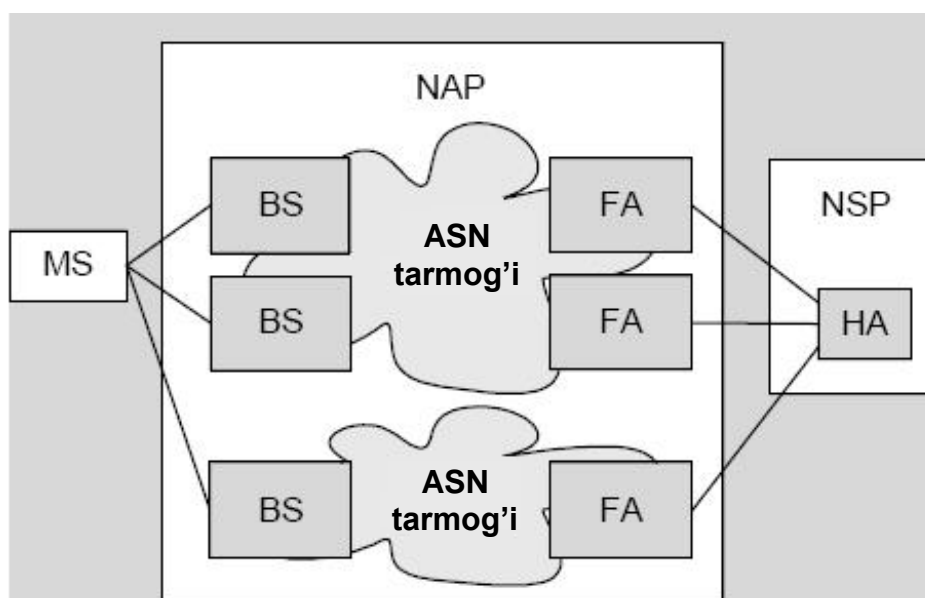
1) MIP mijoz (ingl. *MIP client*). MIP mijozning joylashishiga bog‘liq u ikki turga bo‘linadi:

- MIP protokolini qo‘llab-quvvatlaydigan MIP mijoz AQda ishlatilgan CMIP (ingl. *Client MIP*);

- MIP protokolini qo‘llab-quvvatlash talab qilinmaydigan MIP mijoz ASN tugunida joylashgan va AQ nomidan harakat qiladigan PMIP (ingl. *Proxy MIP*).

2) FA (ingl. *Foreign Agent*) - mehmon tarmog‘i agenti, ASN tugunda joylashgan va uning tarmog‘ida joylashgan barcha AQLar haqida axborotlarga ega bo‘ladi.

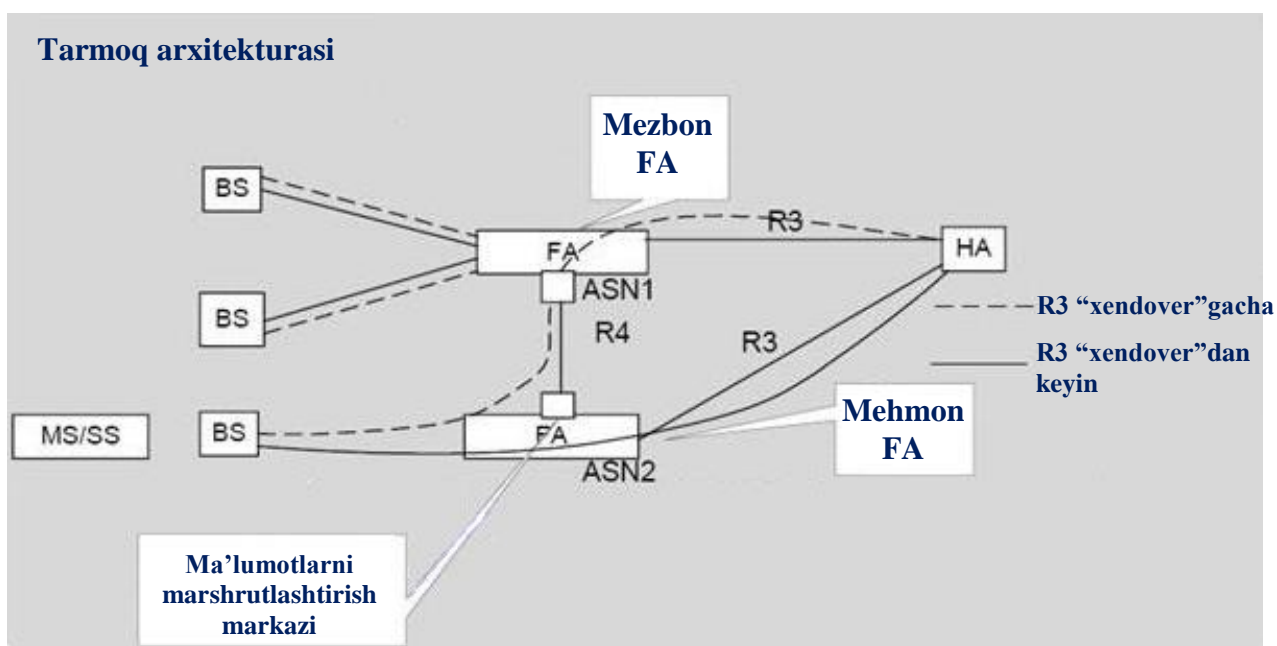
3) HA (ingl. *Home Agent*) – uy tarmog‘i agenti, SSN tugunda joylashgan va SSN boshqaradigan mobillikda yakor (bog‘lovchi markaz) hisoblanadi. NA tugun u kiradigan FA tugun IP manziliga AQning IP manzilining moslik jadvaliga ega bo‘ladi. Shunday qilib, NAda bu A ga mo‘ljallangan paketlarni qayerga (qaysi FA ga) yuborish haqida axborotga ega bo‘ladi. 3.18-rasmda WiMAX tarmog‘ida MIP ning shakllantirilishi keltirilgan.



3.18- rasm. WiMAX tarmog‘ida MIP protokolining shakllantirilishi

NA tugunga kelgan AQ uchun mo'ljallangan paketlar ularni AQga qayta yuboradigan mos FA tugunga qayta yuboriladi. AQ yangi ASNga, ya'ni yangi FA tugunga o'tganida qayta ro'yxatdan o'tkazish protsedurasi amalga oshiriladi. Yangi ASN tugunning MIP mijosi ro'yxatga olishni amalga oshiradi, natijada NA tugundagi jadval yangilanadi. Endi AQ manziliga yangi FA tugunning manzili mos keladi. NA tugun AQga mo'ljallangan paketlarni yangi FA tugunga qayta yuboradi.

SSN va ASN tarmoqlarga bog'liq mobillikni boshqarish turlarining o'zaro ta'sirlashishi 3.19 va 3.20-rasmlarda ko'rsatilgandek, ketma-ket va aralash bo'lishi mumkin.

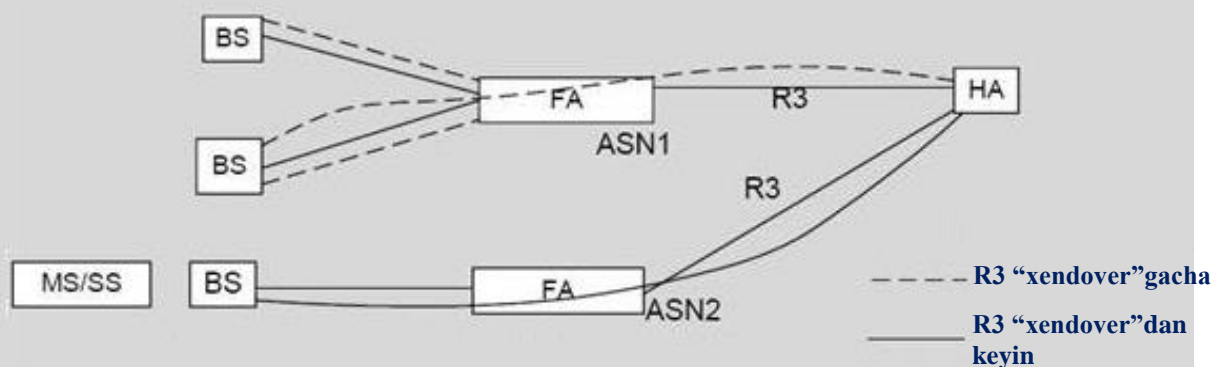


3.19- rasm. Mobillikni boshqarish turlarining ketma-ket o'zaro ta'sirlashishi

Ketma-ket o'zaro ta'sirlashishda AQ bir ASN tarmog'idan boshqa ASN tarmog'iga harakatlanganida dastlab ASN ichida "xendover" bajariladi, keyin SSN turi bo'yicha ASN tarmog'idan boshqa ASN tarmog'iga R3 interfeysi qayta ulanishi amalga oshiriladi. Bu afzal usul hisoblanadi.

Aralash o'zaro ta'sirlashishda AQ bir ASN tarmog'idan boshqa ASN tarmog'iga harakatlanganda R3 tayanch nuqtalarining qayta ulanishi ASN boshqaradigan turlarning protsedurasini bajarilishi jarayonida, masalan, ya'ni ASN tugunda "xendoverga" komandalarni olishda amalga oshiriladi.

Tarmoq arxitekturasi



3.20- rasm. Mobillikni boshqarish turlarining aralash o‘zaro ta’sirlashishi

IEEE 802.16e standartida mobillikni boshqarishning har ikkala turini qo‘llab-quvatlash majburiy. MIP mijoz NA agentda AQni ro‘yxatdan o‘tkazishni va uni FA agent o‘zgarganida, ya’ni AQ boshqa ASN tarmog‘iga o‘tganida qayta ro‘yxatdan o‘tkazishni amalga oshiradi.

AQ ro‘yxatdan o‘tkazish NA agentga qaysi FA tugunga AQ tegishliligi haqida axborotni taqdim etishi bilan tugallanadi.

IEEE 802.16e standarti “xendover” protsedurasini ishlatilishining uchta uslubini qo‘llab-quvvatlaydi.

- “qattiq xendover” (ingl. *Hard Handoff, HHO*);
- BS ni tez qayta ulanishi (ingl. *Fast Base Station Switching, FBSS*);
- makroajratishli “xendover” (ingl. *Macro Diversity Handover, MDHO*).

Ulardan faqat “dag‘al xendover” usuli majburiy, BS tez qayta ulanishi va makroajratishli “xendover” usullari opsional hisoblanadi. WiMAX Forumi tomonidan IEEE 802.16e standarti spetsifikatsiyalari doirasida “dag‘al xendover” protsedurasini optimallashtirish uchun bir necha mexanizmlar ishlab chiqildi. Takomillashtirish avvalo 50 msdan kam “xendover”da 2 darajada javob ta’sirni ushlanishi vaqtini qisqartirish maqsadida bo‘ldi. “Qattiq xendover” protsedurasini atroflicha ko‘rib chiqamiz [8].

AQ bir BSdan boshqasiga qayta ulanishidan oldin, unga yangi BS ni topishi va tanlashi kerak. AQ uchun qo‘shni BS larni qidirishini osonlashtirish uchun mobillikni qo‘llab-quvatlaydigan har bir BS

qo'shnilarni taqdim etish bo'yicha maxsus xabarni davriy ravishda yuboradi (ingl. *Neighbor Advertisement*). Bu xabarda barcha qo'shni BSlar va ularning profili, ish rejimlarini (masalan, OFDM yoki OFDMA texnologiyasi, FTO' massivi o'lchami, polosa kengligi, kanalning tartib raqami, chastotalar to'plami, antennadagi ekvivalent quvvat va boshqalar), har bir BS uchun "xendover" protsedurasining o'ziga xos xususiyatlari, qo'llab-quvvatlanadigan QoS sinflari va boshqalar sanab o'tiladi. AQ so'rovi bo'yicha xizmat qiladigan BS unga "xendover" uchun AQ qo'shni BSlarni skanerlash davomliliigi bo'lgan maxsus vaqt intervallarini (ya'ni, skanerlash intervallarini) tayinlaydi. Skanerlash intervalлари normal ishlash intervallari bilan navbat almashishi mumkin. Skanerlash intervallarini so'rashda AQ BSlarni (masalan, xizmat ko'rsatuvchi BS ro'yxatidan) ular bilan aloqa shartini u tahlil qiladiganlarini sanab o'tishi mumkin.

Skanerlashda assotsiatsiyalash protsedurasi bo'lishi mumkin. Bu opsional funksiya bo'lib, AQga BS so'raydigan QoS fizik parametrlarini va xossalarini olish va saqlashga imkon beradi. Standart uchta assotsiatsiyalash turlarini aniqlaydi:

0-daraja bu oddiy (koordinatsiyalanmagan) ishlov berish. AQ skanerlash intervallari vaqtida BS ularga o'zining xabari bilan javob beradigan maxsus test xabarlarini qo'shni BS larga yuborish bilan ishlov berish protsedurasini bajaradi. Bunda AQ kanaldagi signal/shovqin nisbatini qabul qilingan signalning quvvatini, javob ta'sirini ushlanish vaqtini va boshqalarni aniqlaydi. Bazaviy stansiyalarga so'rov raqobat asosida berilgan so'rov intervallarida beradi.

1-daraja bu xizmat qiladigan BS skanerlashda qatnashishi ko'zda tutiladigan koordinatsiyalangan assotsiatsiyalash. Ham AQdan so'rov bo'yicha, ham BSning o'zi tayinlangan AQ da ishlatilishi mumkin. Xizmat ko'rsatadigan BS qo'shni BSlardan ular uchun qulay vaqtni ishlov berishga so'raydi. Qo'shni BSlar javoban xizmat ko'rsatadigan BS ga ishlov berishga so'rov va so'rovni uzatish sharti uchun ulkan CDMA-kodni uzatadi. Bu shartlar va CDMA-kodlarni xizmat ko'rsatadigan BS AQga xabar qiladi va buning o'zi berilgan vaqtda qo'shni BSlar bilan aloqa qiladi.

2-daraja bu tarmoq bo'yicha bildirishli assotsiatsiyalash bo'lib, u koordinatsiyalangan assotsiatsiyalashga o'xshash, lekin ishlov berishda AQga faqat CDMA-kodni uzatish yetarliligi va qo'shni BSlardan javobni kutishning kerak emasligi bilan farq qiladi. Barcha

qo‘shni BS lar so‘rovni olib xizmat ko‘rsatadigan BS AQsidan aloqa kanalining fizik parametrlari haqidagi axborotlarni uzatadi, xizmat ko‘rsatadigan BS bu axborotlarni to‘playdi va AQga bitta xabarda uzatadi.

Skanerlash va assotsiatsiyalash protseduralari bevosita “xendoverga” olib keladi va qo‘shni BSlar ro‘yxatini shakllantirishga va navbatdagi ulanish uchun ulardan birini tanlashga imkon beradi. “Xendover” protsedurasining o‘zi bir necha bosqichlarni o‘z ichiga oladi:

- bevosita skanerlash va assotsiatsiyalash asosida yacheykani tanlash;
- “xendover” boshlanishi haqida qaror va dasturni ishga tushirish;
- tanlangan BS bilan sinxronlashtirish;
- tanlangan BS bilan bog‘lanishni o‘rnatish (ro‘yxatdan o‘tkazish);
- xizmat ko‘rsatadigan BS bilan bog‘lanishni uzish.

AQ “xendoverning” tugatilishini maxsus final xabari bilan tasdiqladi, lekin final xabarini yuborishgacha istalgan momentda “xendover” protsedurasini uza olmaydi. “Xendover” protsedurasining boshlanishi haqidagi qarorni AQ, xizmat ko‘rsatadigan BS yoki tarmoqning boshqarish tizimi qabul qilishi mumkin. BS zarur AQ kanal resurslari va QoS darajasini baholash asosida “xendover”ni amalga oshirishi mumkin. AQga bu talablar xizmat ko‘rsatadigan va ko‘shni BS imkoniyatlariga kiradi. Agar xizmat ko‘rsatadigan BSning o‘z resurlari yetishmasa, ular qo‘shni BSda bo‘lsa, u holda u AQni qo‘shni BSga qayta ulanishiga majburlaydi.

Guruhli va keng-qamrovli uzatish

IEEE 802.16e standartida guruhli uzatish (kam hollarda, ko‘p nuqtali yoki ko‘p uzatishli) tushunchasi (ingl. *Multicast*) va keng-qamrovli uzatish tushunchasi (ingl. *Broadcast*) kiritilgan. Standartda bu tushunchalar birlashtirilgan va yagona *Multicast and Broadcast Service* (MBS) atamasi ishlatiladi. U guruhli va keng-qamrovli uzatish xizmatlarini aniqlaydi. MBS xizmatlari ikkita bir saytli MBS (bir BS dan uzatish) yoki guruhli MBS (bir necha BS lardan uzatish) rejimlarida SFID taqdim etilishi mumkin va AQ har ikkala rejimlarni qo‘llab-quvvatlashi kerak. MBS uzatishlar uchun ARQ teskari aloqa mexanizmi ko‘zda tutilmagan. Oldindan berilgan trafik xossalari va QoSli MBS transport oqimlariga servis oqimlari SFID va mos

ravishda bog‘lanishlar CID identifikatorlari beriladi. Bu identifikatorlar bo‘yicha AQ MBS xizmatlarni taniydi. Bunda agar guruhli uzatish xabarlarini bir necha AQLar inkor qila olsa, u holda keng uzatishli uzatish xabarlarini barcha AQLar qo‘llab-quvvatlashi kerak. Muhimki, MBS xabarlarni AQ “uyqu” va “kutish” rejimlarida ham qabul qila oladi.

Guruhli MBS rejimida bir necha BSLar maxsus guruhni zonani (hududni) tashkil qiladi, uning barcha BSLariga MBS zonasining identifikatori beriladi. MBS zonasidagi barcha BS va AQLar yagona CID dan foydalanadi va barcha BSLar bir chastota kanalida MBS xabarlarni sinxron translyatsiya qiladi (LTEdagi SFN bir chastotali tarmoqlarga o‘xshash). Bir saytli MBS rejimida MBS servisni olish uchun AQ BSda ro‘yxatdan o‘tkazilishi kerak. Guruhli MBS rejimida esa bunday ro‘yxatdan o‘tkazish talab qilinmaydi. Bundan tashqari AQ MBS zonasidagi hech bir BSda ro‘yxatdan o‘tkazilmasligi mumkin va bunda bu servisni olishi mumkin. Bunda AQ tarmoqda bu servisni oluvchi sifatida ro‘yxatdan o‘tkazilishi yetarli bo‘ladi. AQ haqidagi axborot tarmoq infratuzilmasi orqali bazaviy stansiyalarga uzatiladi. Bunda MBS xizmatlarni oluvchini ro‘yxatdan o‘tkazish tarmoq darajasida amalga oshiriladi.

3.4. WiMAX tarmog‘ini tashkil qilishning o‘ziga xos xususiyatlari, ishlash rejimlari va profillari

3.4.1. WiMAX profillari

Umumiy holatda WiMAX tarmog‘i baza stansiyasi va abonent qurilmasi, shuningdek o‘zaro va boshqa umumiy ulanish tarmoqlari bilan aloqa qiluvchi baza stansiyalaridan iborat bo‘ladi. BS va AQ orasida ulanish bir necha rejimda amalga oshiriladi: doimiy(fiksatsiyalangan aloqa), seansli, ko‘chma va mobil. WiMAX tizimi «oxirgi milya» muammolarini hal qilish uchun va uzoqlashtirilgan ob‘ektlar o‘rtasida keng polosali simsiz aloqani ta’minlash uchun qo‘llaniladi [8].

Tarmoqda hech bo‘lmaganda bitta BS simli umumiy foydalanish tarmog‘iga chiqish imkoniga ega bo‘lsa, BSLar o‘rtasida aloqa o‘rnatiladi. IEEE 802.16 standartlar oilasining tarmoq tuzilishi an’anaviy GSM tarmoqlarinikiga o‘xshash bo‘ladi. BS o‘n kilometr masofagacha signal uzatishni amalga oshiradi, BSLarni o‘rnatish

uchun minora zarur emas – BSlarni uylarning tomiga bir-biriga to‘g‘ridan-to‘g‘ri ko‘rinib turadigan qilib o‘rnatish mumkin [10].

3.10- jadval

WiMAX profillari parametrlari

	Turg‘un WiMAX	Evolyutsion WiMAX	Mobil WiMAX	
Standart	IEEE 802.16-2004	IEEE 802.16e-2005	IEEE 802.16e-2005	
Multiplekslash	OFDM	OFDM	OFDMA	
Nimeltuvchilar ning nominal soni	256	256	512, 1024	
Dupleks rejimi	TDD, FDD, HFDD	TDD, FDD, HFDD	TDD	
Modulyatsiya	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM (opsional)	QPSK, 16-QAM, 64-QAM ("yuqoriga" kanalida-opsional)	
Quvvat sinflari, dBm	0 – 14	0 – 14	16-QAM	QPSK
	14 – 17	14 – 17	18 – 21	20 – 23
	17 – 20	17 – 20	21 – 25	23 – 27
	20 – 23	20 – 23	25 – 30	27 – 30
	23 dan yuqori	23 dan yuqori	30 dan yuqori	30 dan yuqori

WiMAX standarti fizik pog‘onasiga tegishli barcha talablarga muvofiq ravishda amaliyotda "WiMAX profili" atamasi qo‘llaniladi. Quyidagi rasmda ko‘rsatilgandek, bir necha WiMAX profillari o‘zaro farqlanadi.

Bundan tashqari, sertifikatlangan profillar ham mavjud bo‘lib, standartlar talablariga mos ravishda har xil qurilmalarni sertifikatlash maqsadida foydalaniladi. Bunda «Plugfest» (ing. *Plugfest*) deb nomlanuvchi uskunadan foydalanib sertifikatlangan profillardan biri asosida WiMAX standartiga qo‘yilgan talablarga mos holda WiMAX Forum laboratoriyalarida qurilmalarni testlash amalga oshiriladi. Vaqt o‘tishi bilan WiMAX standartiga tegishli bo‘lgan profillar takomillashib bormoqda.

2007 yil boshida quyidagi sertifikatlash profillar tavsiflab berildi: 5 profil doimiy aloqali WiMAX uchun va 13 profil mobil WiMAX uchun. Profillardan ba'zilar 3.11-va 3.12- jadvallarda keltirilgan.

3.11- jadval

WiMAX standartining sertifikatlash profillari

WiMAX tizimlari	Sertifikatsiyali profillar			
	Nomi	Chastota diapazoni, GGs	Dupleks	Kanal kengligi, MGs
Turg'un WiMAX (IEEE 802.16-2004, OFDM)	Air1	3,4 – 3,6	TDD	3,5
		3,4 – 3,6	TDD	7
	Air2	3,4 – 3,6	FDD	3,5
		3,4 – 3,6	FDD	7
		5,725 – 5,850	TDD	10
Evolyutsion WiMAX (IEEE 802.16e-2005, OFDM)	ETG8	4,935 – 4,990	TDD	5
Mobil WiMAX (IEEE 802.16e-2005, OFDMA)	1B	2,3 – 2,4	TDD	5 va 10
	1A	2,3 – 2,4	TDD	8,75
	3A	2,496 – 2,690	TDD	5 va 10
	5AL	3,4 – 3,6	TDD	5
	5BL	3,4 – 3,6	TDD	7

3.4.2. WiMAX tarmog'ining ishlash rejimlari

Avval aytib o'tilganidek, hozirgi kunda keng tarqalgan va asosiy standart hisoblanuvchi WiMAX standartining ikkita versiyasi mavjud: IEEE 802.16d va IEEE 802.16e. IEEE 802.16d standarti qayd etilgan aloqali simsiz ulanishni tavsiflaydi va uzoqlashtirilgan stasionar abonentlar ulanishi uchun mo'ljallangan. O'z texnik xarakteristikasiga ko'ra (o'tkazish polosasi 20 MGs chastota polosasida 75 Mbit/sgacha yetadi, aloqa masofasi 50 kmgacha), bu standart turli variantdagi simli keng polosali abonent ulanish usullarining muqobil varianti hisoblanadi.

IEEE 802.16e standarti harakatdagi foydalanuvchilar uchun keng polosali "mobil" xizmatlarni ko'rsatish uchun mo'ljallangan. Ushbu standartda maksimal ma'lumot uzatish tezligi 5 MGs chastota

polosasida 20 Mbit/sni tashkil etadi, aloqa masofasi – 5-10 kmga teng. IEEE 802.16e standarti BS va AQ orasida bog‘lanishda mobillik (harakatchanlik) jihatdan ayniqsa takomillashgan hisoblanib, shuningdek avvalgi barcha standartlarning imkoniyatlarini ham o‘z ichiga oladi va quyidagi rejimlarda ishlaydi.:

- Fiksatsiyalangan aloqali (bir joydan qo‘zg‘almay yoki statsionar holatda) ulanish (ingl. *Fixed WiMAX*);
- Seansli ulanish (ingl. *Nomadic WiMAX*);
- Ko‘chma yoki siljish rejimidagi ulanish (ingl. *Portable WiMAX*);
- Mobil ulanish (ingl. *Mobile WiMAX*).

WiMAX tarmog‘i ishlash rejimlarini batafsil ko‘rib chiqamiz.

Qayd etilgan ulanish

Qayd etilgan ulanish o‘z tuzilishiga ko‘ra simli keng polosali texnologiyalarga (xDSL, T1/E1, optik tolali texnologiyalar) o‘xshash bo‘ladi. Dastlab IEEE 802.16 standarti 10-66 GGs chastota diapazonida ishlash uchun mo‘ljallangan. Ushbu chastota diapazoni radioaloqaning asosiy muammolaridan biri bo‘lgan – radioto‘lqinlarning ko‘p nurli (ko‘p tashkil etuvchili) tarqalishidan saqlanish imkonini beradi. Ushbu chastota diapazonida bu aloqa kanali kengligi bilan 120 Mbit/sdan ortiqroq tezliklarda ma’lumot uzatishga erishish mumkin. Qayd etilgan ulanish rejimi IEEE 802.16d-2004 standarti bilan tavsiflangan. Shuni alohida ta’kidlash lozimki, qayd etilgan ulanish rejimida xizmat ko‘rsatuvchi ko‘pchilik operatorlar to‘liq mobil rejimga o‘tishni yoki ikkala standartni ham bir vaqtda qo‘llashni loyihalashtirmoqdalar.

Seansli ulanish

Seansli ulanish mavjud qayd etilgan ulanish rejimli WiMAX ga seans tushunchasini qo‘shdi. Seansning mavjud bo‘lishi turli baza stansiyalari orqali ulanishni o‘rnatish va ma’lum bir davr orasida AQni erkin ko‘chishiga imkon beradi. Ushbu rejim asosan portativ qurilmalar (masalan, noutbuk, KPK) uchun ishlab chiqilgan va portativ qurilmalar uchun juda muhim bo‘lgan AQ energiya iste’molini kamaytirish imkonini beradi.

Ko‘chma ulanish

Bu rejimda ulanish uchun biror WiMAX baza stansiyasidan boshqa baza stansiyasiga aloqani yo‘qotmagan holda abonentni avtomatik ulashni amalga oshirish imkoniyati qo‘shilgan (rouming). Lekin ushbu rejim uchun AQ harakatlanish tezligi 40 km/soat dan

oshmasligi kerak. Shunday bo'lsa ham, ushbu rejimdan AQ avtomobilda, velosipedda va yayov holatda chegaralangan tezlik bilan harakatlenganda foydalanishi mumkin. Ushbu rejimga kirish smartfon, kommunikator va KPK lar uchun WiMAX texnologiyasidan foydalanishga mos ravishda amalga oshirilgan. Bunday ko'chma ulanishli WiMAX rejimida ishlovchi qurilmalarning chiqishi 2006 yildan boshlandi.

Mobil ulanish

Ma'lumki, ushbu rejim IEEE 802.16e standartida ishlab chiqilgan va AQ 120 km/soat tezlikkacha harakatlenganda barqaror aloqani ta'minlash imkonini berdi. Mobil WiMAX ning asosiy ustunliklari va kamchiliklariga quyidagilar kiradi:

1. Signalning ko'p nurli tarqalishiga va shaxsiy halaqitlarga bardoshliligi.

2. Kanal o'tkazish qobiliyatining kengayuvchanligi.

3. Asimmetrik oqimni tashkillashtiruvchi va antenna tizimlarini samarali boshqarishda foydalanuvchi vaqt bo'yicha signal tarqatish dupleks (TDD).

4. Xizmat ko'rsatish sifati QoSda HARQ texnologiyasidan foydalanilib, AQ harakat chog'ida o'z yo'nalishini o'zgartirganda aloqani ishonchli saqlab turish imkonini beradi.

5. Kutish rejimlarida AQ energiya ta'minotini tejaydi, batareyaning ishlash muddatini uzaytiradi.

6. AQ qayta ulanishini optimallashtirilgan texnologiyasi – HHO kanallar orasida ulanish vaqtini 50 ms gacha qisqartirish imkonini beradi.

7. MBS guruhli va keng polosali xizmat ko'rsatish xizmatlarini ta'minlaydi:

– Bitta chastotada ko'plab foydalanuvchilarga signal uzatishni ta'minlash orqali tarmoqning yuqori samaradorligiga erishish;

– Tarmoqning radiochastota resurslaridan samarali foydalanish;

– Abonent qurilmasining elektr sarfini kamaytirish;

– Kanallar orasida tezkor ulanishlarni amalga oshirish.

8. Chastotani takrorlash usullari minimal yo'qotishlar bilan chastotadan foydalanish uchun kanallarni ustma-ust qo'yish/kesishtirishni boshqarish imkonini beradi.

9. MAC-kadr o'lchami 5msda kichik paketlardan foydalanib ma'lumot uzatish ishonchliligi va paketlar sonini ko'paytirish xarajatlari orasida o'zaro kelishuvni ta'minlaydi.

WiMAX tarmoqlariga mobil holatda ulanish turli darajadagi mobillikni ta'minlovchi har xil abonent qurilmalari bilan ta'minlanadi. Ularga quyidagilar kiradi:

- binolar ichida qo'llanilish uchun qurilmalar, shuningdek ular klient qurilmalari (*Customer Premises Equipment, CPE*) deb nomlanadi;

- Binolar tashqarisida qo'llash uchun qurilmalar, masalan, tashqi WiMAX antennalari;

- Portativ kompyuterlarga o'rnatiladigan PC-kartalar;

- Portativ kompyuterlar ichiga joylashtirilgan WiMAX modullari;

- WiMAX interfeysiga ega cho'ntak kompyuterlar va kommunikatorlar.

WiMAX tarmog'ining har xil ishlash rejimlari asosiy xarakteristikalari 3.12- jadvalda keltirilgan [4].

3.12- jadval

WiMAX tarmoqlarining ishlash rejimlari

Ulanish turi	Uskuna turi	Qurilmalar soni/abonent xarakati tezligi	"Xendover" ni qo'llab-quvvatlash	802.16-2004 ctandarti	802.16a standarti
Turg'un ulanish	Tashqarida va ichkarida joylashgan "xotspot" lar	Yakka uskuna/ turg'un abonent	Yo'q	Ha	Ha
Ko'chma ulanish	Ichkarida joylashgan "xotspot" lar, portativ ShKlar uchun PCMCIA-adapterlar	Ko'p sonli qurilmalar/ abonent turg'un	Yo'q	Ha	Ha
Portativ ulanish	Portativ ShKlar uchun PCMCIA-adapterlar, kichik adapterlar	Ko'p sonli qurilmalar / piyoda tezligi	Dag'al "xendover"	Yo'q	Ha

Asosan mobil ulanish	Portativ ShKlar uchun PCMCIA-adapterlar, kichik adapterlar, KPK, smartfonlar	Ko‘p sonli qurilmalar / kichik tezlikda harakatlanuvchi transport vositasi	Dag‘al “xendover”	Yo‘q	Ha
To‘liq mobil ulanish	Portativ ShKlar uchun PCMCIA-adapterlar, kichik adapterlar, KPK, smartfonlar	Ko‘p sonli qurilmalar / katta tezlikda harakatlanuvchi transport vositasi	Yumshoq “xendover”	Yo‘q	Ha

3.4.3. WiMAX tarmog‘ini tashkil etishning o‘ziga xos xususiyatlari

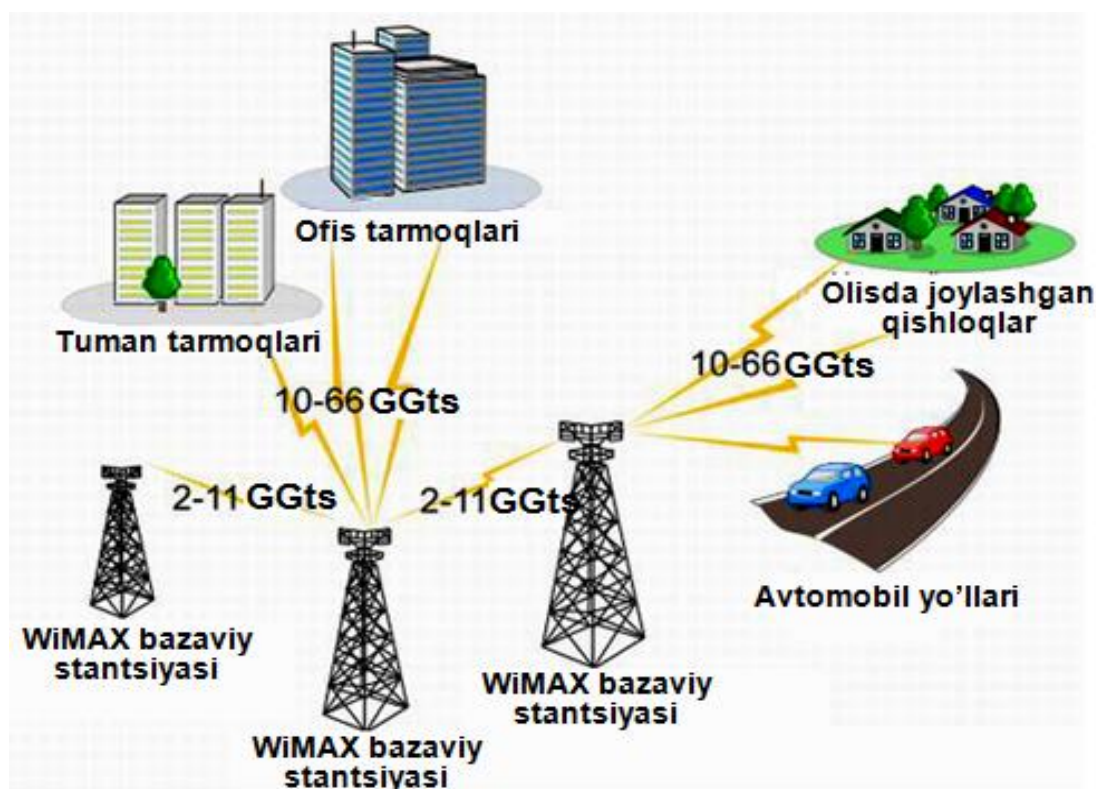
Aytib o‘tilganidek, IEEE802.16 standarti shahar va rayonlar masshtabidagi simsiz tarmoqlarda keng polosali aloqa tashkil qilish mo‘ljallangan (WMAN). Standartning boshqa vazifasi lokal, hududiy va global tarmoqlar o‘rtasida o‘zaro aloqani ta‘minlash hisoblanadi. Bu tarmoqlar, shuningdek simsiz shaxsiy tarmoqlar bilan ham birgalikda ishlaydi hamda simli va simsiz tarmoqlar orasida protokollararo ierarxik bog‘lanishni ta‘minlovchi simsiz ko‘priklarni vujudga keltiradi.

Bu vazifalarni bajarish uchun WiMAX tarmog‘ini tashkil etishning turli variantlari ko‘rib chiqilgan. Umumiy holatda WiMAX tarmog‘i topologiyasi quyidagi ko‘rinishda tasvirlanadi (3.21- rasm.):

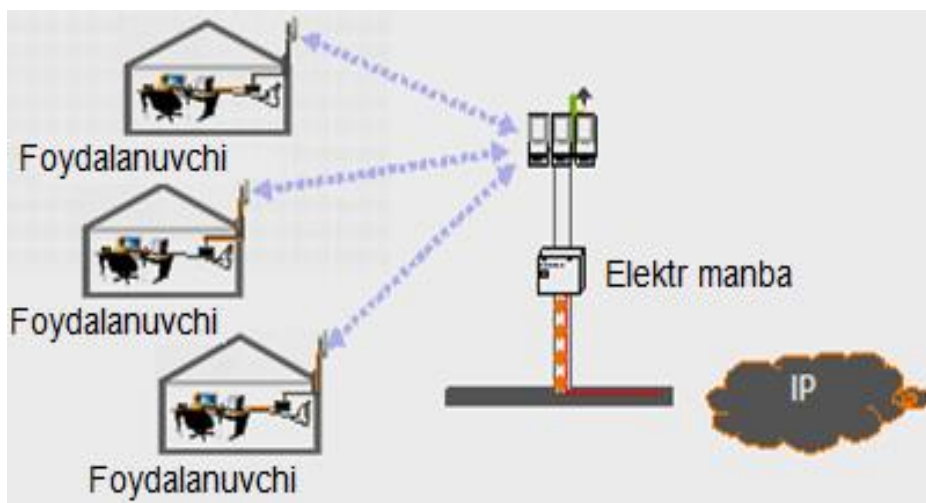
WiMAX tizimlarida avval magistral liniyalarni tashkil etish uchun 10-66 MGs chastota diapazonidan foydalanish ko‘zda tutilgan, hozirgi foydalaniladigan versiyalarida esa 2 dan 11 MGs chastota diapazonida 3,5; 5; 7,5; 8,75 va 10 MGs kanal kengligida ishlaydi. Bunda $\pm 10^{-6}$ chegarada chastota barqarorligini ta‘minlash zarur. Tarmoq baza stansiyalari binolar tomlarida yoki machtalarda joylashtiriladi. Shuningdek, turli baland inshootlardan, simyog‘ochlardan va hattoki, daraxtlardan baza stansiyalarni o‘rnatishda foydalanish mumkin. Biror hududdagi ko‘p sonli abonentlarga simsiz keng polosali ma‘lumotlar uzatish xizmatini taqdim etish uchun WiMAX baza stansiyalari abonent qurilmalari

bilan “nuqta- ko‘p nuqta” topologiyada aloqani amalga oshiradi (3.22-rasm).

Bu chizma bo‘yicha BS WiMAX abonentlari qurilmalari yordamida foydalanuvchilar bilan bog‘lanadilar, keyin signal Ethernet-kabel standarti bo‘yicha yoki to‘g‘ridan-to‘g‘ri aniq kompyuterga yoki IEEE 802.11 (Wi-Fi) ulanish nuqtasi orqali qabul qilinadi. Bu WiMAX orqali kabelli ulanishdan simsiz ulanishga o‘tishda mavjud hudud yoki ofis tizimidagi lokal tarmoqlarning infrastrukturasi saqlab qolish imkonini beradi. Bundan tashqari kompyuterlar ulanishi uchun standart texnologiyalardan foydalanuvchi tarmoqlarni yoyishni maksimal darajada kengaytirish imkonini beradi.



3.21- rasm. WiMAX tarmog‘i topologiyasi



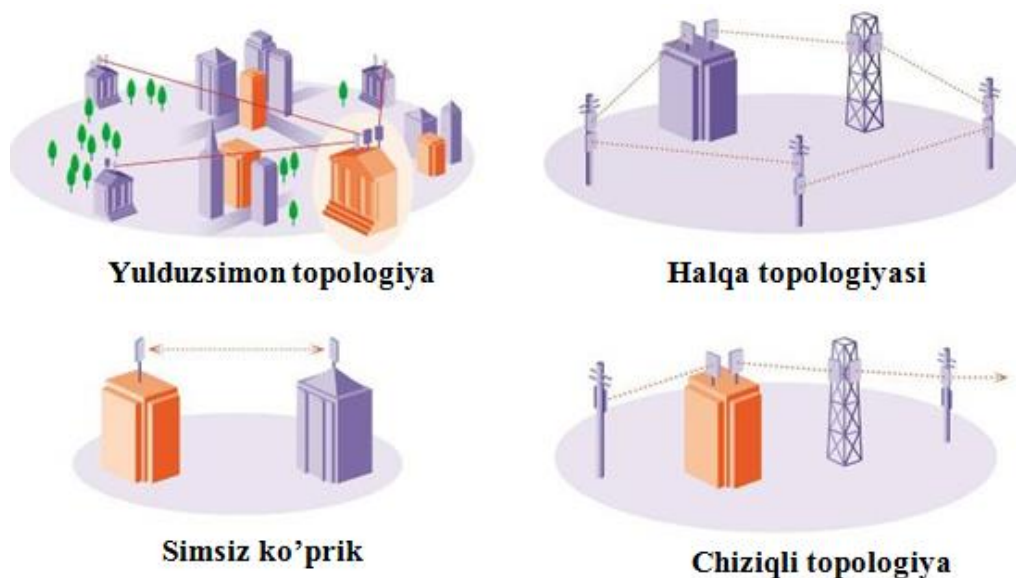
3.22- rasm. «Nuqta-ko‘p nuqta» rejimida WiMAX tarmog‘i topologiyasi

Uzoqlashtirilgan ob‘ektlar orasida simsiz keng polosali aloqani tashkil qilish uchun «nuqta-nuqta» rejimidan foydalaniladi (3.23-rasm).



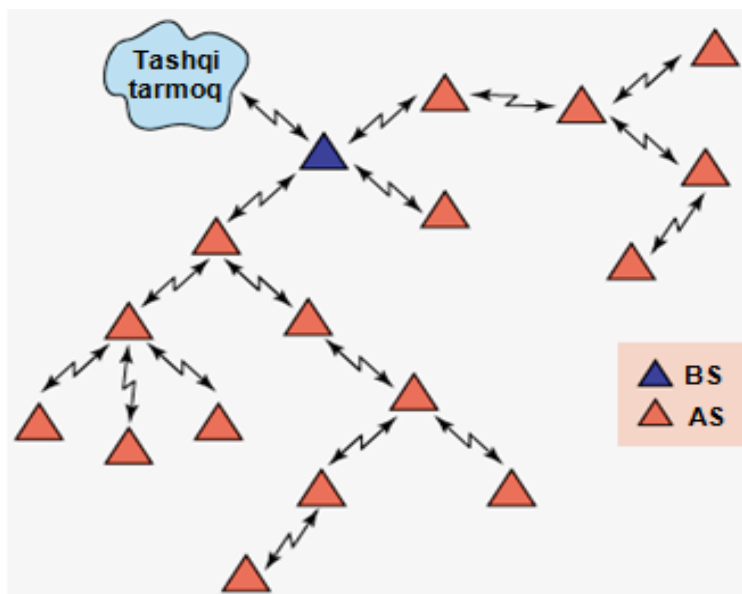
3.23- rasm. “Nuqta-nuqta” rejimidagi WiMAX tarmog‘ining topologiyasi

«Nuqta-nuqta» rejimida turli tarmoq ko‘rinishlari va ularning kombinatsiyalaridan foydalaniladi. 3.24- rasmda WiMAX tizimi uchun qo‘llaniluvchi turli ko‘rinishdagi tarmoq topologiyalari tasvirlangan.



3.24- rasm. “Nuqta-nuqta” rejimidagi WiMAX tarmog‘ining ko‘rinishlari

WiMAX tarmoqlarida shuningdek «**mesh**» rejimida aloqa tashkil qilish mumkin, bunda AQ to‘g‘ridan-to‘g‘ri bir-biri bilan aloqani amalga oshiradi, bazaviy stansiyasi esa asosiy tarmoqlar infrastrukturasida va mesh tarmoqlari o‘rtasida kommutator hisoblanadi. (3.25-rasm). «**Mesh**» rejimini qo‘llash natijasida tarmoqning radioqoplam zonasi yuqori tezlikda ma’lumot uzatishni ta’minlash bilan 50km gacha oshadi, bu holda bitta BSning oddiy holdagi radiusi 5-10 kmni tashkil etadi.

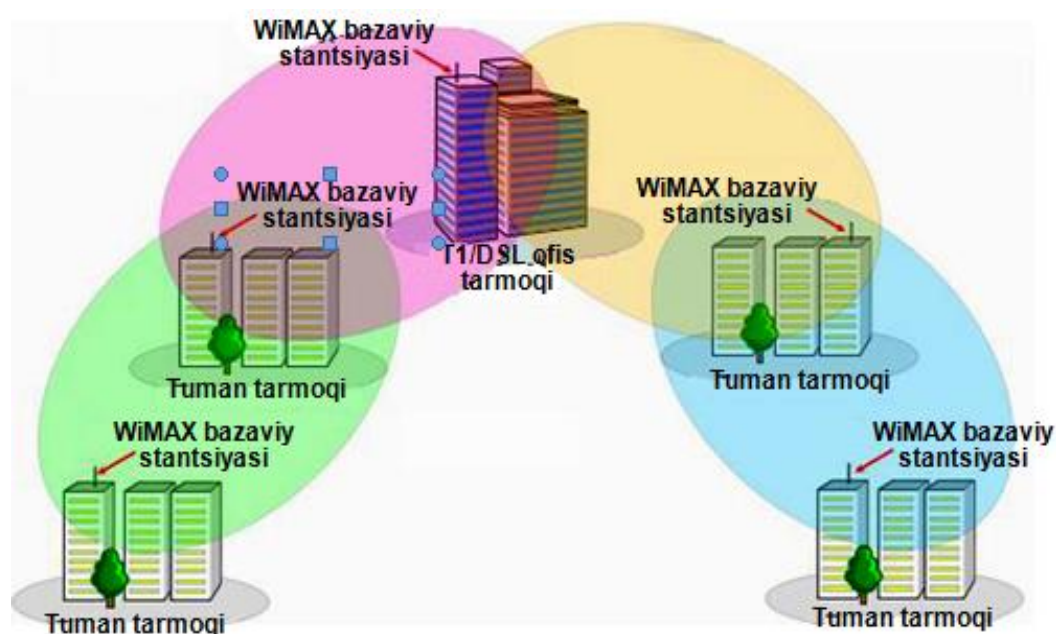


3.25- rasm. «Mesh» rejimida WiMAX tarmog‘i topologiyasi

WiMAX tarmoqlari «ko‘p nuqta - ko‘p nuqta» rejimida qurilishi mumkin, shuningdek u «nuqta-ko‘pnuqta» rejimini ham ta’minlaydi. (3.26-rasm).

Bunda BS lokal trafikni tashkil qilish uchun radioterminal yoki takrorlagich bo‘lishi mumkin. Ma’lumotlar oqimi abonentga yetib borguncha, bir necha takrorlagichlardan o‘tishi mumkin. Bu holatda antenna masofadan sozlanadigan tor yo‘nalishda signal uzatuvchi antenna bo‘ladi. Takrorlagichlar aloqa qilinuvchi nuqtalar orasida to‘g‘ridan-to‘g‘ri aloqa o‘rnatish imkoni bo‘lmagan vaziyatlarda foydalaniladi. Ular BSdan bir yoki bir necha abonent qurilmalariga signal uzatadi.

WiMAX tizimlari qurilmalari o‘z ichiga abonent terminallarini, asosiy tarmoq qurilmalarini, tugunlararo kanallarni va takrorlagichlarni oladi.



3.26- rasm. «Ko‘p nuqta - ko‘p nuqta» rejimidagi WiMAX tarmog‘ining topologiyasi

Abonent qurilmalari

WiMAX tarmoqlarida foydalanish uchun abonent qurilmalari turli ishlab chiqaruvchilar tomonidan ishlab chiqariladi hamda binolar ichida va binolar tashqarisida (noutbuk kabilar) joylashtirilishi mumkin. Shuni alohida ta’kidlash kerakki, binolar ichida joylashtirishga mo‘ljallangan va aloqa o‘rnatishda kasbiy malaka talab

qilmaydigan qurilmalar BS dan uncha katta bo‘lmagan masofalarda ishlash qobiliyatiga ega. Shuning uchun binolar ichida o‘rnatilgan qurilmalar tarmoq infrastrukturasi rivojlantirishda ancha katta investitsiya talab qiladi, ularda BSlarni ko‘proq qo‘llashga to‘g‘ri keladi. Mobil WiMAXning paydo bo‘lishi bilan uning tarmoqlarida aloqani ta‘minlovchi maxsus telefon apparatlari, mobil qurilmalar va kompyuter qurilmalari ishlab chiqarishga katta e‘tibor qaratildi.

O‘zaro ishlash imkoniyatlari va ishlash sifati

WiMAX texnologiyasi katta sonli an‘anaviy tizimlar, simli yoki simsiz tarmoqlar bilan aloqani ta‘minlash maqsadida ishlab chiqilgan (tarmoqlar IPga asoslangan). Ko‘p hollarda bu arxitektura multimediyali IP-tizimlariga (yoki IMS) asoslangan bo‘lib, tarmoqlararo roumingni ta‘minlash, 3G tarmoqlari bilan birgalikda ishlash, IP darajasidagi tarmoqlarda aloqa sifati va xizmatlar to‘plamini ta‘minlash imkonini beradi. IP tarmoqlariga ulanish imkoniyati tufayli WiMAX texnologiyasi boshqa tarmoqlarni kengaytirish “choksiz mobillik” prinsipi bo‘yicha ularni qurish imkoniyatini beradi.

WiMAX texnologiyasi simli tarmoq operatorlariga uzoqlashtirilgan hududlarga ulanish uchun “oxirgi mil” muammolarini hal qilish imkoniyatini beradi, uzoq masofalarga kabel yotqizish kabi ortiqcha xarajatlarni kamaytiradi. IEEE 802.16e standarti mobil aloqa operatorlari xarajatlarini kamaytirishni taklif etadi, mobil aloqa operatorlariga 2G va 3G darajasidagi xizmatlarni, keng polosali ma‘lumot uzatish xizmatlarini va eng zamonaviy raqobatlashuvchi simsiz tarmoq xizmatlarini ta‘minlashni qo‘shishni ta‘minlaydi. WiMAX tarmog‘ini qurishning moliyaviy xarajatlari an‘anaviy sotali ikkinchi va uchinchi avlod tarmoqlarinikidan kamroq bo‘ladi, asosiy xarajatlar BS stansiyalari infratuzilmasini yaratish va qurilish montaj ishlarini olib borish uchun sarflanadi. IP-protokolida qurilgan WiMAX arxitekturasi keng polosali multimediyali ilovalardan foydalanishda eng yaxshi imkoniyatlar taqdim etadi, shuningdek, IP-asosida qurilgan mobil tarmoqlarda qo‘llaniluvchi ovozli va qisqa xabarlarni mobil uzatishni ta‘minlaydi.

3.4.4. WiMAX tarmoqlarini loyihalashtirish va tashkil qilish

2006 yil oxirida IEEE 802.16e standarti mobil profilini yaratish ustida olib borilgan ishlar yakunlandi. Hozirgi kunda standart

radioulanish interfeyslarining ko'plab turlari mavjud, lekin aynan IEEE 802.16e standartini ishlab chiqishda quyidagi algoritm va qurilmalardan qo'llash imkoniyati yaratilgan: adaptiv antenna tizimlari - AAS va murakkab antenna tizimlari- MIMO, ular turli zichlikda tashkil topgan ko'plab qayta akslanuvchi signallarni ishlashini ta'minlaydi. WiMAX tizimlarida yo'naltirish diagrammalarini adaptiv shakllantirish texnologiyasi – Beamformingning qo'llanilishi - (AAS elementi sifatida) tizimlar o'tkazish qobiliyatini oshirish va aloqa masofasini kengaytirish va interferensiya darajasini pasaytirish imkonini beradi. Bu makrosot prinsipi bo'yicha tarmoqlarni qurish holatlarida xizmat ko'rsatish maydonlarining kengayishiga olib keladi. Boshqa tomondan, MIMO texnologiyasi mikro, piko va femto tuzilishlarda ham o'tkazish qobiliyatini oshirishni ta'minlaydi. AAS va MIMO texnologiyalarining birgalikda qo'llanilishi bir-birini to'ldiruvchi sifatida ma'lumot uzatish tezligi va aloqa sifati bo'yicha yetarlicha ustunlik olish imkonini beradi. Bu texnologiyalarni to'liq ko'rib chiqamiz [4].

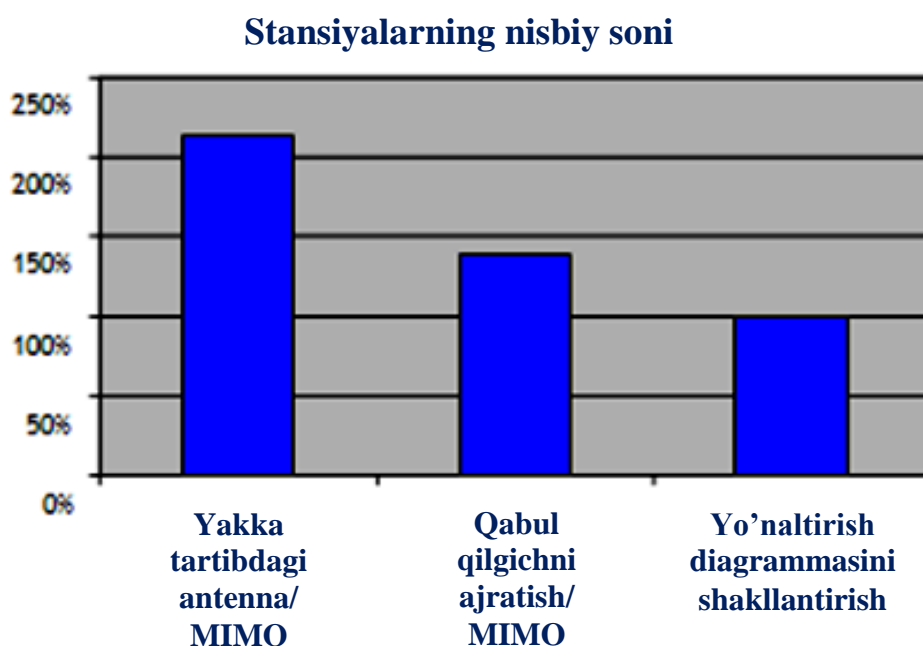
Yo'naltirish diagrammasini adaptiv shakllantirish texnologiyasining qo'llanilishi

Yo'naltirish diagrammasining adaptiv shakllantirish texnologiyasidan foydalanishda (keyinchalik AAS) BS antenasining elektr maydoni uzoq zonada AQ holati o'zgarganida yo'naltirish xususiyatlarini o'zgartirish imkoniyatini AQ tomonga yo'naltiradigan tor yo'naltirilgan bosh yaproqcha ko'rinishida shakllantiriladi. Amalda bir sota ta'siridagi chegaralarda ko'p sonli abonentlar bo'lganida ko'p yaproqchali diagrammalarni shakllantirish (yaproqchalar har bir abonentga yoki abonentlar guruhiga yo'naltiriladi) amalga oshiriladi. Bunga vaqt bo'yicha va OFDM-eltuvchi chastotalar bo'yicha klientlarni ajratish tufayli erishiladi. Bunday ko'p nurli diagrammani shakllantirish uchun BS tarkibidagi alohida qabul qilgich-uzatkichlar signalni ko'p elementli antenna panjarasi orqali qabul qiladi va uzatadi (4 elementli antenna panjaralari), bunda bunday panjaraning har bir element har bir vaqt momentida boshqalariga nisbatan ma'lum fazaviy surilishga ega bo'ladi. Natijada tarkibidagi nurlantirgichning yo'naltirish diagrammalarini (YD) kombinatsiyalanishi tufayli yaxshilangan yo'naltirilganlik xususiyatlariga ega bo'lgan yig'indi diagramma shakllantiriladi (yuqori kuchaytirish koeffitsentili torroq bosh

yaproqcha). Halaqitlar manbalari yoʻnalishida YDda nolinch tashkil etuvchilar shakllantiriladi, bu istalmaydigan yoʻnalishli interferensiyani deyarli toʻliq soʻndirish imkoniyatini beradi. Binobarin, bu konsepsiya har ikkala BSdan AQga va AQdan BSga yoʻnalishlarda ishlaydi. Bunda AQdan qabul qilinadigan signallar ularning joylashgan oʻrnini aniqlash uchun va keyin «pastga» kanalda YDni shakllantirish uchun ishlatilishi mumkin.

YDni shakllantirish gʻoyasi yangi hisoblanmaydi va adaptiv antennalar tizimi yoki “intelektual antennalar” konsepsiyasi boshqa radio tizimlar standartlarida koʻp yillardan buyon ishlatib kelinmoqda. Bu texnologiya asosan BSda ishlatiladi va oxirgi foydalanuvchi qurilmalarni sezilarli oʻzgartirilishini talab qilmaydi. Shunga mos ravishda WiMAX uchun sertifikatlashtirilgan abonent qurilmalari operator qurilmalarining imkoniyatlarini cheklab qoʻymasligi uchun AAS texnologiyasini qoʻllab-quvvatlashi kerakligi qarori qabul qilindi. BS uchun bunday imkoniyat qoʻshimcha, lekin majburiy emas hisoblanadi. AAS texnologiyasidan foydalanishni musbat tomonlari quyidagicha:

Birinchidan, turli uzatkichlar energiyasi va turli qabul qilgichlar sezgirliklari tezroq nurga konsentratsiyalanadi, u holda BS ning taʼsir etishi zonasi kengayadi. Bu hal qiluvchi va «yuqoriga» aloqa liniyasiga tegishli boʻladi. 3.27-rasmda YD ni shakllantirilishining talab qiladigan BSlar soniga taʼsiri keltirilgan.



3.27– rasm. AAS dan foydalanishga BS sonining bogʻliqligi

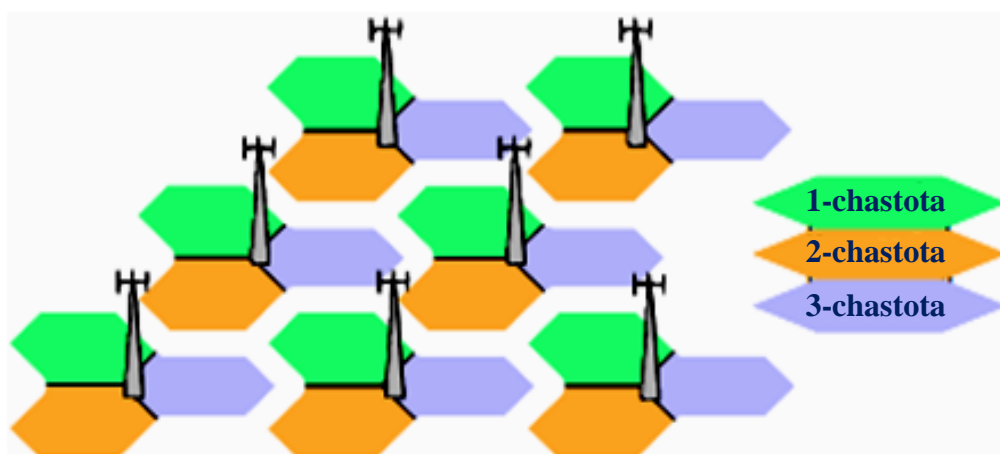
Diagrammada ko‘rinib turibdiki, bir xil qamrash zonasini ta‘minlash uchun bittalik antennali BS dan foydalanilganda va MIMO texnologiyasi qo‘llanilganda AAS dan foydalanilganligiga nisbatan 2.13 marta ko‘p stansiyalar talab qilinadi. Faqat fazaviy surilgan qabul qilgichlardan foydalanilganda esa farq 1.39 martani tashkil etadi.

Shunday qilib, surilgan qabul qilgichlardan yoki faqat MIMO dan foydalaniladigan tizimga taqqoslaganda AAS texnologiyasi minimum 40% bazaviy stansiyalar sonini kamaytirilishini ta‘minlaydi.

Ikkinchidan, signal energiyasi faqat individual abonentlarga yo‘naltiriladi, u holda bu tarmoqning qo‘shni sektorlaridagi boshqa abonentlarga yo‘naltiriladigan yoki qabul qilinadigan energiya miqdori kamayadi, shunga ko‘ra signal – halaqit holati sezilarli yaxshilanadi. Bu konsepsiya ham «pastga», ham «yuqoriga» aloqa liniyalarida ishlaydi.

Boshqa ob‘ektni ko‘rib chiqamiz va uning muhimligini baholaymiz. WiMAX radiotarmog‘i sektorli arxitekturali aloqa tarmoqlari hisoblanadi. O‘xshash qo‘shni BS lar ta‘sir etish zonalarida o‘sha bir chastotalardan foydalaniladi.

WiMAX tarmoqlar uchun ko‘pincha 1:3 chastotalardan takroriy foydalanish sxemasi qo‘llaniladi, bu BS larning uchta sektorli konfiguratsiyasi ishlatilganda barcha qo‘shni BSlar sektorlarida o‘sha bir chastotalar takroriy ishlatilishini bildiradi (3.28 - rasm).



3.28- rasm. WiMAX tarmog‘ining sektorli arxitekturasi

Bu esa o‘z navbatida, radioto‘lqinlar sektorining shartli chegaralaridan tashqarida ham tarqalishi tufayli qo‘shni BS larga uzatishga halaqitlar hosil qilishini bildiradi. Bu ayniqsa BS antennalari binolar tomlari sathidan yuqorida joylashganida yoki BS va AQ

orasida fazoviy bo'shliq bo'lganida kritik hisoblanadi. Bunday hollarda kanallararo interfereniyaga o'z o'rniga ega bo'lishni boshladi va signalning tarqalishiga kuchli ta'sir etadi.

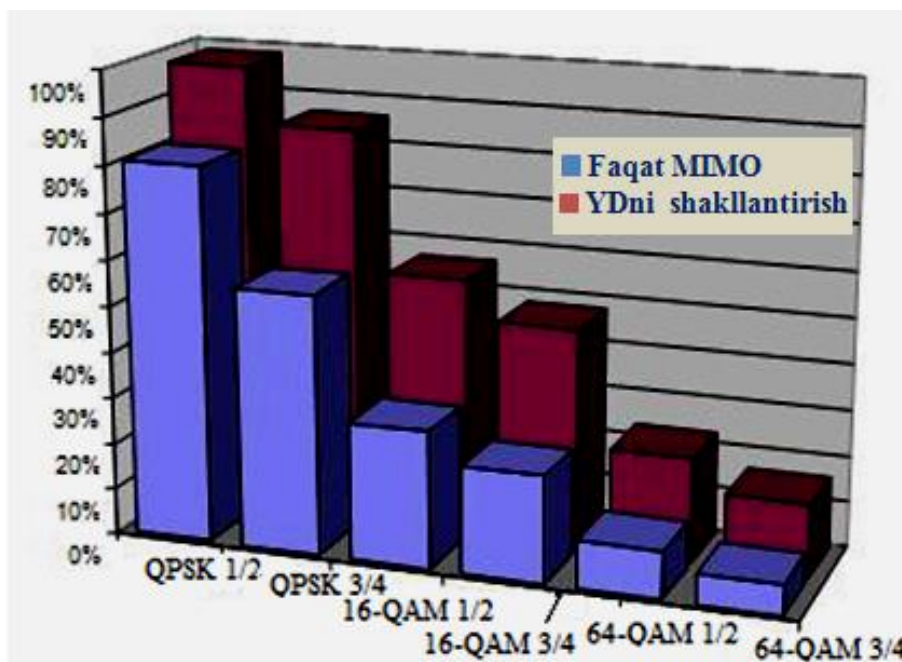
Bunga qarshi turish uchun WiMAX tizimi AMS modulyatsiya usullarini va kodlash sxemalarini adaptiv o'zgartirilishini ta'minlaydi. Masalan, QPSK $\frac{1}{2}$ modulyatsiya+halaqitbardosh kodlash aloqa sifati bo'yicha yaxshi (a'lo) natijalarni beradi, lekin bunda ma'lumotlarni uzatish tezligi bo'yicha yutqazishga to'g'ri keladi. Ya'ni hatto yomon radioaloqa sharoitlarida ham ishonchli radioaloqa ta'minlanadi, lekin bunda kanalning o'tkazish qobiliyati kamayadi. Adaptiv antenna qo'llanilmaganda bu sxema AQ BSning bevosita yaqinida bo'lganida yoki CINR darajaning ideal sharoitlarida ishlatilishi mumkin. Bunda BSning quvvatini oshirilishi yordam bermaydi, aksincha halaqit beradi, chunki bu yerda qo'shni sektorlardagi interferensiya darajasi ortadi.

3.29- rasmda keltirilgan sxemadagi AASli tizim MIMO texnologiyasi qo'llanilgan faqat antennalarni fazoviy surilishini ta'minlaydigan o'xshash yechim bilan taqqoslanadi. Grafik har xil modulyatsiya va kodlash sxemalarida qamrab olinadigan hududga bog'liqlikni ko'rsatadi. Ko'rinib turibdiki, AAS texnologiyasining afzalligi yaqqol ko'rinib turibdi. Hatto, eng ishonchli QPSK $\frac{1}{2}$ sxema AASli tizim qamrab oladigan maydonning 80 % da barqaror ish qobiliyatini ta'minlaydi. Qo'shni BSlar miqdorini o'rnatish vaziyatni tubdan o'nglamaydi, chunki BS qo'shimcha halaqitlarni yuzaga keltiradi.

Shuningdek, AAS texnologiyasi qo'llanilib qurilgan makrosotali arxitekturalar holatida foydalanish mumkin bo'lgan yuqoriroq darajadagi boshqa sxemalar ham bor. Ular spektral samaradorlikni sezilarli oshirilishini ta'minlaydi, bu esa yakunda har bir abonent uchun ma'lumotlarni uzatish tezligini oshirilishiga va o'sha bir o'tkazish qobiliyatida abonentlar sonini oshirilishiga olib keladi.

AAS texnologiyasini qo'llanilishining mobil abonentlarli aloqa tizimi xarakteristikalariga ta'siri darajasini aniqlash uchun baholashni abonentlar harakatlanishining turli tezliklarida ko'p nurlu kanallarning namunaviy modellaridan foydalanib bajarish zarur. Natijada past mobillikli abonentlar uchun (ya'ni 30 km/soatgacha tezlikda harakatlanadigan) aloqaning ishchi xarakteristikalari o'zgarmaydi. Faqat AQning yuqori harakatlanish tezliklarida yutuq bir oz kamayadi, lekin hatto bunda ham adaptiv algoritmlar ishlatilmaydigan

tizimlardagiga qaraganda tizimning ish xarakteristikalari yaxshiroq bo‘ladi.



3.29- rasm. Har xil modulyatsiya va kodlash sxemalari turlarida ASS va MIMO texnologiyalari qo‘llanilganda qamrab olinadigan hudud foizi

AAS texnologiyasining qo‘llanilishi afzalliklaridan yana biri halaqitlarni so‘ndirishli algoritmlarili AAS kombinatsiyalanganida chastotalardan takroriy foydalanish koefitsientini 1 qiymatgacha yetishi mumkin. Bu barcha BSlarda barcha mavjud chastotalar polosasi ishlatilishi mumkinligini bildiradi. Bu tizimning spektral samaradorligini qo‘shimcha oshirish, shuningdek, hatto chastota resursi cheklanganida WiMAX tarmog‘ini ishlatilishiga imkon beradi.

Shunday qilib, BS tarkibida AAS texnologiyasini ishlatilishi o‘tkazish qobiliyatini deyarli 40 % ga oshirilishiga olib keladi, bunda har bir kanalning spektral samaradorligi 2,1 bit/sek/Gs/sektorga yetadi.

MIMO texnologiyasining qo‘llanishi

Yuqorida ta’riflaganimizdek, ko‘p uzatgich va ko‘p qabul qilgichli uzatish asosida (MIMO) signallarni qayta ishlash ancha istiqbolli texnologiya hisoblanadi. Bu texnologiya simsiz keng polosali tarmoqlarda sotalarning o‘tkazish qobiliyatini va ma’lumot uzatish tezligini oshirishni ta’minlaydi. Juda zich joylashgan shahar sharoitlari mikrosotalar, pikosotalar yoki femtosotalarda BS va AQ

orasida signalni ko'p marta aks ettirish imkonini beradi. Buni maksimal darajada ta'minlash uchun uzatilayotgan oqimlarni bir vaqtda ko'p marotaba yuqori darajada dekorrelyatsiyalashni ta'minlash kerak. Bu texnologiya sxemalari antennalar ichiga joylashtirilishi yoki turli turdagi qutblanish antennalaridan foydalanishi mumkin. MIMODA signalni dekoderlash oddiy holatda amalga oshirilmagani sababli abonent qurilmasini ham murakkabligini oshirishni talab etadi.

WiMAX tizimlarida MIMODan foydalanish quyidagi ikkita asosiy ustunlikni ta'minlaydi:

– **Aloqa ishonchliligini oshirish.** MIMODan foydalanuvchi va foydalanmaydigan qurilmalarni taqqoslanganda «yuqoriga» liniyada ishlash sifatining yaxshilanishi kuzatiladi. Radioto'lqinlarning kuchli sochilishi holatlarida ma'lumot uzatishda ancha ishonchlilik va barqarorlikni ta'minlaydi.

– **Kanalning o'tkazish qobiliyatini oshirish.** Yuqori darajadagi modulyatsiyalash imkoni mavjudligi sababli va bir vaqtda bir necha mustaqil oqimlarni uzatishi sababli MIMO tizimlari bitta antennali sxemalar bilan taqqoslanganda, quyidagicha o'tkazish qobiliyatini oshirishni ta'minlaydi: makrosotalarda 30% gacha va mikrosotalarda 100% gacha.

Shuningdek, MIMO texnologiyasining ustunligi sifatida an'anaviy antenna tizimlariga qaraganda ishchi xarakteristikalarining barqarorligini ta'kidlab o'tish zarur. Abonent 3 km/soatdan 120 km/soatgacha tezliklarda harakatlenganda aloqaning yomonlashish xarakterlari kuzatilmaydi. MIMOLI tizimlarning jiddiy kamchiligi signalni qayta akslantirish holatlarida sifat xarakteristikalari yo'qolishi hisoblanadi.

AAS va MIMO texnologiyalarini solishtirish

BS xizmat ko'rsatish zonasi

MIMO uchun ikki qabul qilib uzatuvchi antennali element va AAS uchun 4 antennali 4 ta uzatgichdan foydalanib, maksimal xizmat ko'rsatish masofasi AAS va MIMO texnologiyalarini solishtirish quyidagi natijalarni beradi (3.13- jadval).

Jadval natijalari «pastga» va «yuqoriga» aloqa liniyalarining maksimal resurslaridan foydalanganda, aloqa kanalining aniq energetik imkoniyati uchun mos keladi. Jadvaldan ko'rinadiki, AAS texnologiyasi MIMO texnologiyasi bilan solishtirganda 5 dBga

kuchaytirish koeffitsientini oshirishni ta'minlaydi, bu nazariy holatda xizmat ko'rsatish masofasi 100% gacha ortishiga olib keladi.

3.13- jadval

AAS va MIMO texnologiyalaridan foydalanishda antenna tizimlarining kuchaytirish koeffitsienti qiymatlari

	CPE alohida blok ko'rinishida		CPE PCMCIA platasi ko'rinishida	
	MIMO	Yo'naltirish diagrammalarini shakllanishi	MIMO	Yo'naltirish diagrammalarini shakllanishi
Tizimning kuchaytirish koeffitsienti	157,7db	162,7 db	153,3db	157,9db

Tarmoqning o'tkazish polisasi

AAS texnologiyasi bu ko'rsatkich bo'yicha MIMO ga qaraganda yuqori natijalar beradi. Bir tipdagi tarmoqlar uchun har bir sektorda chastota spektridan foydalanish samaradorlik ko'rsatkichlari quyida keltirilgan (3.14- jadval).

Natijalar ko'rsatadiki, AAS texnologiyasidan foydalanish bilan tarmoqning xizmat ko'rsatish aloqa sifatini 90% gacha oshirishni ta'minlash mumkin.

MIMO texnologiyasi mikrosotali tizimlarda juda yuqori o'tkazish qobiliyatini ta'minlaydi, lekin bunga abonent qurilmalarini qo'shimcha murakkablashtirish hisobiga erishiladi. Yana, eslatib o'tish kerakki, BS va AQ bevosita ko'rinish holatlarida MIMOLI sxema yomon ishlaydi.

3.14- jadval

AAS va MIMO texnologiyalaridan foydalanishda tarmoq spektral samaradorlik ko'rsatkichlari

Sxema	Sotaning maydoni bo'yicha o'rtalashtirilgan spektr samaradorligi
Yo'naltirish diagrammasini shakllantirish	2,1 bit/sek/Gs
MIMO	1,7 bit/sek/Gs
Yo'naltirish diagrammasini shakllantirish + MIMO	2,5 bit/sek/Gs

Bu kamchilik ikki texnologiyani birlashtirish bilash tuzatilishi mumkin, bu tarmoqni yoyishning barcha shartlarida optimal yechim olish imkonini beradi. AAS texnologiyasining qo‘llanilishi WiMAX tarmoqlarini birlamchi yoyish darajasiga mos keladi. MIMOning qo‘shilishi mikro va piko sotali tarmoqlarda yuqori abonentlar sig‘imini talab qiladigan tarmoqlarda amalga oshiriladi. AAS va MIMOning birlashishi bitta umumiy antenna tizimlari yordamida ta‘minlanishi mumkin, bu holatda BSni oddiy dasturiy ta‘minotni yuklash orqali modernizatsiyalash imkoniyati bo‘ladi.

AAS va MIMO texnologiyalarini birlashtirish imkoniyati

Hozirgi kunda amaliyotda qo‘shimcha imkoniyatlar olish uchun AAS va MIMO texnologiyalarini birlashtirish bo‘yicha qilingan ishlar mavjud. Lekin bunda bir necha qiyinchiliklar yuzaga keladi, masalan, antennalarni joylashtirish bo‘yicha talablar. AAS texnologiyasini qo‘llaganda antennalar bir-biriga yetarlicha yaqin joylashishi kerak (odatda, nurlanuvchi to‘lqinning yarim uzunligi hisobida), antenna elementlari uchun MIMO sxemalar qo‘llanganda esa antennalar bir-biridan uzoqlikda joylashishi lozim yoki qutblanishlari turlicha bo‘lishi kerak. Yuqoridagilarga bog‘liq holda, bu texnologiyalarni ikki jihat bo‘yicha birlashtirish imkoniyati mavjud:

- bir-biriga yaqin bo‘lgan optimal masofalarda AASli tizimlarda MIMO ni qo‘llash.

- Har bir panel elementlari orasidagi masofa yetarlicha kichik bo‘lganda, ikki elementli antenna panellari juftliklarini qo‘llash.

Birinchi variant aloqa kanallari energetik imkoniyatlarini oshirishda katta foyda beradi. Uni tadbqiq qilish uchun baza stansiyalari standart to‘rt elementli antenna panellaridan foydalanish hisobi yetarlicha oson ishlab chiqilgan bo‘lishi mumkin, ular tizimni keyinchalik almashtirishni talab qilmaydi. «AAS+MIMO» texnologiyalarini birlashtirish BSda dasturiy ta‘minotni yuklash orqali amalga oshirilishi mumkin.

Ikkinchi variantda eng yaxshi ishchi xarakteristikalariga erishiladi. AAS hisobi bo‘yicha olingan aniq talablarga bog‘liq ravishda 30 %gacha kanalning o‘tkazish qobiliyatini oshirish mumkin. Bu sxema mavjud apparat bazasida yetarlicha oddiy holatda amalga oshiriladi.

WiMAX tarmoqlarini yoyishning qiyinchiliklari

To‘rtinchi avlod tarmoqlariga qo‘yiladigan talablarga mos ravishda WiMAX tizimlariga aloqa seanslarini qayta ishlash dinamik

algoritmlarini ta'minlash, radioefir shartlariga mos ravishda signal qaya ishlash usullarini soddalashtirish kabi talablar qo'yiladi.

Agar WiMAX tizimlari "signal-shovqin" nisbatining yuqori ko'rsatkichiga va ishonchli signalga ega bo'lsa, yuqori tezlikli uzatish rejimini tanlash mumkin, bunda signal qabul qilgichlarda oson va aniq dekodlanadi. Radiomuhitning yomon parametrlil holatlarida tizim ancha chidamli signal qayta ishlash usullarini tanlaydi (masalan, OFDM-simvolidan foydalanib kam bitli yuqori quvvatli signal chiqarish), bu esa signalni aniqroq dekodlash imkonini beradi. Shuning uchun WiMAX tarmoqlarini yoyish bir qator murakkabliklarga ega, bunda nafaqat signal pog'onasi va CINR koeffitsientlari hisobga olinadi, shuningdek Abonent qurilmalari uchun kanal resurslarini dinamik taqsimlash mexanizmlari bilan aniqlanadi. Ko'plab aloqa tizimlari 2-3 profildagi aloqa seanslariga ega, shuningdek WiMAX tizimlarida bir vaqtda 7 tagacha profil mavjud bo'lishi mumkin, lekin WiMAX tizimlarida signalni qayta ishlash algoritmlari boshqa simsiz tizimlarga nisbatan ancha murakkabroq bo'lib tuyuladi.

3.5. WiMAX tarmoqlarida radiochastota diapazonidan foydalanish

3.5.1. WiMAX tizimlari uchun radiochastotalarni taqsimlashda butun dunyo an'analari

WiMAX bu simsiz keng polosali ulanish (SKPU) tarmoqlarini yaratish uchun ishlab chiqilgan texnologiya bo'lib, ular an'anaviy sotali aloqa tizimlari ishlatmaydigan chastotalar polosasida, ya'ni 2 GGs dan yuqori diapazonda ishlaydi. WiMAX tarmoqlari ishlatadigan chastotalar spektri 2,3 GGs va 2,7 GGs orasidagi diapazondagi polosani (Shimoliy Amerikada foydalaniladigan), qayd etilgan xizmatlar uchun 3,3 GGs va 3,8 GGs orasidagi diapazondagi polosani, shuningdek, Wi-Fi va simsiz telefoniya foydalaniladigan "litsenziyalanmagan" 2,4 GGs va 5,8 GGs polosani o'z ichiga oladi. Zamonaviy IEEE 802.16 standartlari 2 GGs va 6 GGs orasidagi butun chastotalar diapazonini qo'llab-quvvatlasada, WiMAX forumi 2,5 GGs, 3,5 GGs va 5,8 GGs polasalarda sertifikatlarni olishga yo'naldi. Qurilgan WiMAX tarmoqlarining asosiy ulushi 3,5 GGs diapazonga to'g'ri keladi, bu yerda butun dunyoda o'rnatilgan qurilmalarning 40

foiziga to‘g‘ri keldi, keyin 5 GGs; 5,2 GGs; 5,4 GGs; 5,6 GGs; 5,8 GGs diapazonlar keladi. SKPU jahon bozorining 85 foizi atrofidani operator tarmoqlari tashkil etadi, qolgan qism esa xususiy korporativ tarmoqlarga to‘g‘ri keladi [14].

Lekin, bunda WiMAX tizimlari uchun alohida radiochastotalar polosasi ajratilmadi. WiMAX uchun 2,5 GGs yoki 3,5 GGs chastotalar diapazonidagi “biriktirilgan” spektr haqida gapirilganda ham bu diapazonlarda chastotalar polosasining turliciligiga ega bo‘linadi. Masalan, AQSh, Kanada va Lotin Amerikasining bir necha davlatlarida SKPU tizimlari uchun spektr 2,3 GGs polosalarda va 2,5 GGS hamda 2,7 GGs orasidagi diapazonda ruxsat etiladi, u holda Wi-Fi tizimlari va simsiz telefonlar uchun 2,4 GGs polosa ishlatilayotgani bois, unga ruxsat etilmaydi. Chastotalarni taqsimlashda 3,5 GGs polosada va 3,3 GGs va 3,8 GGs orasidagi diapazonda murakkab vaziyat vujudga keldi.

Bosh muammo shundaki, ko‘zda tutilgan polosalar turli tarqalish xarakteristikali turli diapazonlar qismlaridan, uzatkichlar quvvatlariga talablar va qurilmalarni ishlatilishi imkoniyatlaridan iborat. Vaziyat yanada murakkablashadiki, simsiz keng polosali ulanishga taqsimlangan spektr hatto alohida olingan kontinentlarda ham deyarli garmonlashtirilmagan. Lekin, hatto prinsipial umumiy spektr texnik ajratilishi mumkin bo‘lgan joylarda ham siyosiy reja muammosi vujudga keladi, chunki turli davlatlarda radiochastota spektrini ishlatish bo‘yicha turli talablar amal qiladi. Natijada, xalqaro va milliy spektrdan foydalanish qoidalari labirintida WiMAX tizimlarini rivojlantirish uchun yo‘llarni qo‘yish oson bo‘lmaydi va katta kuchlarni talab qiladi.

3.5.2. WiMAX tizimlari uchun spektrni ajratishga bog‘liq muammolar

Avval ko‘rsatilganidek, IEEE 802.16 standarti spetsifikatsiyalari keng chastotalar diapazonida ishchi polosalarni aniqlaydi, shuning uchun WiMAX tizimlari nazariy jihatdan 66 GGsdan kam bo‘lgan istalgan chastotalarda ishlashi mumkin. WiMAX Forumi WiMAX tarmoqlarini qurish uchun uchta 2,5 GGs, 3,5 GGs va 5,8 GGs chastotalar oraliqlarini aniqlagan bo‘lsa-da, amalda bu masalada hozircha global ko‘lamda birlik yo‘q. Bunday garmonlashtirish esa, avvalo oxirgi uskunaning narxini kamaytirish uchun zarur. Mur

qonuni deyiladigan qonun (yoki ishlab chiqarishning oshirilishi hisobiga tejash qonuni) WiMAX qurilmalarini ishlab chiqarish (mobil terminallar yoki oʻrnatiladigan WiMAX-kartalar) ommaviy boʻlishi uchun mahsulot birligining tannarxi kamaytirilishi (mos ravishda oxirgi narx) kerakligini nazarda tutadi. Binobarin, narxni tashkilashtirishning bunday konsepsiyasi bazaviy qurilmalar uchun ham toʻgʻri boʻladi [7].

Shunday qilib, dunyoning turli regionlarida WiMAX tarmoqlarini qurish uchun turli chastotalar polosalariga ruxsat etiladi, lekin ilgʻorlik WiMAX Forumi aniqlaydigan polosalarga beriladi. Yevropada, masalan, WiMAX tizimlari uchun sezilarli chastota resurslari 3,5 GGs diapazonda ruxsat etiladi. AQShda eng katta ruxsat etiladigan polosa 3,5 GGs diapazonda joylashgan va endilikda asosan Sprint Nextel va Clearwire kompaniyalari orasida taqsimlangan. Janubiy-Sharqiy regionda koʻrinib turibdiki, boshqa diapazonlarga ham ruxsat etilsada, 2,3 GGs diapazon ommaviy boʻlib qoladi. Hindiston va Indoneziyada 2,5 GGs va 3,3 GGs diapazonlardagi polosalar ishlatiladi, Pokistonning milliy WiMAX operatori esa 3,5 GGs diapazonda ishlaydi.

Analog televideniye diapazoni (700 MGs) WiMAX tarmoqlarini qurish uchun ruxsat etilishi mumkin, lekin, birinchidan, toʻliq raqamli televideniye oʻtilishni kutish zarur, ikkinchidan, bu diapazon uchun boshqa texnologiyalar ham daʼvogarlik qilmoqda. 2008 yilda AQShda bu spetрни taqsimlash boʻyicha auksion oʻtkazildi va natijada spetрning eng katta ulushlari Verizon Wireless va AT&T kompaniyalarga ajratildi. Va bu har ikkala kompaniyalar bevosita WiMAX tizimlariga raqobatda boʻlgan LTE tarmoqlarini qurishda oʻzlarining istaklarini bildirishdi. Evrokomissiya esa, WiMAX ni qoʻshganda simsiz aloqa tizimlari uchun 500-800 MGs diapazondagi spektrni qayta taqsimlash masalasini koʻrib chiqmoqda. Yevropada eng istiqbolli 770-862 MGs polosa hisoblanadi, u birinchi navbatda analog teleuzatishda boʻshatiladi. Shuningdek, Yevropa Ittifoqi WiMAX texnologiyalari ham ular qatoriga kiradigan HSPA va EVDO texnologiyalari kabi istiqbolli keng polosali tarmoqlari uchun 900 MGs diapazondan foydalanishni maʼqulladi.

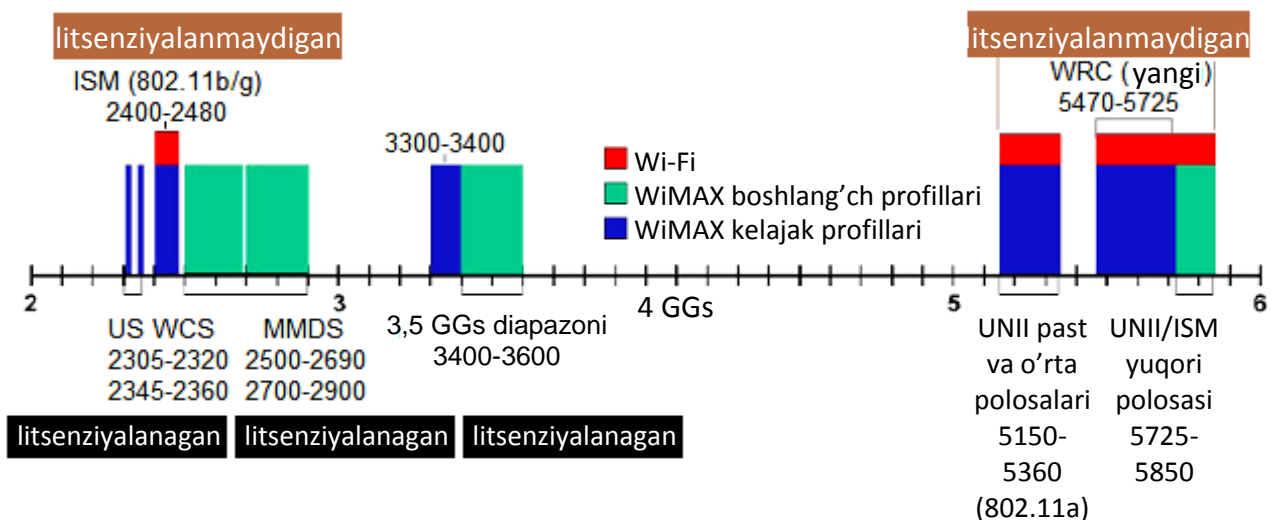
Taʼkidlash kerakki 2007 yilning oktyabrida HTI radioaloqa Sektori (ITU-R) qabul qilgan WiMAX texnologiyalarining IMT-2000 standartlar oilasiga kiritilishi haqidagi qarori shunga olib keladiki, mobil WiMAX qurilmalari (xususan, bugungi kunda 2,5-2,69 GGs

diapazonda) yanada unifikatsiyalanadi va uni IMT-2000 dasturini tan oladigan dunyoning istalgan mamlakatida ishlatish mumkin bo‘ladi.

3.5.3. Turli chastotalar diapazonlarida va dunyoning turli davlatlarida spektrning taqsimlanishining o‘ziga xos xususiyatlari

3.30–rasmda 2 dan 6 GGsgacha diapazonda SKPU tizimlari uchun ruxsat etiladigan chastotalar polosasi keltirilgan.

Rasmdan ko‘rinib turibdiki, polosalar litsenziyalanadigan va litsenziyalanmaydigan sifatida identifikatsiyalangan. Litsenziyalanadigan deyilganda qoidaga ko‘ra, rostlovchiga bu chastotalar polosasini ishlatgani uchun to‘laydigan foydalanuvchilarga (operatorlarga, tashkilotlarga, kompaniyalarga) “qat’iy biriktiriladigan” chastotalar polosasi tushuniladi. Litsenziyalanmaydigan polosalar bepul asosda istalgan foydalanuvchi uchun ruxsat etiladigan polosalar hisoblanadi. IEEE 802.11a/b/g/n (Wi-Fi) standartlari, masalan, litsenziyalanmaydigan polosalarga asoslangan va bunda u bu chastotalar doirasida raqobat qiladigan texnologiyalardan yetarlicha “himoyalangan” bo‘lib qoladi. Bunda shuni ta’kidlaymizki, “litsenziyalanmaydigan chastotalar” tushunchasi yetarlicha o‘ziga xos va faqat Yevropaning bir necha davlatlari va AQSh uchun xarakterlidir. Boshqa davlatlarda esa, barcha foydalanishga ruxsat etiladigan chastotalar litsenziyalanadi [11].



3.30– rasm. 2 GGsdan 6 GGsgacha diapazonda SKPU tizimlari uchun ruxsat etiladigan chastotalar polosasi

Litsenziyalanmaydigan chastotalar polosasi (qayerda ularga ruxsat etilsa) avvalo, SKPU xizmatlari uncha katta bo‘lmagan kompaniya-provayderlari uchun o‘ziga tortadi, chunki ular tarmoqlarni qurishda vaqtni va mablag‘ni tejaydi. So‘nggi hisobda, bu oxirgi foydalanuvchiga xarajatlarni kamaytiradi va keng polosali ulanishning alternativ simli uzatish xizmatlariga raqobatbardosh bo‘lib qoladi.

Litsenziyalanmaydigan spektr ayniqsa AQShda o‘ziga tortgan, chunki u yerda 2 GGsdan 6G Gsgacha diapazondagi litsenziyalanadigan chastotalardagi kamchiliklar sinalmoqda. Boshqa tomondan, litsenziyalanadigan chastotalar polosasiga ”ega” bo‘lgan yirik operatorlar “VIP- sinf” kabi xizmatlarni taqdim etishi mumkin, shuning uchun ularning xizmatlari ishonchli va sifatli bo‘ladi va bu ularning raqobatli afzalligini oshirishga xizmat qiladi.

3,5 GGs diapazoni

Bu diapazon litsenziyalanadigan chastotalar polosasi diapazoniga kiradi va Yevropa, Lotin Amerikasi va Osiyoning ko‘plab davlatlarida SKPU tarmoqlarini qurish uchun ruxsat etiladi. Diapazon global masshtabda “o‘ta yuklangan” SKPU tarmoqlari hisoblanadi. Umumiy 300 MGs (3,3 GGsdan 3,6 GGsgacha) polosa simsiz WAN-tarmoqlar uchun magistral liniyalarni qurish bo‘yicha keng imkoniyatlarni ta’minlaydi. Bu diapazonning bunday ommaviyligi ko‘p sonli qurilmalarning paydo bo‘lishi va WiMAX tizimlarining ishlab chiqaruvchilari va operatorlari orasida sog‘lom raqobatni vujudga kelishiga olib keladi. 3.31-rasmda SKPU tizimlari uchun 3,5GGs diapazondagi chastotalar polosasi ruxsat etiladigan dunyoning turli regionlaridagi davlatlarning ro‘yxati keltirilgan.

5 GGs diapazoni

Bu diapazonda dunyoning turli regionlarida SKPU tizimlari uchun ajratilgan chastotalar polosalarining bir-birlarini yopib qolish holati vujudga keldi. Butundunyo radioaloqa konferensiyasi tomonidan SKPU tarmoqlari ishlatishi uchun qo‘shimcha 5470 MGs – 5725 MGs diapazondagi chastotalar polosasi ajratilgan. Bevosita WiMAX tarmoqlari diapazonning yuqori polosasida, ya’ni 5725 MGs – 5850 MGs chastotalardagi diapazonda qurilmoqda, chunki bu yerda raqobat qiladigan texnologiyalar va interferensiyalar kam (masalan, Wi-Fi tarmoqlardan), tashqi antennaning ruxsat etiladigan quvvati esa 2-4Vt ni (bu diapazonning pastki va o‘rta polosalaridagi 1Vt dan farqli ravishda) tashkil etadi. Wi-Fi tarmoqlari U-NII pastki va o‘rta

polosalarida ishlaydi, ular SKPU tarmoqlari uchun o‘z samaradorligini ko‘rsatdi.

Bu dipazonning “litsenziyalanmaydigan” xarakteri sababli operatorlar tarmoqlari uchun uni kompaniyalar bosqichma-bosqich o‘zlashtirishi ko‘zda tutilmoqda (magistral tarmoqlardan tashqari).

Boshqa tomondan, 4G darajadagi xizmatlarni taqdim etishga qodir bo‘lgan chastotalar polosasiga (ya’ni, 10MGs va 20MGs kenglikdagi polosalar) aynan yuqori diapazonlarda (ya’ni, 2GGsdan yuqori) ruxsat etiladi. Va shuning uchun faqat past chastotali diapazonlarni o‘zlashtirish tarmoqlarning o‘tkazish qobiliyati bo‘yicha talablarni qoniqtira olmaydi va ko‘rinadiki, amalda turli diapazonlardagi chastotalar polosalarini ishlatadigan kombinatsiyalangan tarmoqlar o‘z o‘rniga ega bo‘ladi

2,5 GGs diapazoni

Bu diapazonda SKPU tarmoqlarini qurish uchun AQSH alohida qiziqish bildirilmoqda va bir necha nimdiapazonlar ajratilmoqda.

WCS nimdiapazoni – bu WCS (ingl. *Wireless Communications Service*) simsiz aloqa xizmatlari uchun ajratilgan 15 MGs kenglikdagi 2305 MGs – 2320 MGs va 2345 MGs – 2360 MGs diapazonlardagi chastotalar polosalari juftligidir.

Bu polosalar orasidagi 25 MGs interval SKPU tarmoqlari uchun potensial interferensiya muammosi bo‘lgan raqamli radioeshittirishga (ingl. *Digital Audio Radio Service, DARS*) ajratilgan. Bu diapazonda oshirilgan spektral samaradorlikli texnologiyalar mavaffaqiyatli bo‘lishi mumkin. Ular OFDM-multiplekslash hamda adaptiv modulyatsiya va kodlash asosidagi texnologiyalar hisoblanadi. AQSHda bu diapazondagi asosiy litsenziya egalari Verizon, BellSouth, AT&T va Metricom kompaniyalari hisoblanadi.

ISM nimdiapazoni - ISM (ingl. *Industrial, Scientific and Medical services*) sanoat, ilmiy va meditsina ilovalari uchun polosa, AQSHda ajratilgan va litsenziyalanmaydigan hisoblanadi. Nimdiapazon SKPU tarmoqlarini qurish uchun 2400...2480 MGs polosada taxminan 80 MGs kenglikka ega. Bu polosada WLAN sinfidagi tarmoqlar uchun yaxshi “yaroqlilikni” namoyon qilgan Wi-Fi tarmoqlari ishlaydi. Wi-Fi va WiMAX tarmoqlarining o‘zaro ta’sirlashish imkoniyatlarini aniqlaydigan bo‘lajak WiMAX profillari bu ikki texnologiyani birlashtira olishi mumkin va buning hisobiga SKPU xizmatlarining qoplash zonasini kengaytirishi mumkin.

MMDS nimdiapazoni 2500 MGs dan 2690 MGs gacha diapazondagi (IMT kengaytirish diapazoni) 6 MGs dan kenglikdagi 31 ta kanalni o‘z ichiga oladi va shuningdek, o‘z tarkibida qayd etilgan interaktiv televideniye (ingl. *Instructional Television Fixed Service, ITFS*) xizmatlariga ega bo‘ladi. Dastlab bu spektr yetarlicha o‘zlashtirilmagan edi, chunki televizion yo‘nalishga ega bo‘lgan va AQShda SKPU tarmoqlarini rivojlantirish uchun ham ajratilgan. Bu diapazonda asosiy chastota foydalanuvchilari Sprint va Nextel kompaniyalari hisoblanadi. Yaqin bir necha yillarda tahlilchilar bu diapazonda SKPU bozorining o‘shishini aytishmoqda.

WiMAX Forumi o‘z qiziqishlarini litsenziyalanadigan 3,5GGs polosalariga va litsenziyalanmaydigan U-NII 5GGs yuqori polosalariga yo‘naltirmoqda. Bu yerda interferensiya sathi past, signalning ruxsat etiladigan quvvatlari yuqori va o‘tkazish qobiliyati keng bo‘ladi. Bu butun dunyoda WiMAX standartining yuqori o‘shish sur‘atlarini ta’minlaydi, shuning uchun bu polosalar potensialroq bozorlar bo‘ladi va ishlab chiqarishning oshirilishi hisobiga iqtisod qilishni ta’minlashga qodir bo‘ladi.

WiMAX uchun qo‘shimcha chastotalar polosalari

WiMAX tarmoqlarini va boshqa SKPU tizimlarini qurish uchun dunyoning turli regionlarida hozirgi vaqtda qo‘shimcha chastotalar polosalari ko‘rib chiqilmoqda. Masalan, Yaponiyada 4,9 GGs – 5,0 GGs polosa 2007 yildan ruxsat etilgan, 5,47 GGs – 5,725 GGs polosa esa kelajak uchun zahira sifatida ko‘rib chiqilmoqda. Bunda birinchi polosada BSni qurish uchun litsenziyalash talab qilinadi va 5 MGs, 10 MGs va 20 MGs kengliklardagi polosalar qo‘llab-quvvatlanadi, shu bilan bir vaqtda ikkinchi polosada litsenziyalash talab qilinmasligi mumkin va 20 MGs kenglikdagi polosa qo‘llab-quvvatlanadi. Shimoliy Amerika bozori dastlab jamoat xavfsizligi xizmatlari uchun polosa hisoblangan 4,9 GGs diapazonida WiMAX tarmoqlarini qurishga qiziqish bildirmoqda. Hatto WiMAX tarmoqlari va shunga o‘xshash xizmatlar uchun pastroq 800 MGs litsenziyalanadigan diapazon va 915 MGs litsenziyalanmaydigan kabi chastotalar polosalaridan foydalanishga qandaydir qiziqish bor. WiMAX standarti tovushlarni va katta hajmlardagi ma’lumotlarni uzatish xizmatlaridagi, mobillikda foydalanuvchilarning ehtiyojlarini qoniqtirishga qodir uzoq kutilgan spektral samaradorlikka va yuqori o‘tkazish qobiliyatiga olib kelishga “va’da” bermoqda. Bu to‘g‘ri ko‘rinish bo‘lmaganida ishlashga qodirligi tufayli ko‘proq

foydalanuvchilarni jalb qilishga, qurishga kam harajatlarga katta aloqa masofasiga (uzoqligiga) va standartlashtirish hamda o‘zaro ta’sirlashish hisobiga arzon abonent qurilmalari bozoriga ommaviy kirib borishga imkon beradi. Ko‘rinib turibdiki, bu keng polosali mobillikka va 4G tizimlarni shakllantirishga yo‘l hisoblanadi.

O‘zbekistonda WiMAX tizimlari uchun chastotalarning ajratilishi

O‘zbekistonda zamonaviy simsiz keng polosali tarmoqlarni joriy etish jarayoni O‘zbekiston aloqa va axborotlashtirish agentligi (O‘zAAA) tomonidan faol qo‘llab-quvvatlanmoqda va ular uchun chastotalarni ajratish imkoniyati deyarli barcha uchta 2,5 GGs, 3,5 GGs va 5 GGs diapazonlarda ko‘zda tutilgan. 3.15-jadvalda O‘zbekistonda 2010 yilning oxirlari holatigacha chastotalarga ruxsat etilishi darajasi keltirilgan [20].

3.15- jadval

O‘zbekistonda WiMAX tizimlari uchun chastotalarga ruxsat etilishi

Diapazon	Ruxsat etilishi darajasi
2,3 GGs	WiMAX tarmog‘i qurilgan (IEEE 802.16e standarti)
2,4 GGs	Wi-Fi (b/g/n) tarmoqlari foydalanishi uchun ajratilgan
2,5 GGs	Harakatdagi aloqa fuqaro xizmatlari foydalanishi mumkin.
3,5 GGs	Harakatdagi fuqaro xizmatlari ikkilamchi asosda foydalanishi mumkin. WiMAX tarmog‘i qurilgan (IEEE 802.16d standarti)
5,15 GGs - 5,25 GGs	Harakatdagi fuqaro xizmatlari ikkilamchi asosda foydalanishi mumkin.
5,25 GGs - 5,35 GGs	Wi-Fi (a/n) tarmoqlari foydalanishi uchun ajratilgan
5,7 GGs - 5,8 GGs	Umuman olganda hukumatga mo‘ljallangan diapazon, lekin unda qo‘shma foydalanish uchun polosalar mavjud

2,5GGs diapazon (2,3 GGs - 2,7 GGs keng intervalda) hozir ayniqsa shaharlarda o'ta yuklangan, chunki unda hozirda Wi-Fi xot-spotlar ishlamoqda va LTE keng polosali tarmoqlarni (ya'ni, 10 MGs va 20 MGs polosalarli) qurish rejalashtirilmoqda. Shuning uchun WiMAX tarmoqlarini qurish uchun 3,4 GGs - 3,6 GGs diapazon ma'qulroq bo'lib qoladi, etiladigan qurilmalar paydo bo'lganidan keyin esa 5 GGs diapazon o'zlashtirishi mumkin. Umuman olganda shuni tasdiqlash mumkinki, O'zbekistonda WiMAX tarmoqlarini qurish uchun chastotalarning ajratilishi muammosi hal etiladigan masala.

Bunga qaramasdan 2011 yilning boshiga kelib mamlakatda ham qayd etilgan, ham mobil WiMAX xizmatlarini taqdim etadigan faqat bitta operator (EVO savdo markali Super iMax kompaniyasi) ishlamoqda. 2010 yilning oxiriga kelib EVO 9 ta viloyatni qamrab oldi va o'z abonentlari sonini 13000 kishigacha yetkazdi. EVO tarmog'i ikkita WiMAX standartidan (IEEE 802.16d va IEEE 802.16e), ikkita chastota diapazonidan (mos ravishda 3,5 GGs va 2,3 GGs) foydalanadigan kombinatsiyalangan tarmoq namunasi hisoblanadi.

Yangi WiMAX tarmoqlariga kelsak, 2011 yilning boshiga kelib O'zAAA ning ma'lumotlariga ko'ra, 2010 yilda WiMAX tarmoqlarini qurish va tizimlarini ishlatishga ega bo'lgan 2ta sotali operator va 4ta Internet-provayder bunday tarmoqlarni qurish rejalari haqida bildirmadi.

Bu yerda ta'kidlash joizki, umumiy foydalanishdagi aloqa tarmoqlari (ularga WiMAX tarmoqlari ham kiradi) doimo ularning tijoriy foydaliligiga asoslanadi. Mos ravishda operatorlarga, avvalo, shaharlar va zich joylashgan hududlar qiziqarli (manfaatli). Lekin yirik shaharlarda WiMAX texnologiyasi simli ulanish texnologiyalari va sotali aloqa tizimlari tomonidan katta raqobatga duchor bo'ladi. Shuning uchun ko'plab mutaxassislar WiMAX texnologiyasiga simli ulanish va mobil aloqa murakkab yoki mumkin bo'lmagan joylarda qo'llanilishini tavsiya qilish bilan an'anaviy simli ulanish va mobil tarmoqlarga to'ldirish yoki zaxira rolini berishmoqda.

Umumiy foydalanishdagi tarmoqlardan farqli ravishda korporativ aloqa tarmoqlari hamma vaqtlarda ham zich joylashgan hududlarda (energetiklar shaharchasi, neftgaz majmuasi korxonolari ishchilari va boshqalar) qurilavermaydi. Olisdagi joylardagi radiochastota spektri nisbatan bo'sh va 20 MGsgacha kenglikdagi chastotalar polosasini

ajratish ajratish mumkin. Shuning uchun yirik shaharlardan olisdagi korporativ tarmoqlardan WiMAX texnologiyalari imkoniyatlarining maksimal ishlatilishini kutish kerak. Shu bilan birga, bunday tarmoqlar dastlab asosiy qo'llanilishi bo'yicha o'ziga yetarli (qo'shimcha bo'lmagan) tarzda qurilishi mumkin.

WiMAX texnologiyalarining qo'llanilishiga olib keladigan korporativ tarmoqlarning yana bir o'ziga xos xususiyatlaridan biri ko'plab korporatsiyalarda abonent terminallarni sotib olish uchun moliyaviy vositalarning mavjudligi hisoblanadi (hozirda umumiy foydalanishdagi aloqa tarmoqlari abonentlari uchun terminallar narxi juda qimmat bo'lgan holda).

3.5.4. WiMAX texnologiyasining yaqin yillardagi rivojlanish istiqbollari

Hozirgi kunda asosan IEEE 802.16.2004 va IEEE 802.16e versiyalari orqali ma'lum bo'lgan WiMAX standarti kabelli tarmoqlar darajasidagi yuqori o'tkazish qobiliyatini va katta radiusli hududda keng polosali ulanishni ta'minlaydigan simsiz aloqa texnologiyasidir. WiMAX jihozlari 2 – 11 GGs diapazonida 10MGs kenglikdagi bir nechta kanallarda ishlaydi. Turli davlatlarda chastotalarning o'ziga xos tarzda taqsimlanishi WiMAX texnologiyasidan har xil diapazonlarda ishlash imkoniyati zaruratini taqozo etadi. Masalan, WiMAX uchun Shimoliy Amerikada 2,5 GGs va 5 GGs diapazonlari, Markaziy va Janubiy Amerikada 2,5 GGs; 3,5 GGs va 5 GGs diapazonlari, Yaqin Sharq, Afrika, G'arbiy va Sharqiy Yevropada 3,5 GGs va 5 GGs diapazonlari, Osiyo va Tinch okean regionida esa 2,3 GGs; 3,5 GGs va 5 GGs diapazonlaridagi chastotalar ishlatilishi ko'zda tutilgan [17].

Real tizimlarda IEEE 802.16 standartining barcha rejimlari va imkoniyatlari hali o'z ifodasini topmagan bo'lsa-da, yangi texnologiya ishlamoqda va rivojlanmoqda. IEEE 802.16 standartidagi OFDMA TDD rejimini simsiz aloqa global standartlari - IMT-2000 (*IMT-2000 OFDMA TDD WMAN*) tarkibiga kiritish haqidagi XTI ning 2007 yilning 19 oktyabridagi qarori buning tasdig'idir [7]. Shuni yoddan chiqarmaslik kerakki, WiMAX faqat texnologiya sifatidagina emas, balki axborot fazosini qurishdagi yangi yondashuv sifatida ham e'tirof etiladi. Ammo bu texnologiyaning kelgusida qanchalik muvaffaqiyatli bo'lishini mobil aloqaning istiqbolli standartlari (xususan, LTE va

LTE Advanced standartlari) bilan raqobat belgilaydi va buni vaqt ko'rsatadi. Hozircha WiMAX tarmoqlari o'z rivojini davom ettirmoqda, IEEE 802.16 standartlari ham bir joyda turmayapti. Xususan, yaratilish va muhokama etish bosqichida qator yangi to'ldirishlar turibdi. Ayni paytda tizimning ma'lumot almashish tezligini oshirish (100Mbit/sek.dan yuqori), spektral samaradorligini va aloqa sifatini ko'tarish, yangi mobillik (harakat) darajalarini kiritish va foydalanuvchilarning katta guruhlarini samarali qo'llab-quvvatlashni ta'minlaydigan yangi radiointerfeysni ko'zda tutgan IEEE 802.16m loyihasi faol muhokama qilinmoqda. Shu bilan birga, IEEE 802.16 Rev2 standartining aniqlashtirilgan versiyasining paydo bo'lishi ham kutilmoqda. Bu versiyaga ko'p oraliqli rele tarmoqlari bo'yicha to'ldirishlar (802.16j) va boshqa qator hujjatlar kiradi [17].

Nazorat savollari

1. Wimax tizimlarining ishlash printsiplarini tushuntiring
2. Wimax tizimlining arxetekturasini tushuntiring
3. Wimax tarmog'ining ishlash rejimlarini tushuntiring
4. Wimax tarmog'ini tashkil etishning o'ziga xos xususiyatlari qanday?
5. Wimax va Wi-Fi tizimlarini taqqoslang.
6. WiMAX tizimlari uchun radiochastotalarni taqsimlashda butun dunyo an'analari qaysilar?
7. WiMAX tizimlari uchun spektrni ajratishga bog'liq muammolari mavjudmi?
8. Turli chastotalar diapazonlarida spektrning taqsimlanishining o'ziga xos xususiyatlari mavjudmi?
9. WiMAX tizimining afzalliklari va kamchiliklari tushuntiring
10. WiMAX texnologiyasining rivojlanish istiqbollari tushuntiring

4- BOB. SIMSIZ TARMOQLARDA XAVFSIZLIK MASALALARI

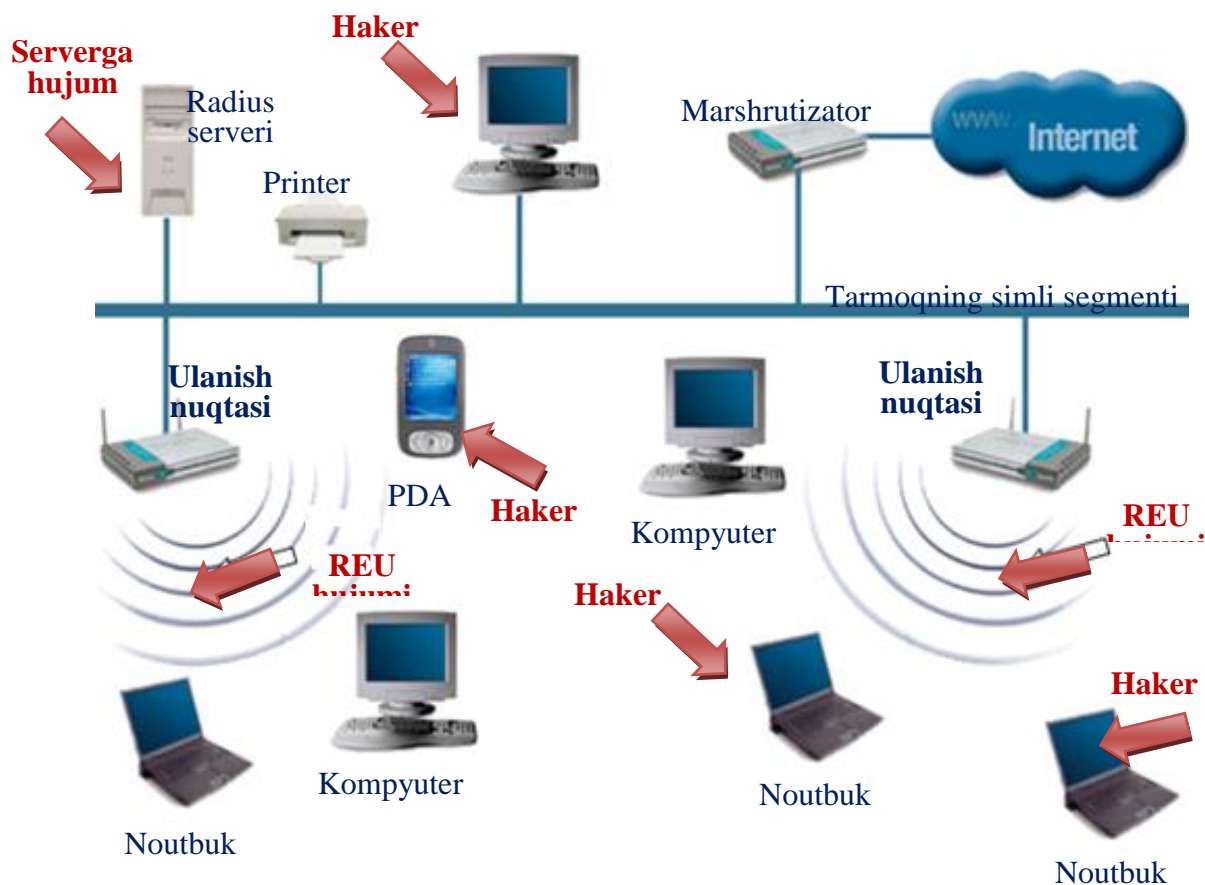
4.1. Wi-Fi simsiz tarmoqlar xavfsizligiga tahdidlar va xavflar

Simsiz tarmoqning xavfsizligini ta'minlash simli tarmoqni himoyalashdan ko'ra yanada murakkab. Himoyalash barcha tarmoqni ishlatadigan va ma'murlashtiradigan shaxslar uchun birinchi o'rinda turishi kerak. Xavfsizlik tizimining umumiy ishlash prinsipi 4.1-rasmda sxematik tasvirlangan [13].



4.1- rasm. Xavfsizlik tizimining umumiy ishlash prinsipi

Ulanish nuqtasining ishlashi diapazonida WLAN tarmog'i ulanish nuqtasi bilan bog'lanish bajariladigan mos ro'yxatga olish ma'lumotlariga ega bo'lgan barcha shaxslar uchun ochiq bo'ladi. Simsiz tarmoq adapteriga ega bo'lish va buzish yo'llarini bilish bilan g'arazgo'y WLAN tarmog'i ulanishni olishi uchun WLAN tarmog'i bo'lgan joyda jismonan bo'lmasligi mumkin (4.2-rasm).



4.2- rasm. WLAN tarmog‘i arxitekturasi va bo‘lishi mumkin hujumlar yo‘nalishi

Xavfsizlik masalalari gap korporativ tarmoqlar haqida borganida yanada katta ahamiyatga ega bo‘ladi, chunki kompaniyaning hayot faoliyati ma’lumotlarning himoyalanganligiga bog‘liq bo‘ladi. Xavfsizlik tizimining buzilishi kompaniyalarga, ayniqsa, agar kompaniya o‘z mijozlarining moliyaviy ma’lumotlari bilan amallarni bajarsa halokatli oqibatlariga olib kelishi mumkin. Simsiz tarmoqlar yanada ko‘plab korxonalarda qurilmoqda va ko‘plab hollarda nafaqat qulay variant, balki tarmoqning juda muhim qismi hisoblanadi. WLAN tarmoqlari hamma vaqt hujumlarga uchrasada, ularning ommaviylikini ortishi bilan ular birinchi raqamli nishon bo‘lib qolmoqda.

Simsiz aloqa tarmoqlarining axborot xavfsizligiga tahdidlar o‘z-o‘zicha emas, balki axborot tarmog‘ida bo‘lgan texnologiyalarning zaifliklari orqali namoyon bo‘ladi.

Xavfsizlikka tahdidlar quyidagilar hisoblanadi:

- a) ma’lumotlarni o‘g‘irlash (nusxa ko‘chirish);
- b) ma’lumotlarni yo‘q qilish;
- c) ma’lumotlarni modifikatsiya qilish(buzish);

- d) ma'lumotlarga foydalana olishni buzish (blokirovkalash);
- e) ma'lumotlarning haqiqiylikni inkor qilish;
- f) xato ma'lumotlarni majburan qabul qildirish.

Axborot xavfsizligiga tahdidlarni tashuvchilar tahdidlar manbalari hisoblanadi. Tahdidlar manbalari ham sub'ektlar (shaxslar), ham ob'ektiv namoyon bo'lishlar qatnashishi mumkin. Binobarin, tahdidlar manbalari ham himoya qilinadigan ob'ektning ichida joylashishi – ichki manbalar, ham uning tashqarisida joylashishi mumkin – tashqi manbalar. Ichki va tashqi manbalarga bo'lish oqlangan, chunki o'sha bir tahdidlar uchun ichki va tashqi manbalarga qarshi turish usullari turlicha bo'lishi mumkin.

Barcha tahdidlar manbalari aniq bir tarmoqlarga ob'ektlarga bog'lanmasdan quyidagilar orqali shartlanadigan uchta asosiy guruhlarga bo'lish mumkin:

- a) sub'ektning ta'sir etishi orqali (tahdidlarning antropogen manbalari);
- b) texnik vositalar orqali (tahdidlarning texnogen manbalari);
- c) tabiiy manbalar orqali.

Ma'lumki, zaiflik deganda buzuvchining atayin yoki tasodifiy ta'sirlarida uning xavfsizligi tizimni buzilish xavfiga uchratadigan apparatlar-dasturiy vositalarida yoki tizimning ishlashishi tashkil etishdagi ma'lum yoki gumon qilinadigan kamchilik tushuniladi, shuning uchun xavfsizlikka tahdidlarning ishlatilishiga yo'naltirilgan buzuvchining istalgan muvaffaqiyatli hujumi mobil aloqa texnologiyalarining qurilishi o'ziga xos xususiyatlari va zaifliklari haqida buzuvchilar tomonidan olingan bilimlarga qat'iy tayanadi.

Shu munosabat bilan buzuvchilar tomonidan mobil aloqa tarmoqlarining zaifliklarining ishlatilishi holatlarida axborot xavfsizligini u yoki bu xarakteristikalarini (konfidensiallik, yaxlitlik va foydalana olishlik) buzilishiga olib kelishi mumkin bo'lgan zaifliklarni o'rganish va tahlil qilish hamda buzuvchi ta'sirlarining bo'lishi mumkin oqibatlarini aniqlash zarur.

Mobil aloqa tarmoqlariga qo'llanilsa bo'ladigan zaifliklarni paydo bo'lishi manbalarini eng umumiy tasniflanishini ko'rib chiqamiz.

Himoya qilish ob'ektlariga yo'naltirilgan qandaydir ta'sirni sodir qilish potensial imkoniyati sifatida tahdidlar o'z-o'zicha emas, balki aniq bir ob'ektda xavfsizlikni buzilishiga olib keladigan zaifliklar (omillar) orqali namoyon bo'ladi.

Ob'ektga xarakterli bo'lgan zaifliklarni undan ajratib bo'lmaydi va ishlash jarayonining kamchiliklari, tizim arxitekturasining xossalari, almashtirish protokollari va interfeyslari, qo'llaniladigan dasturiy ta'minot va apparatlar platformalari, ishlatish va joylashtirish sharoitlari bilan shartlanadi.

Tahdidlar manbalari xavfsizlikni buzish uchun (mulk egasiga, axborotlar foydalanuvchisi yoki egasiga zarar yetkazish) zaifliklarni ishlatishi mumkin. Bundan tashqari, tahdidlar manbalarining zarar yetkazadigan u yoki bu zaifliklarni aktivlashtirishi bo'yicha yomon niyatda bo'lmagan ta'sirlari bo'lishi mumkin.

Har bir tahdid bilan turli zaifliklar taqqoslanishi mumkin. Zaifliklarning yo'q qilinishi yoki sezilarli kuchsizlantirilishi xavfsizlikka tahdidlarning bo'lishi mumkin ishlatilishiga ta'sir qiladi.

Xalqaro amaliyot ko'rsatadiki, simsiz aloqa tarmoqlaridagi axborot xavfsizligi muammosi haligacha yechilmagan. Birinchi navbatda bu efir bo'yicha uzatiladigan ma'lumotlarni qo'lga kiritish deshifrlash va radiokanal orqali axborot tizimiga ruxsat etilmagan ulanish ehtimolining yo'q qilinmaganligiga bog'liq. Bu muammo barcha radiotizimlar uchun odatiy hisoblanadi, binobarin, ularda simli tizimlardan farqli ravishda niqobdan chiqaruvchi belgilar topologik sohada emas, balki axborot-signalli sohada ustunlik qiladi. Bundan tashqari, xavfsiz foydalana olish tarmoqlari sohasidagi mavjud tahdidlarning batafsil modeli va ular bilan kurashish usullari ishlab chiqilmagan.

4.1- va 4.2- jadvallarda tahdidlarning asosiy turlari va ham signalli, ham axborot darajalaridagi tahdidlarning ishlatilishi sharoitlari haqida umumiy ma'lumotlar keltirilgan.

4.1- jadval

Simsiz tarmoqlarda signalli darajadagi tahdidlarning turlari va manbalari

Tahdidlar	Tahdidlarning ishlatilishi sharoitlari	Tizimning zaif elementi
<i>Tabiiy kelib chiqishdagi tahdidlar</i>		

Elektromagnit nurlanishlar	Qabul qilish apparaturasining yomon ekranlashtirilishi, ikkinchi darajali polosalar	Qabullagich
Interferensiya	Qaytaruvchi sirtlarning mavjudligi, antennalarning past joylashtirilishi	Qabullagich, uzatkich
Mexanik surilishlar	Mahkamlanmagan detallarning mavjudligi	Antennalar
<i>Inson faoliyati natijasidag vujudga keladigan (antropogen) tahdidlar</i>		
Ishlab chiqishdagi apparatli va dasturiy xatoliklar	Apparaturaning to'liqsiz testlanishi	Butun tizim
Almashtirish protokoli xatoliklari	Komandalar va direktivalar sohalarida signalli va mantiqiy sohalardagi kesishmalarning mavjudligi	Boshqarish tizimi
Aloqa reglamentini buzish	Protokolning to'liqsiz ishlatilishi	Boshqarish tizimi
Signalni uzatish va qabul qilishdagi xatoliklar	Halaqitlar sharoitlarida ishlash	Qabul qilish va uzatish tizimlari
Asosiy kanaldagi signalni qo'lga kiritish	Qabul qilish apparaturasining mavjudligi	Uzatish kanali
Ikkinchi darajali kanallardagi signalni qo'lga kiritish	Asosiy kanal signalining past filtrlanishi	Ta'minot va yerga ulash zanjirlari
Shifrlashdan oldin va keyin signalni qo'lga kiritish	Kanallarda shifrlanmagan va rasshifrovka qilingan ma'lumotlarning mavjudligi	Qabul qilish va uzatish traktlari

Uzatishni olib borayotgan akustik, vibratsion va boshqa signallarni qo‘lga kiritish	Qabul qilish va uzatish punktlarining foydalana olishliligi	Butun tizim
---	---	-------------

4.2- jadval

Simsiz tarmoqlarda axborot darajasidagi tahdidlarning turlari va manbalari

Tahdidlar	Tahdidlarning ishlatilishi sharoitlari	Tizimning zaif elementi
<i>Ma'lumotlarni qo'lga kiritish</i>		
Qo‘lga kiritish uchun uzatish kanalini aniqlash	Uzatiladigan ma'lumotlarda farqli belgilarning mavjudligi, bitta kanalda ishlash	Kanallarni shifrlash va boshqarish tizimi
Ma'lumotlar formatini aniqlash	Qo‘shimcha tuzatishlarsiz standart formatlardan foydalanish	Kodlash va shifrlash tizimi
Paketlarni (kadrlarni) qayta tiklash	Sinxronlashtirishni niqoblash va foydalana olish markerlarining mavjud emasligi	Almashtirishni boshqarish tizimi
Chiziqli dekodlash	Ma'lumotlarni uzatish statistikasining to‘planishi, uzatishda ishlatilishi mumkinligi	Koder/dekoder
Dekodlangan ma'lumotlarni deshifrovka qilish	Qabul qilinadigan (qo‘lga kiritiladigan) signal asosida korrelyatning mavjudligi, kalitlarning obro‘sizlatirilishi (komprometatsiyasi), shifrlanmagan signal blokining olinishi	Ma'lumotlarni almashtirishni tashkil etish tizimi
<i>Ma'lumotlarni buzish</i>		

Chaqiruvni imitatsiyalash yo‘li bilan xato signalni uzatish	Almashtirish protokoli aniqlanishining mumkinligi	Qabul qilish va uni boshqarish tizimi
Aloqa seansining borishida xato signalni uzatish	Identifikatsion preambulalarning ajratilishi va aniqlanishining mumkinligi	Qabul qilish va uni boshqarish tizimi
Xato ma'lumotlarning qonuniy uzatilishi	Ta'sir etish ob'ektlarining mantiqiy yoki fizik manzillarining mavjudligi	Butun tizim
Uzatish siganlining buzilishi	Sinxronlashtirishning ochilishi va kanalga buzishsiz kirishning mumkinligi	Qabullash-uzatish tizimi
<i>Boshqarishni qo'lg'a kiritish</i>		
Boshqarish ketma-ketliklarini abonentga uzatish	Master-kodlarni olishning, himoya qilish tizimlarining kodlarini obro'sizlantirishning (komprometatsiyasining) mumkinligi	Boshqarish tizimi
Boshqarish ketma-ketliklarini markaziy stansiyaga uzatish	Master-kodlarni olishning, himoya qilish tizimlarining kodlarini obro'sizlantirishning (komprometatsiyasining) mumkinligi, protsessorga va boshqarish dasturlariga foydalana olishning mumkinligi	Uzatish kanali
Boshqarish tizimini qayta dasturlashtirish	Masofadan boshqarish komandalarining mavjudligi, dasturiy ta'minotga foydalana olishning mumkinligi	Markaziy stansiyaning protsessor qurilmalari, boshqarish tizimi

ISO hujjatlarida telekommunikatsiyalar tizimlari xavfsizligiga tahdidlarning turlari va toifalari bo'yicha bo'lingan tasniflanishining bir necha usullari ajratilgan. Bundan tashqari, xavfsizlikka tahdidlarni tahlil qilishda axborot xavfsizligiga barcha tahdidlarning yig'indi ta'sir etish xarakteristikasi ishlatiladi. Bunda tahdidlarning tasniflanishi har bir darajaga tarqatiladi:

- a) alohida elementlardan tashkil topgan *tarmoq infratuzilmasiga*;
- b) *tarmoq xizmatlariga*;
- c) *ilovalarga*.

Uchinchi avlod istiqbolli mobil aloqa tarmoqlari xavfsizligiga tahdidlarning tahlil qilish ko'rsatadiki, ularning ko'pchiligi quyidagilarga olib keladi:

- a) jinoyatchilar xizmatlarga REU oladigan, ya'ni ularning hisoblarini ro'yxatga olingan foydalanuvchi to'laydigan *niqoblanishga*;

- b) foydalanuvchi ma'lumotlari trafigining konfidensialligini, foydalanuvchi joylashgan o'rnining ma'lumotlarini va boshqalarni buzilishini keltirib chiqara oladigan *ma'lumotlarning qo'lga kiritilishiga*;

- c) abonentlarni obuna qilishdagi *firibgarlikka (frodga)*.

Xavfsizlikka tahdidlar turlarini tahlil qilish tahdidlarni identifikatsiya qilishdan iborat:

- a) telekommunikatsiyalar aniq bir tizimida;
- b) "qonuniy qo'lga kiritish" ga qo'yiladigan talablarning bajarilmasligi bilan shartlanadigan;
- c) personal ma'lumotlar bilan;
- d) tarmoqlararo aloqada;
- e) telekommunikatsiyalar tizimining yaxlitligida;
- f) boshqarishda;
- g) xavfsizlik siyosatining muvofiqlashtirilmaganligi tufayli.

Keltirilgan tahdidlar turlaridan har biri axborot xavfsizligiga aniq bir tahdidlarning ko'plab sonlari kiradigan nimko'plik hisoblanadi. Tarmoq taqdim etadigan xizmatlarning har biri bo'yicha tahdidlar har bir turlarining soni o'nlab va yuzlabni tashkil etadi. Ularni identifikatsiya qilish uchun ko'p sonli dastlabki berilganlarga (xususan, ishlash protseduralari bo'yicha qurilmalar ishlab chiqaruvchilaridan) ega bo'lgan mutaxassislar-tahlilchilarning yuqori malakasi zarur bo'ladi.

Shunday qilib, mobil aloqa tarmoqlariga tahdidlarni quyidagi guruhlarga bo‘lish mumkin:

- a) ma’lumotlarga REU;
- b) yaxlitlikka tahdidlar;
- c) xizmat ko‘rsatishda rad etish;
- d) o‘z o‘rniga ega bo‘lgan harakatlarning rad etilishi yoki inkor qilinishi;
- e) xizmatlarga ruxsat etilmagan foydalana olish.

Jinoyatchi ishlatadigan eng xavfli tahdidlar va maqsadlar 4.3-jadvalda keltirilgan.

4.3- jadval

Mobil aloqa tarmoqlaridagi xavfsizlikka eng xavfli tahdidlar ro‘yxati

Tahdidning nomi	Buzuvchining maqsadlari
Foydalanuvchi trafigiga REU	Ma’lumotlarga foydalana olish
Boshqarish signallariga va ma’lumotlariga REU	Yanada samaraliroq hujumlarga tayyorgarlik ko‘rishni tahlil qilish
Kommunikatsiyalar qatnashuvchisi yoki tarmoqqa xizmat ko‘rsatuvchi ostida niqoblanish	Trafikni, boshqarish signallari va ma’lumotlarini qo‘lga kiritish, keyingi hujumlarda foydalanish uchun qonuniy foydalanuvchilar haqidagi ma’lumotlarni olish
Trafikni aktiv va passiv tahlil qilish	Tarmoqqa keyingi foydalana olish uchun ma’lumotlarni aniqlash
Ro‘yxatga olingan foydalanuvchi ostida niqoblanish	Xizmatlarga to‘lovsiz foydalana olish
Ilovalar va ma’lumotlar yaratuvchisi ostida niqoblanish	Terminalni blokirovkalash, tarmoqning ishlashini buzish

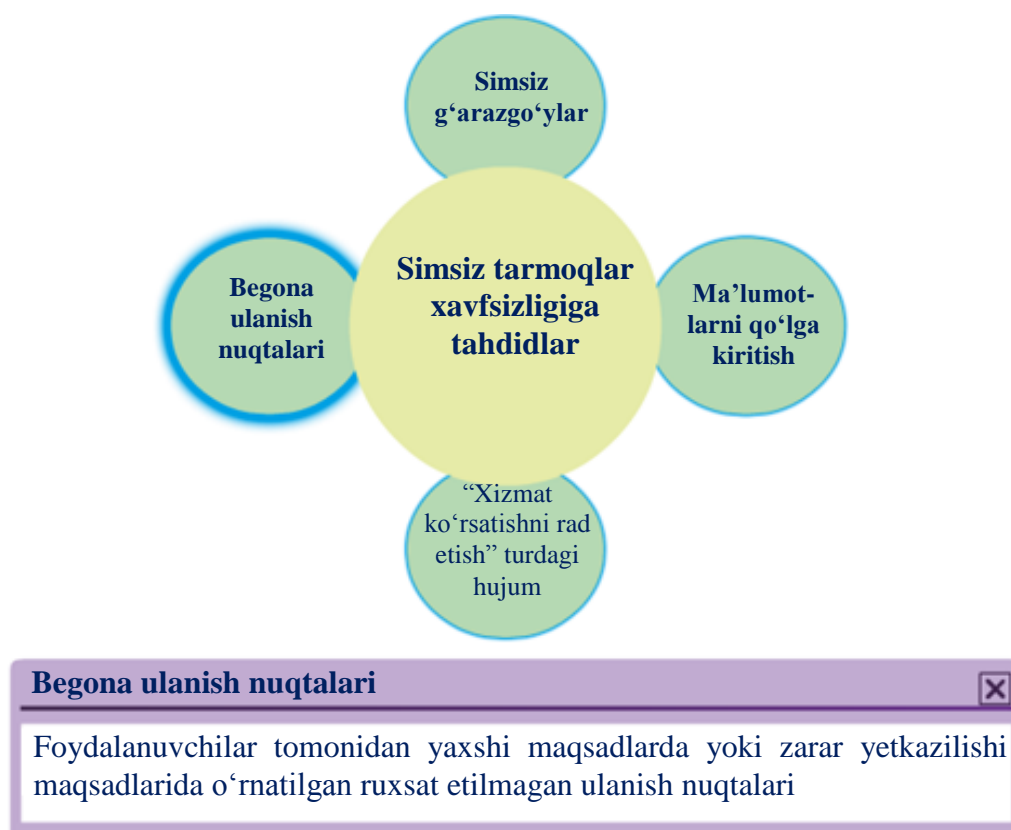
Foydalanuvchi imtiyozlaridan noto'g'ri foydalanish	Xizmatlarga to'lovsiz foydalana olish
Abonentdan g'irlangan terminal va universal integratsiyalangan tarmoq kartasidan (Universal Integrated Circuit Card, UICC), foydalanish	Boshqalar hisobiga xizmatlarga to'lovsiz foydalana olish
IMEI-terminal mobil qurilmasining xalqaro identifikatsion nomerini o'zgartirish	O'g'irlangan terminaldan foydalanish
Abonentning terminallarida va universal identifikatsiya qilish modulidagi (Universal Subscriber Identity Module, USIM) ma'lumotlar yaxlitligining buzilishi	Xizmatlarga foydalana olishni blokirovkalash
UICC/USIM dagi identifikatsion ma'lumotlar konfidensialligining buzilishi	Xizmatlarga ruxsat etilmagan foydalana olish

Xalqaro amaliyot ko'rsatadiki, axborot xavfsizligi muammosi u va boshqa operatorlar nuqtai nazaridan mobil aloqa tarmoqlarini umumiy foydalanishdagi telekommunikatsiyalar tarmoqlariga ulanganida vujudga keladi. Mobil aloqa tizimlaridagi huquqbuzarliklarning ortishi fonida axborot hujumlarini aks ettiradigan va huquqbuzarlarni aniqlaydigan axborot xavfsizligini ta'minlashning zamonaviy choralari, usullari va vositalarini tadqiq qilish zarur. Simsiz aloqa tarmoqlarining axborot xavfsizligini ta'minlash masalasi xavfsizlikka tahdidlar va zaifliklarni tahlil qilishni, ishlashishini monitoring qilishni va qarshi turishning mos choralari ko'rishni o'z ichiga oladi.

Xavfsizlik masalalari gap korporativ tarmoqlar haqida borganida yanada katta ahamiyatga ega bo'ladi, chunki kompaniyaning hayot

faoliyati ma'lumotlarning himoyalanganligiga bog'liq bo'ladi. Xavfsizlik tizimining buzilishi kompaniyalarga, ayniqsa, agar kompaniya o'z mijozlarining moliyaviy ma'lumotlari bilan amallarni bajarsa halokatli oqibatlariga olib kelishi mumkin. Simsiz tarmoqlar yanada ko'plab korxonalarda qurilmoqda va ko'plab hollarda nafaqat qulay variant, balki tarmoqning juda muhim qismi hisoblanadi. WLAN tarmoqlari hamma vaqt hujumlarga uchrasada, ularning ommaviyligini ortishi bilan ular birinchi raqamli nishon bo'lib qolmoqda.

Hujumlar tashqi shaxslar va norozi xodimlar tomonidan uyushtirilishi mumkin, lekin bundaylardan tashqari, hujum istalgan xodim tomonidan atayin bo'lmagan holda uyushtirilishi mumkin (4.2-rasm) [13].



4.2- rasm. Simsiz tarmoqlar xavfsizligiga umumiy tahdidlar

Simsiz tarmoqlar asosan quyidagi tahdidlarga uchraydi:

- simsiz g'arazgo'ylar;
- zarar yetkazadigan ilovalar;
- ma'lumotlarni qo'lga kiritish;
- DoS-hujumlar.

Quyida simsiz tarmoqqa DoS-hujumlarining vujudga kelishi sabablari keltirilgan.

Qurilmalarning noto'g'ri sozlanishi – konfiguratsiya xatoliklari WLAN tarmog'ini o'chirilishi sababi bo'lishi mumkin. Masalan, ma'mur konfiguratsiyani tasodifan o'zgartirishi va tarmoqni uzishi yoki g'arazgo'y ma'mur huquqlari orqali WLAN tarmog'ini atayin o'chirishi mumkin.

Simsiz tarmoq bo'yicha ma'lumotlarni almashishga atayin to'sqinlik qiladigan g'arazgo'y – bunday g'arazgo'ylar simsiz tarmoqni to'liq yoki ruxsat etilgan qurilmalar muhitga ulana olmaydigan darajagacha o'chirishga urinadi.

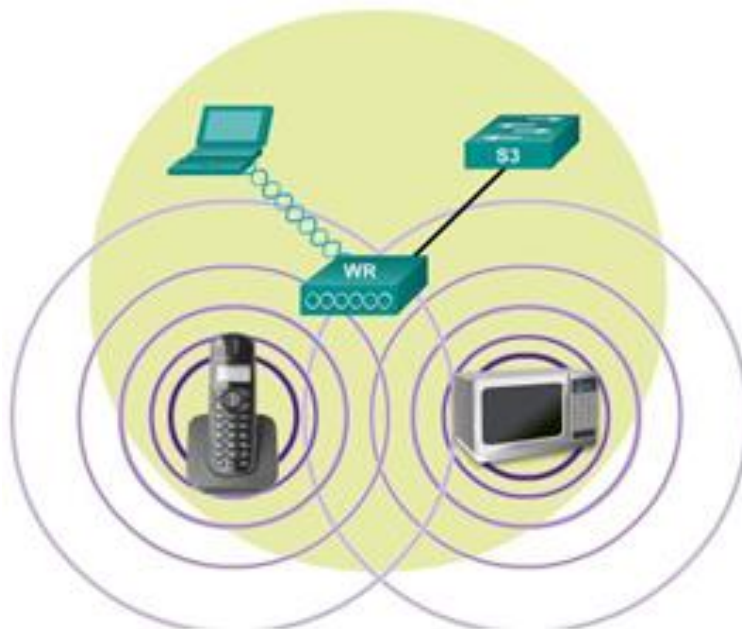
Tasodifiy halaqitlar – WLAN tarmog'i ditsenziyalanmaydigan chastotalar polosalarida ishlaydi va demak barcha simsiz tarmoqlar xavfsizlik funksiyasiga bog'liq bo'lmagan holda boshqa simsiz qurilmalardan halaqitlar ta'siriga uchraydi. Tasodifiy halaqitlar mikroto'lqinli pechlar, radiotelefonlar, radioenagalar va boshqalar kabi qurilmalarning ishlashi natijasida vujudga keladi. 2,4 GGsli polosa 5 GGsli polosaga qaraganda ko'proq halaqitlar ta'siriga uchraydi.

Qurilmalarning noto'g'ri sozlanishi va zarar yetkazuvchi hujumlar natijasidagi DoS-hujumlar xavfini minimallashtirish uchun barcha qurilmalarning himoyalanganligini ta'minlash, parollarni ishonchli joyda saqlash, zaxira nusxalarini yaratish va konfiguratsiyani faqat ishdan tashqari soatlarda o'zgartirish kerak bo'ladi.

Tasodifiy halaqitlar faqat boshqa simsiz qurilmalar ishlaganida vujudga keladi. Optimal yechim WLAN tarmog'ini halaqitlar bilan bog'liq muammolarini monitoring qilish va ularning vujudga kelishi bilan bunday muammolarni yechilishi hisoblanadi. Binobarin, 2,4 GGs polosa katta darajada halaqitlar ta'siriga uchraydi, eng kuchsiz zonalarda 5 GGs polosadan foydalanish mumkin. WLAN tarmoqlari uchun ayrim yechimlar ulanish nuqtalari bilan kanallarni avtomatik sozlanishini ta'minlaydi, halaqitlarni kompensatsiyalash uchun 5 GGs polosadan foydalanishga imkon beradi. Masalan, 802.11n/ac/ad standartining ayrim yechimlari halaqitlarga qarshi turish uchun avtomatik sozlanadi.

4.3-rasmda radiotelefon yoki mikroto'lqinli pech WLAN tarmog'i bo'yicha ma'lumotlarni almashlash uchun halaqitlarni hosil qilishi mumkinligi tasvirlangan.

Cisco CleanAir texnologiyasi 802.11 standartiga kirmaydigan halaqitlar manbalarini aniqlash va topishga imkon beradi. Bu texnologiya muhitdagi o'zgarishlarga avtomatik moslasha oladigan tarmoqni yaratadi.



Oddiy foydalanuvchilar qurilmalari WLAN tarmog'i qurilmalarining ishlashiga halaqitlarni hosil qilishi mumkin, bu xizmat ko'rsatishni rad etishga olib kelishi mumkin

4.3- rasm. Tasodifiy halaqitlar

4.2. Boshqarish kadrlaridan foydalaniladigan DOS – hujumlar

Ehtimoli kam bo'lsada, g'arazgo'ylar tasodifiy halaqitlarni hosil qiladigan radioelektron qarshi turish qurilmalaridan foydalanish bilan atayin DoS-hujumlarni uyushtirishi mumkin. Ehtimolligi kattaki, g'arazgo'ylar ulanish nuqtasining resurslarini ishlatish bilan boshqarish kadrlarini o'zgartirishga urinadi va kanallarni shunchalik yuklaydiki, ular ruxsat etilgan foydalanuvchilar trafigiga xizmat ko'rsata olmaydi [13].

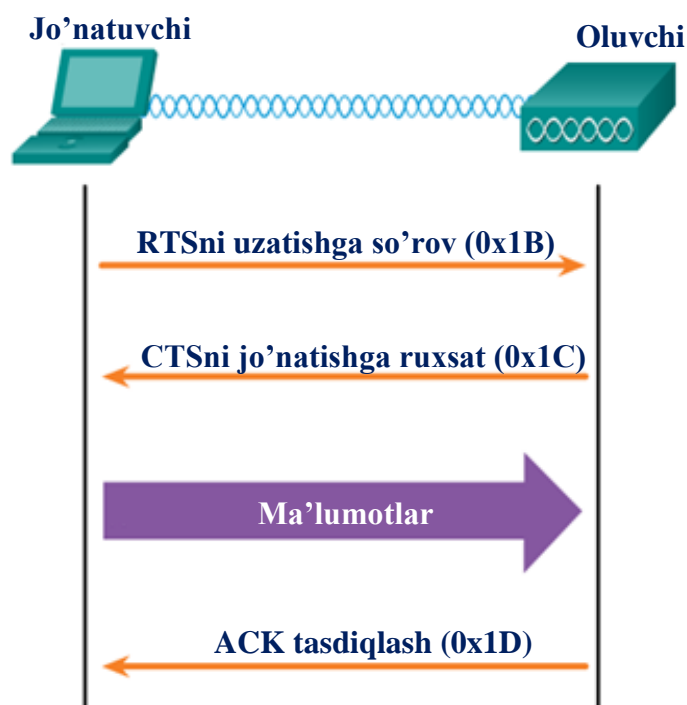
Boshqarish kadrlarini har xil DoS-hujumlarini tashkil etish uchun ishlatish mumkin. Boshqarish kadrlaridan foydalaniladigan ikkita turlardagi hujumlar keng tarqalgan.

Xato uzish yo'li bilan hujum — bunday hujumni amalga oshirish uchun g'arazgo'y BSS chegaralaridagi barcha simsiz qurilmalarga “bog'lanishni bekor qilish” komandalari to'plamini jo'natadi. Bu

komandalar barcha mijozlarning uzilishini keltirib chiqaradi. Uzilganida barcha mijozlar birdaniga takroran bog‘lanishni bajarishga urinadi, bu trafik hajmini keskin ortishiga olib keladi. G‘arazgo‘y bog‘lanishni bekor qilish kadrlarini jo‘natishni davom ettiradi va sikl takrorlanadi.

CTS kadrlarini jo‘natishga ruxsat etishlar ko‘chkisimon hujumi — bu turdagi hujum barcha qolgan simsiz mijozlar uchun o‘tkazish polosasi va ulanishni rad etishni monopollashtirish uchun CSMA/CA muhitida qarama-qarshiliklarni hal etish usulidan foydalanganida vujudga keladi. Buning uchun g‘arazgo‘y soxta STAgA CTS kadrlarini jo‘natishga ruxsat etishlarni BSSga ko‘chkisimon tarqatadi. Radiochastotalar muhitini birgalikda ishlatadigan barcha qolgan simsiz mijozlar CTS kadrlarini qabul qiladi va g‘arazgo‘y CTS kadrlarini uzatishni to‘xtatmaguncha ma‘lumotlar uzatishni bajarishdan to‘xtaydi.

4.4-rasmda simsiz mijoz va ulanish nuqtasi muhitga ulanish uchun CSMA/CA usulini qanday ishlatishi tasvirlangan.



4.4- rasm. CSMA/CA usulidan foydalaniladigan normal rejimda ishlash

4.5-rasmda g‘arazgo‘y soxta simsiz mijozga CTS kadrlarini ko‘chkisimon tarqatilishini hosil qilishi tasvirlangan. Endi barcha qolgan mijozlar CTS kadrda berilgan davrning tugashini kutishga

majbur bo‘ladi. Lekin g‘arazgo‘y CTS kadrlarini jo‘natishni davom ettiradi. Natijada qolgan mijozlar doimo kutishga majbur bo‘ladi. Shunday qilib, g‘arazgo‘y muhitni nazorat qiladi.

Izoh. Bu boshqarish kadrlaridan foydalaniladigan hujumlarga bitta misol xolos. Ko‘plab boshqalari ham mavjud.



4.5- rasm. CTS kadrlarni jo‘natishga ruxsat etishlar ko‘chkisimon DOS hujumini hosil qiladigan g‘arazgo‘y

Bunday hujumlarning vujudga kelishi xavfini kamaytirish uchun Cisco korporatsiyasi qator yechimlarni, shu jumladan kadrlar va qurilmalar spufingidan himoyalash uchun Cisco Management Frame Protection (MFP) funksiyasini ishlab chiqdi. Cisco Adaptive Wireless suqilib kirishlarni oldini olish tizimi bu yechimni hujumlar signaturalarini taqqoslash yo‘li bilan oldingi bosqichlarda suqilib kirishlarni aniqlash funksiyalari bilan to‘ldiradi.

IEEE 802.11 standart bo‘yicha qo‘mitasi ham simsiz tarmoqlar xavfsizligi ikkita standartini ishlab chiqdi. Cisco MFP funksiyasidan foydalanadigan 802.11i standarti simsiz tarmoqlar uchun xavfsizlik mexanizmlarini aniqlaydi, shu bilan bir vaqtda 802.11w boshqarish kadrlarini himoyalash standarti boshqarish kadrlarini o‘zgartirilishiga bog‘liq muammolarni hal etishga yo‘naltirilgan.

4.3. Zararli ulanish nuqtalari

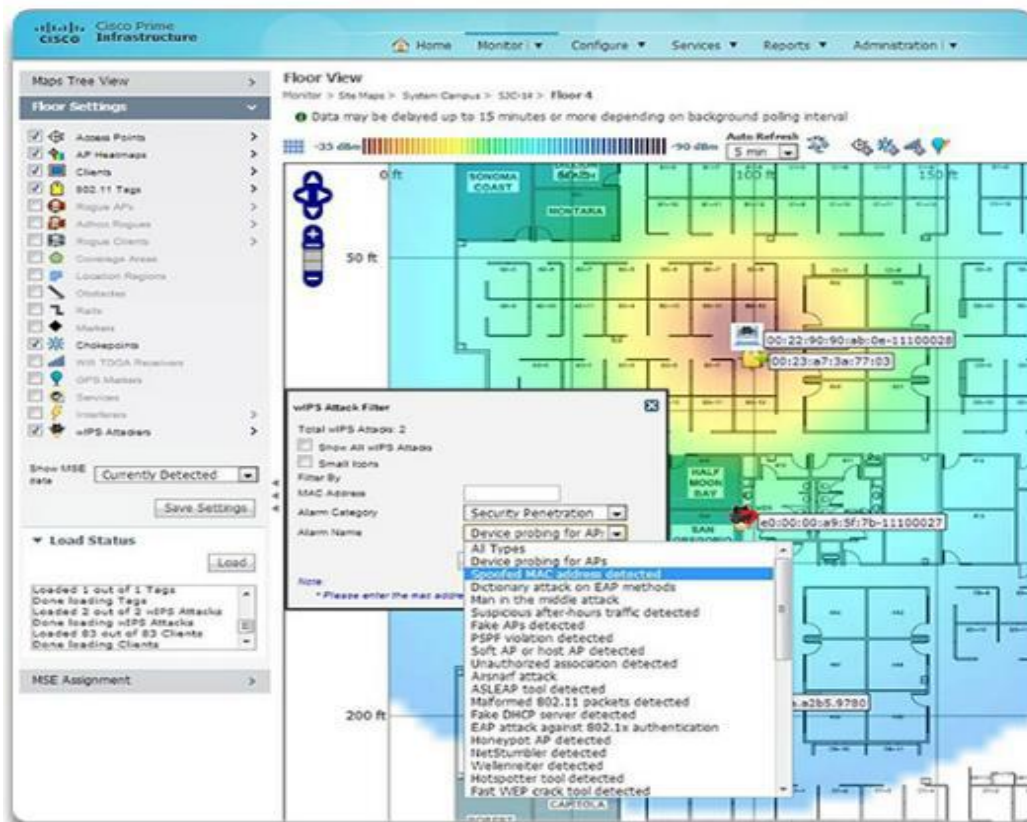
Zararli ulanish nuqtalari simsiz marshrutizator hisoblanadi, uni quyidagicha xarakterlash mumkin [13].

Bunday marshrutizator yaqqol mualliflashtirishsiz va korporativ siyosatning buzilishida korporativ tarmoqqa ulanadi. Ob'ektlarga ulanishga ega bo'lgan istalgan foydalanuvchi himoyalangan tarmoq resurslariga ulanishni nazariy ta'minlaydigan uncha qimmat bo'lmagan simsiz marshrutizatorni (g'arazli maqsadlarda) o'rnatishi mumkin.

G'arazgo'y mijozning ma'lumotlarini qo'lga kiritish (masalan, simsiz mijozlarning MAC-manzillari) yoki tarmoqning resurslariga ulanishni olish uchun ma'lumotlar paketlarini qo'lga kiritishi va niqoblashi yoki qo'lga kiritish bilan hujumni uyushtirish maqsadlarida bunday marshrutizatorni ulashi mumkin.

Personal ulanish nuqtasini qanchalik oddiy yaratishni ham hisobga olish kerak bo'ladi. Masalan, tarmoqqa himoyalangan ulanishga ega bo'lgan foydalanuvchi Wi-Fi tarmog'iga ulanish nuqtasi sifatida o'z mualliflashtirilgan Windows tugunini sozlaydi. Bunda ruxsat etilmagan qurilmalar xavfsizlik choralarini aylanib o'tadi va bitta umumiy qurilma sifatida tarmoq resurslariga ulanishni oladi.

Zararli ulanish nuqtalarining o'rnatilishini oldini olish uchun tashkilotlar ruxsat etilmagan ulanish nuqtalarining borligiga radiosignallar chastotalarini aktiv monitoring qilish uchun dasturiy ta'minotni ishlatishi kerak. Masalan, 4.6-rasmda Cisco Prime infratuzilmasi tarmoqlarini boshqarish uchun dasturiy ta'minot ekrani suratida radiochastotalar xaritasi tasvirlangan bo'lib, u aniqlangan soxta MAS-manzilli g'arazgo'yning joylashish o'rnini aniqlaydi.



4.6- rasm. Begona ulanish nuqtasi aniqlanganidagi ekranning ko‘rinishiga misol

Izoh. Cisco Prime tarmoq haqidagi barcha ma’lumotlarni umumiy taqdim etish va markazlashtirilgan joylashtirishni ta’minlash orqali boshqa o‘xshash dasturlar bilan o‘zaro ta’sirlashishadigan tarmoqlarni boshqarish uchun dasturiy ta’minot hisoblanadi. Bu DT juda yirik tashkilotlarda o‘rnatiladi.

4.4. Qo‘lga kiritish bilan hujum qilish

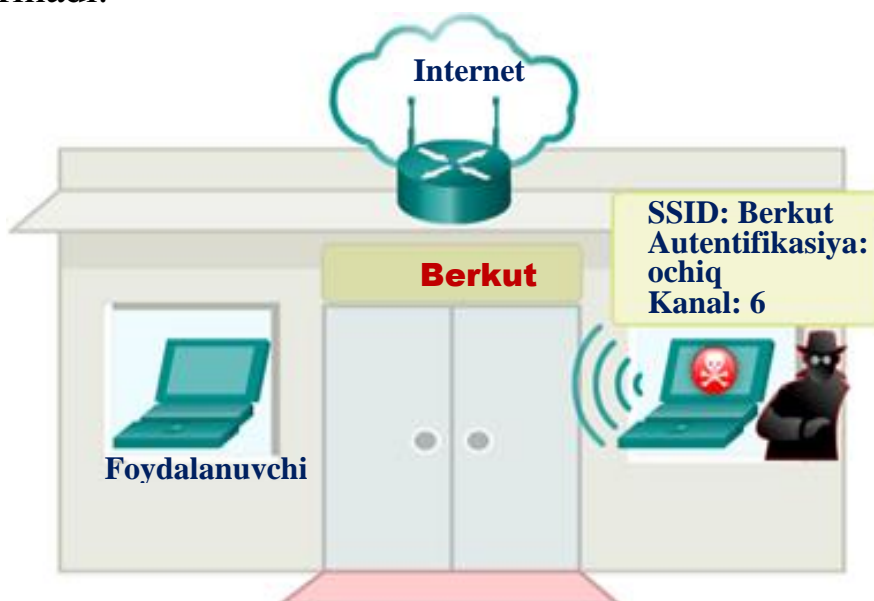
G‘arazgo‘y qo‘llashi mumkin bo‘lgan eng murakkab hujumlardan biri qo‘lga kiritish bilan hujum qilish hisoblanadi. Qo‘lga kiritish bilan hujum qilishning ko‘plab yo‘llari mavjud [13].

Bunday hujumlarning eng keng tarqalgan turlaridan biri “yovuz o‘xshash” deyiladi, uning doirasida g‘arazgo‘y zararli ulanish nuqtasini kiritadi va uning ruxsat etilgan ulanish nuqtasidagi kabi SSID nomidan foydalanish bilan sozlaydi. Wi-Fi tarmog‘iga bepul ulanish taklif etiladigan joylar, masalan, aeroportlar, kafe va restoranlar bunday turdagi hujumlar uchun eng ommaviy nishon

hisoblanadi, chunki bunday ob'ektlarda ochiq autentifikatsiyalash ishlatiladi.

Simsiz mijozlar ulanganida simsiz ulanishni taklif etadigan ikkita ulanish nuqtasi aks etadi. Zararli ulanish nuqtasining yonida turganlar quvvatliroq signalni aniqlaydi va “yovuz o‘xshash” ulanish nuqtasi bilan bog‘lanishni bajaradi. Endi foydalanuvchi trafigi begona ulanish nuqtasiga jo‘natiladi, u o‘z navbatida, ma’lumotlarni qo‘lga kiritadi va ularni ishonchli ulanish nuqtasiga qayta uzatadi. Ruxsat etilgan ulanish nuqtasidan teskari trafik zararli ulanish nuqtasiga jo‘natiladi, qo‘lga kiritiladi, keyin esa hech narsani shubha qilmaydigan stansiyaga (STA) jo‘natiladi. G‘arazgo‘y foydalanuvchining parolini, shaxsiy ma’lumotlarini o‘g‘irlashi, tarmoqqa ulanishni olishi va foydalanuvchining tizimini oshkora etishi mumkin.

Masalan, 4.7- rasmda g‘arazgo‘y “Berkut” kafesida joylashgan va hech narsani shubha qilmaydigan simsiz mijozlar trafiginini qo‘lga kiritishga urinadi.



4.7- rasm. G‘arazgo‘y “yovuz o‘xshash” hujumini boshlaydi

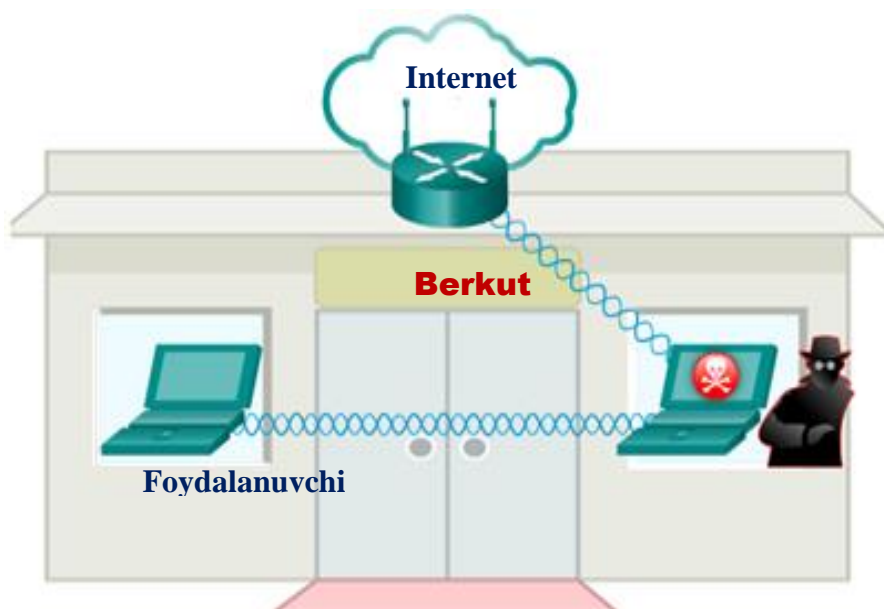
G‘arazgo‘y o‘zining noutbukini ruxsat etilgan simsiz marshrutizatoridagi kabi o‘sha SSID va kanalga ega bo‘lgan “yovuz o‘xshash” turdagi ulanish nuqtasi qiladigan dasturiy ta’minotni ishga tushiradi.

Qo‘lga kiritish orqali hujumlarni oldini olish muvafaqiyati WLAN tarmog‘i infratuzilmasining murakkabligiga va tarmoqni sinchiklab monitoring qilinishiga bog‘liq bo‘ladi. Jarayon WLAN tarmog‘idagi ruxsat etilgan qurilmalarni aniqlashdan boshlanadi. Buning uchun foydalanuvchilar autentifikatsilash jarayonidan

o'tishlari kerak bo'ladi. Barcha ruxsat etilgan qurilmalar aniqlanganidan keyin shubhali qurilmalar yoki trafik borligiga tarmoqni monitoring qilishni bajarish mumkin bo'ladi.

4.8- rasmda foydalanuvchi ikkita mumkin bo'lgan simsiz ulanishni ko'radi va bog'lanish uchun "yovuz o'xshash" turdagi ulanish nuqtasini tanlaydi. G'arazgo'y foydalanuvchining ma'lumotlarini qo'lga kiritadi va ularni ruxsat etilgan ulanish nuqtasiga qayta uzatadi, u esa o'z navbatida, "yovuz o'xshash" turdagi ulanish nuqtasiga teskari javob trafigini jo'natadi. "Yovuz o'xshash" turdagi ulanish nuqtasi javob trafigini qo'lga kiritadi va ma'lumotlarni hech narsani shubha qilmaydigan foydalanuvchiga qayta uzatadi.

Eng zamonaviy WLAN qurilmalari ishlatiladigan WLAN korporativ tarmoqlari ma'murlarga suqulib kirishlarning oldini olish simsiz tizimi (IPS) sifatida kompleksda ishlaydigan instrumentlarni taqdim etadi. Bunday instrumentlar yordamida zararli ulanish nuqtalari va bir darajali tarmoqlar aniqlanadigan skanerlar, shuningdek ulanish nuqtasining aktivligi va yuklanishiga radiochastotalar spektrini monitoring qilishni amalga oshiradigan radioresusrlarni boshqarish instrumentlari kiradi. Ulanish nuqtasiga katta yuklama ruxsat etilmagan yuklamaning bo'lishi mumkin borligi haqida xabar beradi.



4.8- rasm. "Yovuz o'xshash" turdagi hujum muvaffaqiyatli amalga oshirildi

Simsiz tarmoqlarda ma'lumotlarning yaxlitligi va konfidensialligini ta'minlash uchun kriptografik vositalar qo'llaniladi. Lekin xatoliklar kommunikatsiyalarning buzilishiga va g'arazgo'ylar tomonidan ma'lumotlarni ishlatilishiga olib keladi.

4.5. Simsiz tarmoqlarda qo'llaniladigan kriptografiya usullari

Kriptografiya deb - kodlangan xabarlarini tuzish va ochish haqidagi fanga aytiladi. Kriptografiya *autentifikatsiyalash*, *yaxlitlik* va *konfidensiallik* mexanizmlari uchun muhim element hisoblanadi [13].

Autentifikatsiyalash ma'lumotlarni uzatuvchi yoki oluvchining shaxsini tasdiqlash vositasi bo'lib xizmat qiladi. Yaxlitlik ma'lumotlar o'zgartirilmaganligini bildiradi, konfidensiallik esa ma'lumotlarni jo'natuvchi va oluvchidan tashqari hech kimga tushunarli bo'lmasligini ta'minlaydi. Odatda kriptografik mexanizmlar algoritmi (matematik funksiya) va maxfiy kattalik (kalit) ko'rinishida bo'ladi.

Autentifikatsiyalash, ma'lumotlarning yaxlitligi va konfidensialligi uchta kriptografik funksiyalar - simmetrik shifrlash, asimmetrik shifrlash va xesh-funksiyalar orqali ta'minlanadi.

Simmetrik shifrlash. Ko'pincha maxfiy kalitlar yordamida shifrlash deyiladigan simmetrik shifrlash asosan ma'lumotlarning konfidensialligini ta'minlash uchun ishlatiladi. Ma'lumotlarning konfidensialligini ta'minlash uchun abonentlar ma'lumotlarni shifrlash va deshifrlash uchun ishlatiladigan yagona matematik algoritmi birgalikda tanlashi kerak. Bundan tashqari, ular qabul qilgan shifrlash/deshifrlash algoritmi bilan ishlatiladigan umumiy kalitni (maxfiy kalitni) tanlash kerak bo'ladi.

Simmetrik shifrlashga misol 4.9- rasmda keltirilgan.



4.9- rasm. Simmetrik shifrlashga misol

Bugungi kunda Data Encryption Standard (DES), 3DES (yoki «uchtalik DES») va International Data Encryption Algorithm (IDEA) kabi maxfiy kalitlar algoritmlari keng ishlatiladi. Bu algoritmlar 64

bitlardan bloklar bilan xabarni shifrlaydi. Agar xabarning hajmi 64 bitdan oshsa (odatdagidek), uni har birida 64 bitdan bloklarga bo‘lish, keyin esa ularni qandaydir tarzda birlashtirish kerak bo‘ladi. Bunday birlashtirish quyidagi to‘rtta usullardan biri orqali amalga oshiriladi:

- elektron kod kitobi bilan (Electronic Code Book - ECB);
- shifrlangan bloklar zanjiri bilan (Cipher Block Changing - CBC);
- x-bitli shifrlangan teskari aloqa bilan (Cipher FeedBack - CFB-x);
- chiqish teskari aloqa bilan (Output FeedBack - OFB).

Maxfiy kalit bilan shifrlash ko‘pincha ma’lumotlarning konfidensialligini ta’minlash uchun ishlatiladi va o‘zgartirilmaydigan “tikilgan” dasturlar (firmware) yordamida juda samarali amalga oshiriladi. Bu usulni autentifikatsiyalash va ma’lumotlarni yaxlitligini ta’minlash uchun ishlatish mumkin, lekin raqamli imzo usuli samaraliroq hisoblanadi.

Maxfiy kalitlar usulini kamchiliklari quyidagilar hisoblanadi:

- maxfiy kalitlarni tez-tez almashtirish kerak, chunki doimo ularni tasodifan ochilishi xavfi mavjud;
- maxfiy kalitlarning xavfsiz generatsiyalanishi va tarqatilishini ta’minlash qiyin.

Asimmetrik shifrlash. Asimmetrik shifrlash ko‘pincha umumiy kalit bilan shifrlash deyiladi, bunda turli, lekin bir-birlarini o‘zaro to‘ldiradigan kalitlar, shifrlash va deshifrlash algoritmlari ishlatiladi. Umumiy kalit orqali shifrlashdan foydalanish bilan aloqani o‘rnatish uchun har ikkala tomonlarga ikkita umumiy va xususiy kalitlarni olish kerak bo‘ladi (4.10-rasm). Ma’lumotlarni shifrlash va deshifrlash uchun tomonlar turli kalitlarni ishlatadi.



4.10- rasm. Asimmetrik shifrlash

Umumiy kalitlar algoritmlaridan foydalanish maqsadlariga quyidagilar kiradi:

- ma'lumotlarning konfidensialligini ta'minlash;
- jo'natuvchini autentifikatsiyalash;
- birgalikda foydalanish uchun umumiy kalitlarni xavfsiz olish.

Umumiy/xususiy kalitlarni generatsiyalash mexanizmlari yetarlicha murakkab hisoblanadi, lekin natijada juda katta tasodifiy sonlar bilan juftliklar olinadi, ulardan bittasi umumiy kalit, boshqasi esa xususiy kalit bo'ladi. Bunday sonlarni generatsiyalash katta protsessorlar quvvatlarini talab qiladi, chunki bu sonlar, ularning ko'paytmalari qat'iy matematik mezonlarga javob berishi kerak. Lekin bu jarayon har bir umumiy/xususiy kalitlar juftligining noyobligini ta'minlash uchun juda kerak bo'ladi. Umumiy kalitlar yordamida shifrlash algoritmlari unumdorlikni cheklashi tufayli ma'lumotlarning konfidensialligini ta'minlash uchun kam ishlatiladi. Buning o'rniga ular ko'pincha autentifikatsiyalash, raqamli imzo va kalitli boshqarish yordamida amalga oshiriladigan ilovalarda ishlatiladi.

Eng ma'lum umumiy kalitlar algoritmlaridan RSA (Rivest-Shamir-Adleman, Rivest-SHamir-Adelman) va ElGamal (El-Gamal) algoritmlarini keltirish mumkin.

Xavfsiz xesh-funksiya. Xavfsiz xesh-funksiya deb hisoblash oson, lekin teskari qayta tiklash deyarli mumkin bo'lmaydigan funksiyaga aytiladi. Kirish xabari matematik funksiya (xesh-funksiya) orqali o'tkaziladi va natijada chiqishda qandaydir bitlar ketma-ketligi olinadi (4.11-rasm). Bu ketma-ketlik "xesh" (yoki "xabarga ishlov berish natijasi") deyiladi. Xesh-funksiya istalgan uzunlikdagi xabarni qabul qiladi va chiqishda qayd etilgan uzunlikdagi xeshni beradi.

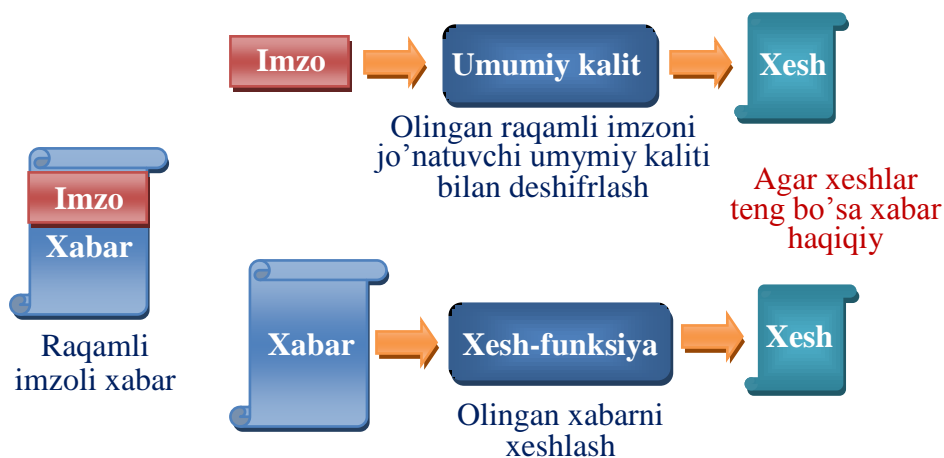
Oddiy xesh-funksiyalar quyidagilarni o'z ichiga oladi:

- Message Digest 4 (MD4) algoritmi;
- Message Digest 5 (MD5) algoritmi;
- xavfsiz xesh algoritmi (Secure Hash Algorithm - SHA).



4.11- rasm. Xesh-funksiyani hisoblash

Raqamli imzo. Raqamli imzo hujjatga qo‘shiladigan shifrlangan xesh hisoblanadi. Raqamli imzo bilan shifrlash prinsipini 4.12- rasm tushuntiradi.



4.12- rasm. Raqamli imzo bilan xabarning haqiqiyligini tekshirish

U jo‘natuvchini va hujjatning yaxlitligini autentifikatsiyalash uchun ishlatilishi mumkin. Raqamli imzolarni xesh-funksiyalar va umumiy kalitlar kriptografiyasi birligi yordamida yaratish mumkin.

Raqamli sertifikat. Raqamli sertifikat deb raqamli imzoli xabarga aytiladi, u hozirgi vaqtda umumiy kalitning haqiqiyligini tasdiqlash uchun ishlatiladi. Eng keng tarqalgan X.509 sertifikatning umumiy formati quyidagi elementlarni o‘z ichiga oladi:

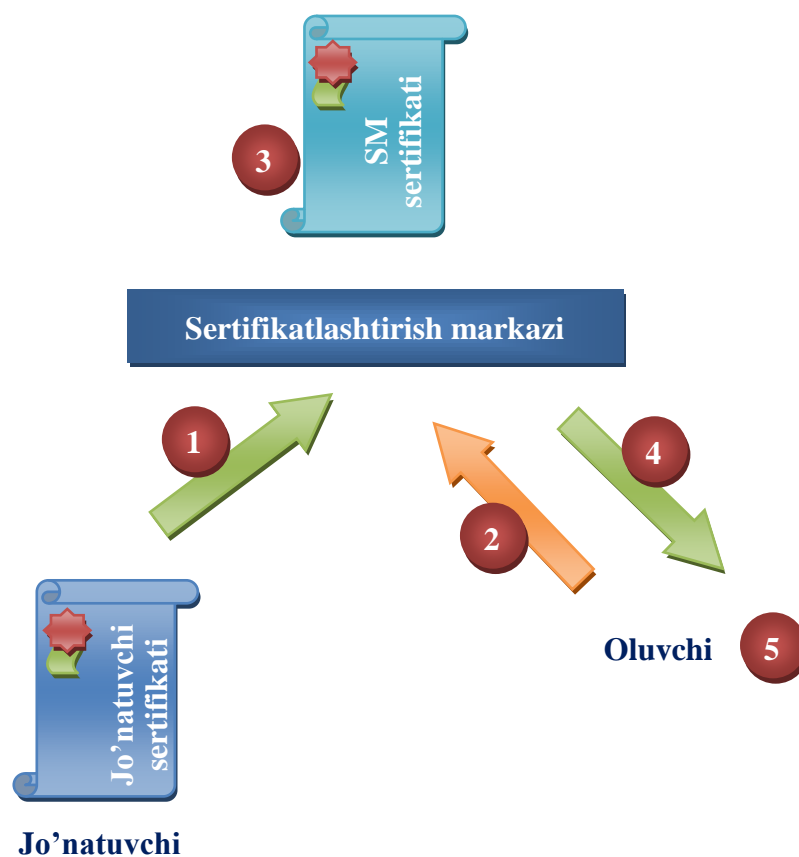
- versiyalar;
- sertifikatning turkum raqami;
- algoritm haqidagi ma’lumotlar emitenti;
- sertifikat emitenti;
- sertifikatning amal qilishni boshlanishi va tugashi;
- sertifikat sub’ekti umumiy kalit algoritmi haqidagi ma’lumotlar;
- emissiyalaydigan tashkilotning imzosi.

Sertifikatni beradigan emissiyalaydigan tashkilot yoki *sertifikatlashtirish markazi* (Certification Authority - CA) to‘liq ishoniladigan ishonchli uchinchi tomon hisoblanadi. Umumiy kalitni uzatilishi quyidagicha bo‘lib o‘tadi (4.13- rasm):

- jo‘natuvchi umumiy kalitni o‘z ichiga oladigan sertifikatni yaratadi;
- oluvchi sertifikatlashtirish markazidan jo‘natuvchining sertifikatini so‘raydi;

- sertifikatlashtirish markazi jo‘natuvchining sertifikatini imzolaydi;
- sertifikatlashtirish markazi imzolangan oluvchining sertifikatini jo‘natadi;
- oluvchi sertifikatlashtirish markazining imzosini tekshiradi va jo‘natuvchining umumiy kalitini ajratib oladi.

Bu sxemani ishlatish uchun foydalanuvchilar orasida CA umumiy kalitni ishonchli tarqatish tizimi zarur bo‘ladi. Buning uchun ochiq kalitlar infratuzilmasi *PKI* (Public Key Infrastructure) yaratilgan. PKIdan foydalanish avtomatlashtirish yo‘li xavfsizlikni boshqarishni soddalashtirishga, raqamli sertifikatlarni oshkor etilishining sezilarli murakkabligi tufayli xavfsizlik rejimini kuchaytirishga, boshqarishni takomillashtirish va himoyalash bilan integratsiyalashga, biznes-resurslarga himoyalangan ulanishni nazorat qilishni kuchaytirishga imkon beradi.

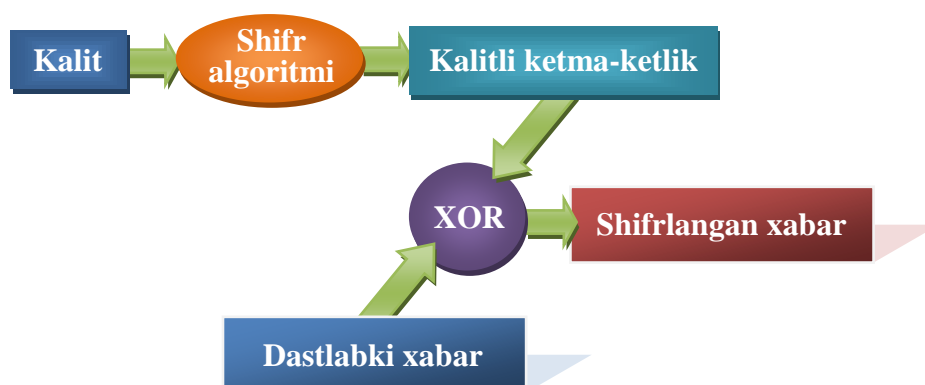


4.13- rasm. Raqamli sertifikatli kalitni uzatish

Oqimli shifrlash. Oqimli shifrlashda oldindan berilgan kalit va dastlabki xabar asosida shifrlash algoritmi generatsiyalaydigan kalitli ketma-ketlikda 2 modul bo‘yicha (“inkor qiluvchi YOKI”, XOR

funksiyasi) bitlab qo‘shish bajariladi. Kalitli ketma-ketlik shifrlanishi kerak bo‘lgan dastlabki xabar uzunligiga mos bo‘lgan uzunlikka ega bo‘ladi (4.14-rasm).

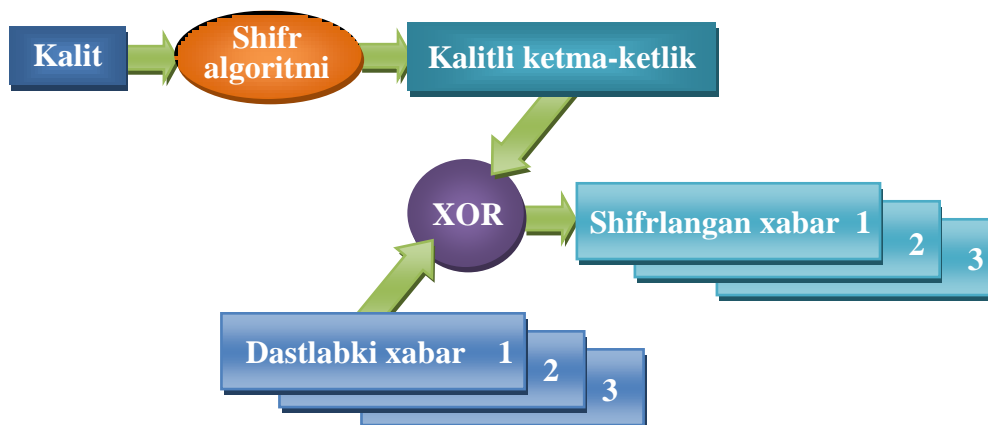
Blokli shifrlash. Blokli shifrlash jarayonida o‘zgarmaydigan oldindan aniqlangan uzunlikdagi bloklar bilan ishlaydi. Dastlabki xabar bloklarga bo‘laklanadi va XOR funksiya kalitli ketma-ketlik va har bir blok ustida hisoblanadi. Blokning o‘lchami qayd etilgan, dastlabki xabarning oxirgi bo‘lagi esa normal blok uzunligigacha bo‘sh simvollar bilash to‘ldiriladi (4.15-rasm). Masalan, 16-baytli bloklar bilan blokli shifrlashda 38 baytli uzunlikdagi dastlabki xabar 16 baytdan ikkita bloklarga va 6 bayt uzunlikdagi bitta blokka bo‘laklanadi, keyin u normal blok uzunligigacha bo‘sh simvollar 10 ta baytlari bilan to‘ldiriladi.



4.14- rasm. Oqimli shifrlash

Ko‘rsatilgan kamchiliklarni tuzatish uchun quyidagilar ishlatiladi:

- initsializatsiya vektorlari (Initialization Vectors-IVs);
- teskari aloqa (feedback modes).

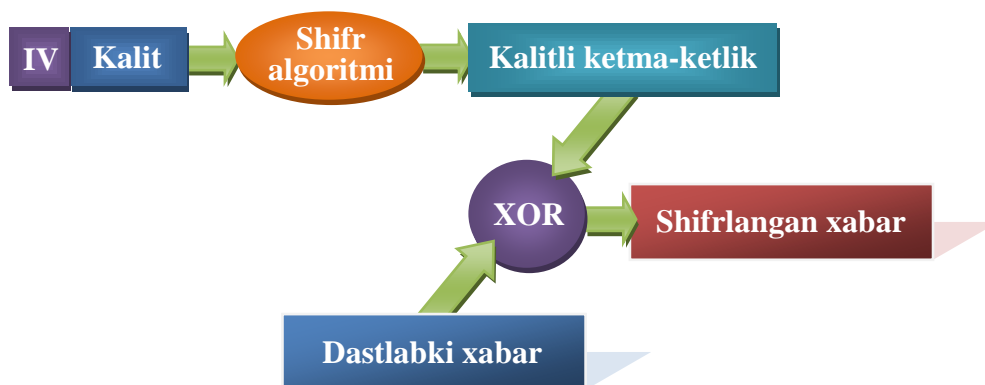


4.15- rasm. Blokli shifrlash

Shifrlash jarayoni boshlanguncha 40 yoki 104-bitli maxfiy kalit simli tarmoqqa kiradigan barcha stansiyalar orasida taqsimlanadi. Maxfiy kalitga initsializatsiya vektori qo‘shimcha qilinadi.

Initsializatsiya vektori (Initialization Vectors-IVs). Initsializatsiya vektori kalitli ketma-ketlikni modifikatsiyalash (o‘zgartirish) uchun ishlatiladi. Initsializatsiya vektori ishlatilganda kalitli ketma-ketlik shifrlash algoritmi orqali generatsiyalanadi, uning kirishiga IV bilan qo‘shilgan maxfiy kalit beriladi. Initsializatsiya vektori o‘zgarganda kalitli ketma-ketlik ham o‘zgaradi. 4.16-rasmda dastlabki xabar shifrlash algoritmi orqali uning kirishiga maxfiy kalit va initsializatsiya vektori kombinatsiyasi berilganidan keyin generatsiyalanadigan yangi kalitli ketma-ketlikdan foydalanib shifrlanadi, bu chiqishda shifrlangan xabarni hosil qiladi.

IEEE 802.11 standarti radiokanalga uzatiladigan har bir yangi freym uchun initsializatsiya vektorining yangi qiymatini ishlatilishini tavsiya qiladi.



4.16- rasm. WEP shifrlash algoritmi

4.6. Simsiz tarmoqlardagi autentifikatsiyalash usullari

Simsiz WLAN tarmoqlarining (Wi-Fi) xavfsizligi doimo alohida havotirlikni keltirib chiqarmoqda, chunki tarmoqning chegaralari doimo kengayib bormoqda. Simsiz aloqa signallari qattiq to‘siqlar – shiplar, pollar, devorlar orqali, uy yoki ofis chegaralaridan tashqariga uzatilishi mumkin. WLAN tarmoqlarini qat’iy xavfsizlik choralarisiz o‘rnatilishi hamma joylardan, hatto ko‘chada Ethernet-portlarni o‘rnatish bilan teng bo‘ladi [12].

Simsiz tarmoqqa suqilib kirishga urinadigan g‘arazgo‘ylar tomonidan tahdidlarning oldini olish va ma’lumotlarni himoyalash uchun ikkita xavfsizlikni ta’minlash funksiyalari ishlatilgan.

SSID identifikatorini yashirish. Ulanish nuqtalari va ayrim simsiz marshrutizatorlar SSID identifikatori signali kadrini uzishga imkon beradi. Simsiz mijozlar tarmoqqa ulanish uchun SSID nomini qo‘lda aniqlashi kerak.

MAC-manzillarni filtrlash. Ma‘mur mijozlarga ularning fizik qurilmalari MAS-manzillariga bog‘liq ravishda simsiz ulanishga ruxsat etishi yoki ta‘qiqlashi mumkin. Bu ikkita funksiyalar ko‘plab foydalanuvchilarni elakdan o‘tkazsada, aslida na SSID identifikatorini yashirish, na MAC-manzillarni filtrlash bilimdon buzuvchiga halal bermaydi. Aynan SSID identifikatorini hatto ulanish nuqtasi keng uzatishli tarqatishni bajarmasa ham aniqlash mumkin, MAS-manzillarni esa soxtalashtirish mumkin.

Simsiz tarmoqni himoyalashning optimal usuli autentifikatsiyalash va shifrlash tizimlaridan foydalanish hisoblanadi (4.17-rasm).

Ma‘lumotlarni himoyalashda “autentifikatsiya” atamasi inson sub’ekti terminal yoki tarmoqni o‘zida mujassamlashtirishiga bog‘liq bo‘lmagan ular taqdim etadigan axborot bo‘yicha ulanishga ma’sul ob’ekt haqiqiylikini tekshirish protsedurasi uchun ishlatiladi.

Simsiz tarmoqlarda autentifikatsiyalash standartlari bir nechta tashkil etadi. Ulardan har biri o‘z kamchiliklariga va afzalliklariga ega. Har birida o‘zining murakkab ishlash prinsipi mavjud. Absolyut himoyalangan standartlar bo‘lmaydi va shuning uchun har bir autentifikatsiyalash mexanizmining zaifliklari masalalariga e’tibor qaratish kerak.

Dastlabki 802.11 standartida ikkita autentifikatsiyalash turlari berilgan:

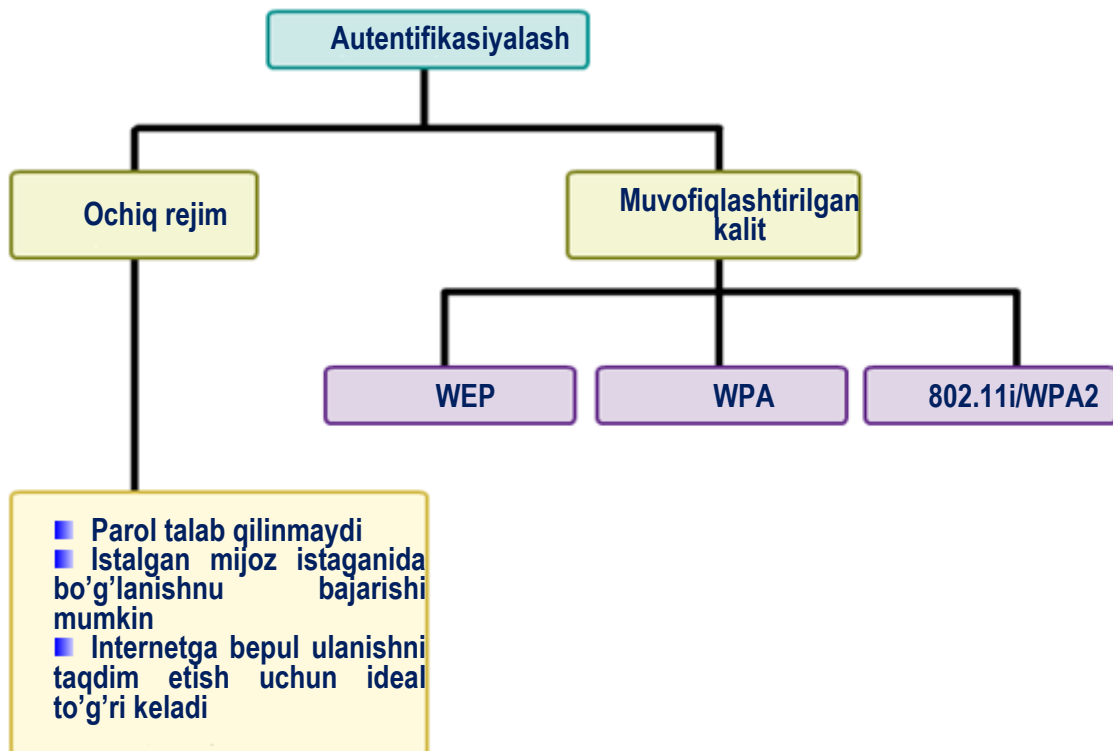
Ochiq tizimni autentifikatsiyalash. Barcha simsiz mijozlar ulanishni oson bajarishi mumkin va bunday tizim faqat xavfsizlik alohida ahamiyatga ega bo‘lmagan joylarda (masalan, Internetga bepul ulanish taqdim etiladigan joylar – kafe, mehmonxonalar va boshqalarda) ishlatilishi mumkin.

Muvofiqlashtirilgan kalitni autentifikatsiyalash. Simsiz mijoz va ulanish nuqtasi orasida uzatiladigan ma‘lumotlarni autentifikatsiyalash va shifrlash uchun WEP, WPA yoki WPA2 kabi mexanizmlar taqdim etiladi. Lekin ulanish uchun parolni oldindan tomonlar orasida muvofiqlashtirish talab qilinadi.



4.17- rasm. Autentifikatsiyalash

4.18-rasmda har xil autentifikatsiyalash turlari haqida qisqacha ma'lumotlar keltirilgan.



4.18- rasm. Autentifikatsiyalash usullari

Simsiz tarmoqlarda asosiy autentifikatsiyalash standartlari IEEE802.11, WPA, WPA2, va 802.1x standartlari hisoblanadi.

An'anaviy xavfsizlikli IEEE802.11 standarti. An'anaviy xavfsizlikli IEEE802.11 standarti (Tradition Security Network-TSN) ikki *ochiq autentifikatsiyalashni (Open Authentication)* va *umumiy kalitli autentifikatsiyalashni (Shared Key Authentication)* ko'zda tutadi. Simsiz tarmoqlarda autentifikatsiyalashda 802.11 standarti doirasiga kiradigan ikki boshqa mexanizmlar, aynan *simsiz lokal tarmoq identifikatorining tayinlanishi (Service SetIdentifier-SSID)* va *abonentning uning MAS-manzili bo'yicha autentifikatsiyalash (MAC Address Authentication)* ham keng ishlatiladi.

Simsiz lokal tarmoq identifikatori (SSID) tarmoqlarni bir-birlaridan mantiqiy ajratishga imkon beradigan simsiz tarmoq atributi hisoblanadi. Umumiy holda simsiz tarmoq abonentni talab qilinadigan simsiz lokal tarmoqqa ulana olishi uchun o'zida mos SSID ni berishi kerak. SSID ma'lumotlarning konfidensialligini ta'minlamaydi va shu bilan birga simsiz lokal tarmoq radio ulanish nuqtasiga nisbatan abonentni autentifikatsiyalamaydi. Bir necha segmentlarda nuqtaga ulanadigan abonentlarni ajratishga imkon beradigan ulanish nuqtalari mavjud. Bunga shu bilan erishiladiki, ulanish nuqtasi bir emas, bir nechta SSIDlarga ega bo'lishi mumkin.

4.7. WPA, WPA2 va 802.1x shifrlash protokollari

Simsiz texnologiyalar uchun axborot xavfsizligini ta'minlash masalalari juda muhim hisoblansada, birinchi Wi-Fi standartlari zaif himoya tizimlariga ega bo'lgan yoki umuman ega bo'lmagan. Bunga sabab dastlab mazkur texnologiyalarning bunchalik ommaviylashishi va muvofiq ravishda xavfsizlik muammolarining bunday keskin bo'lishi kutilmaganligidir. Birinchi WEP (ingl. *Wired Equivalent Privacy* – simli tarmoqlardagi xavfsizlik darajasiga teng) shifrlash protokoli 1999 yilda joriy etilgan va “11b” standartida ishlatilgan edi. WEP protokoli simmetrik (uzatkich va qabul qilgichda bir xil) statik (o'zgaraydigan) 64 bit uzunlikdagi kalitlarni (aslida 40 bitlik kalitga, 24 bitlik initsializatsiya vektori qo'shiladi) ishlatadi va bu kalitlarni birma-bir tanlash yo'li bilan bir necha sekundlarda aniqlab olish mumkin. Bunday zaiflik WEP yordamidagi shifrlashni samarasiz qildi. WEP protokolida dinamik (o'zgaruvchan) shifrlash kalitlaridan foydalanish ham muammoni faqat qismangina hal etdi. Shuning uchun

WEP zaifligini to'liq tuzatish uchun kalitni va shifrlash algoritmini kuchaytirish talab etildi [1].

Bu maqsadda IEEE ning standartlar bo'yicha qo'mitasi Wi-Fi texnologiyasi uchun xavfsizlik tizimini yangitdan ishlab chiqishga qaror qildi. Natijada 2004 yilning iyunida Wi-Fi Alliance guruhi tomonidan ishlab chiqilgan, shuningdek WPA-2 protokoli sifatida ma'lum bo'lgan yangi IEEE 802.11i standarti paydo bo'ldi. IEEE 802.11i standarti simsiz tarmoqlarning xavfsizligi uchun uzoq muddatli va kengaytirilgan yechim hisoblanadi va WEP kamchiliklaridan holi bo'lgan tamomila yangi xavfsizlik tizimi deb ataladi. IEEE 802.11i standarti simsiz uskunalar xavfsizligi bo'yicha qo'shimcha imkoniyatlar ta'minlashni ko'zda tutgan "kuchaytirilgan tarmoq xavfsizligi" - RSN (ingl-n *Robust Security Network*) konsepsiyasini ishlatadi. Bu esa apparat qismida va dasturiy ta'minotda o'zgarishlarni talab qiladi va shu bilan RSN ga to'liq moslashadigan tarmoqlarni WEP protokolini ishlatadigan mavjud jihozlar bilan moslashmaydigan qilib qo'yadi. Shunday qilib, bir qancha vaqt ham RSN, ham WEP jihozlari qo'llab- quvvatlanadi, keyinchalik esa WEPli uskunalar ishlatishdan umuman chiqarib tashlanadi.

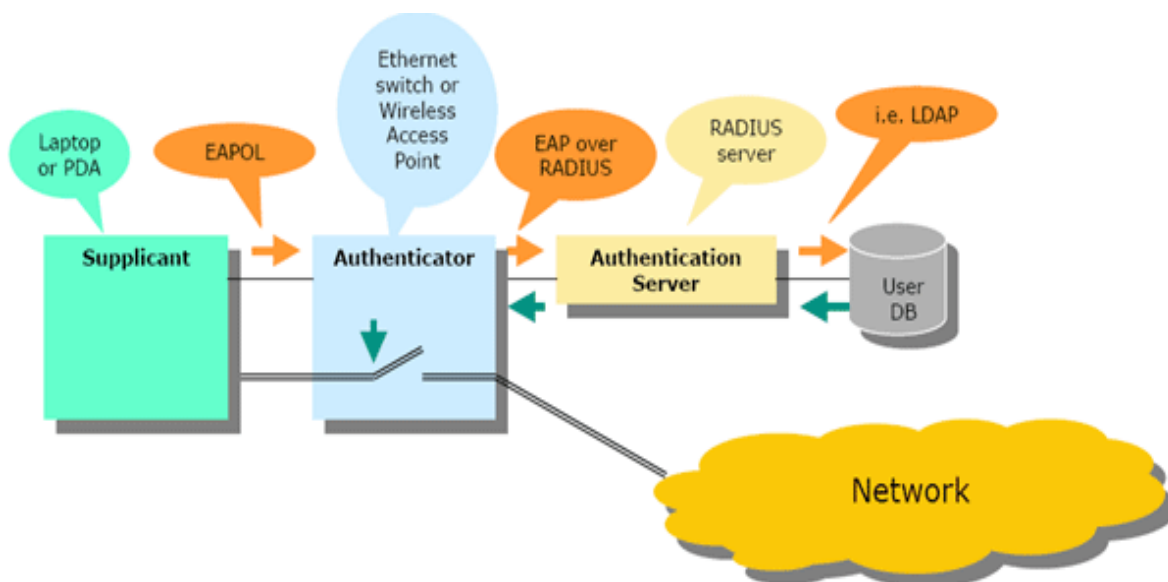
WPA2 (Wireless Protected Access ver. 2.0) – bu Wi-Fi simsiz tarmoqlarida ma'lumotlarni himoyalanihini ta'minlaydigan algoritmlar va protokollar to'plamining ikkinchi versiyasi hisoblanadi. Ko'zda tutiladiki, WPA2 oldingi texnologiyalarga qaraganda Wi-Fi simsiz tarmoqlarida himoyalanganlikni sezilarli oshirishi kerak. Yangi standart, xususan quvvatliroq AES (Advanced Encryption Standard) shifrlash algoritmini va 802.1X autentifikatsiyalashni majburiy ishlatilishini ko'zda tutadi.

Bugungi kunga kelib korporativ tarmoqda ishonchli xavfsizlik mexanizmini ta'minlash uchun WPA2 qo'llanadigan qurilmalar va dasturiy ta'minot ishlatilishi zarur (va shart). Oldingi protokollar avlodlari bo'lgan WEP va WPA yetarli bo'lmagan kuchli himoya va shifrlash algoritmlarili elementlarga ega. Buning ustiga WEP asosidagi himoyalashli tarmoqlarni buzib kirish uchun endi dasturlar va uslublar ishlab chiqilgan, ularni Internetdan oson olish va hatto tayyorlanmagan buzuvchilar tomonidan muvaffaqiyatli ishlatilishi mumkin.

WPA texnologiyasi quyidagi bir necha komponentlardan tashkil topgan:

- 802.1x protokoli — autentifikatsiyalash, mualliflashtirish va ro‘yxatga olish (AMRO) uchun universal protokol;
- EAP protokol — kengaytiriladigan autentifikatsiyalash protokoli (Extensible Authentication Protocol);
- TKIP protokoli — kalitlarning vaqtinchalik yaxlitlik protokoli, boshqa tarjima varianti vaqt bo‘yicha kalitlar yaxlitligi protokoli (Temporal Key Integrity Protocol)
- MIC — paketlarning yaxlitligini kriptografik tekshirish (Message Integrity Code)
- RADIUS protokoli.

802.1x protokoli bir necha funksiyalarni bajarishi mumkin. Bu holda bizni foydalanuvchini autentifikatsiyalash va kalitlarni taqsimlanishi funksiyalari qiziqtiradi. Ta’kidlash zarurki, autentifikatsiyalash “port darajasida”, – ya’ni foydalanuvchi faqat uning autentifikatsiyalanishi (hisobga olish ma’lumotlari) jarayoniga tegishli bo‘lgan paketlarni uzatishi/qabullashiga ruxsat etilganida bo‘lib o‘tadi. Va faqat muvaffaqiyatli autentifikatsiyalashdan keyin qurilmaning (ulanish nuqtasi yoki kommutatorning) porti ochiq bo‘ladi va foydalanuvchi tarmoq resurslariga ulanishni oladi (4.19-rasm).



4.19- rasm. 802.1x: ishlash prinsipi

Autentifikatsiyalash funksiyasi EAP protokoliga yuklanadi, u o‘z-o‘zidan faqat autentifikatsiyalash usullari uchun karkas hisoblanadi. Protokolning o‘ziga xos xususiyati shundan iboratki, uni autentifikatorida (ulanishi nuqtasida) ishlatish oson, chunki unga turli

autentifikatsiyalash usullarining hech qanday o'ziga xos xususiyatlarini bilish talab qilinmaydi. Autentifikator mijoz va autentifikatsiyalash serveri orasidagi bo'g'in bo'lib xizmat qiladi. Quyidagi autentifikatsiyalash usullari mavjud:

- EAP-SIM, EAP-AKA — GSM mobil aloqa tizimlarida ishlatiladi;

- EAP-MD5 — CHAPga o'xshash eng oddiy usul (barqaror emas);

- EAP-MSCHAP V2 — MS-tarmoqlarda login/parol asosida autentifikatsiyalash usuli;

- EAP-TLS — raqamli sertifikatlar asosida autentifikatsiyalash;

- EAP-SecureID — bir martalik kalitlar asosidagi autentifikatsiyalash usuli.

Autentifikatsiyalash usuli quyidagi uchta komponentlardan tashkil topgan:

- Supplicant — tarmoqqa ulanishga urinadigan mijoz mashinasida ishga tushirilgan dastur;

- Authenticator — ulanish tuguni, autentifikator (802.1x protokoli qo'llanadigan simsiz ulanish nuqtasi yoki simli kommutator);

- Authentication Server — autentifikatsiyalash serveri (odatda bu RADIUS-serveri).

WPA2 protokollari ikkita personal (Personal) va korporativ (Enterprise) rejimlarda ishlaydi. **WPA2-Personal** rejimida ochiq matnda chiqarilgan parolli jumladan 256-razryadli PSK kalit (PreShared Key) generatsiyalanadi. PSK kalit SSID (Service Set Identifier) identifikatori bilan simsiz qurilmalarning o'zaro ta'sirlashish uchun PTK (Pairwise Transient Key) vaqtinchalik seanslar kalitlarini generatsiyalash uchun ishlatiladi. WEP statik protokolidagi kabi WPA2-Personal protokoliga tarmoqning simsiz qurilmalarida kalitlarni tarqatish va saqlash zaruratiga bog'liq ma'lum muammolar o'ziga xos, bu uni o'nlab qurilmalardan iborat uncha katta bo'lmagan tarmoqlar qo'llash uchun to'g'ri keladigan qiladi, shu bilan bir vaqtda korporativ tarmoqlar uchun WPA2-Enterprise optimal bo'ladi.

WPA2-Enterprise rejimda statik kalitlarni taqsimlanishi va ularni boshqarishga tegishli muammolar hal etiladi, uning ko'plab autentifikatsiyalash korporativ servislari bilan integratsiyalanishi esa ro'yxatga olish yozuvlari asosida ulanishni nazorat qilishga imkon

beradi. Bu rejimda ishlash uchun foydalanuvchining nomi va paroli, xavfsizlik sertifikatini yoki bir martalik parol kabi registratsion ma'lumotlar talab qilinadi, autentifikatsiyalash esa ishchi stansiya va autentifikatsiyalash markazi serveri orasida amalga oshiriladi. Ulanish nuqtasi yoki simsiz kontroller bog'lanishlar monitoringini o'tkazadi va autentifikatsion so'rovlarni mos autentifikatsiyalash serveriga (bu RADIUS serveri, masalan Cisco ACS) yo'naltiradi. WPA2-Enterprise rejimi uchun asos bo'lib 802.1X standart xizmat qiladi, u foydalanuvchilarni autentifikatsiyalashi va ham simli kommutatorlar uchun, ham simsiz ulanish nuqtalari uchun yaroqli bo'lgan qurilmalarni qo'llaydi.

WPA protokolidan farqli ravishda barqarorroq AES shifrlash algoritmi ishlatiladi. WPAga o'xshash WPA2 ham ikkita WPA2-PSK va WPA2-802.1x turlarga bo'linadi.

Ma'lumotlarni yaxlitligi va konfidentsialligini ta'minlashning yangi ishonchliroq mexanizmlarini ko'zda tutadi: Counter Cipher-Block Chaining Mode (CCM) rejimidagi Advanced Encryption Standard (AES) shifrlash algoritmiga asoslangan CCMP (Counter-Mode-CBC-MAC Protocol) protokoli. CCM ikkita mexanizmlarni birlashtiradi: konfidentsiallikni ta'minlash uchun Counter (CTR) va autentifikatsiyalash uchun Cipher Block Chaining Message Authentication Code (CBC-MAC).

WRAP (Wireless Robust Authentication Protocol) protokoli Offset Codebook (OCB) rejimdagi AES shifrlash algoritmiga asoslangan.

TKIP protokoli oldin chiqarilgan qurilmalar bilan teskari moslashuvchanlikni ta'minlaydi. O'zaro autentifikatsiyalash va kalitlarni yetkazilishi IEEE 802.1x/EAP protokoli asosida amalga oshiriladi. Xavfsiz Independent Basic Service Set (IBSS) Ad-Hoc tarmoqlardagi xavfsizlikni oshiradi. Roving ta'minlanadi.

Simsiz tarmoqlar xavfsizligini ta'minlashdagi CCMP mexanizmiga hissanii IEEE 802.11i standarti ham qo'shadi. IEEE 802.11i standarti ishonchli himoyalangan tarmoq (Robust Security Network, RSN) va ishonchli himoyalangan tarmoq bog'lanishi (Robust Security Network Association, RSNA) tushunchasini kiritadi va bundan keyin barcha algoritmlarni quyidagilarga bo'ladi:

- RSNA-algoritmlar (RSNAni yaratish va ishlatish);
- Pre-RSNA-algoritmlari.

Pre-RSNA-algoritmlarga quyidagilar kiradi:

- WEP;
- Mavjud IEEE 802.11 autentifikatsiyalash (standartning 1999 yilgi tahririda aniqlangan autentifikatsiyalash nazarda tutiladi).

Ya'ni bu turdagi algoritmlarga WEP-shifrlashli yoki WEP-shifrlashsiz Open System va Shared Key autentifikatsiyalash kiradi.

RSNA-algoritmlarga quyidagilar kiradi:

- TKIP;
- CCMP;
- RSNA o'rnatilishi va terminallashtirilish protsedurasi (shu jumladan IEEE 802.1x autentifikatsiyalashdan foydalanish);
- Kalitlarni almashlash protsedurasi.

Bunda CCMP algoritmi majburiy, TKIP esa opsional hisoblanadi va eski qurilmalar bilan moslashuvchanlikni ta'minlash uchun mo'ljallangan.

Standart orqali ikkita funksional modellar ko'zda tutilgan:

- IEEE 802.1x bo'yicha autentifikatsiyalash bilan, ya'ni EAP protokoli qo'llaniladigan;

– Autentifikator va mijozda yozilgan oldindan aniqlangan kalit yordamida (bunday rejim Preshared Key, PSK deyiladi). Bunday holda PSK kalit PMK kalitining rolini bajaradi va ularning keyingi autentifikatsiya va generatsiyalash protsedurasi hech qanday farqlanmaydi.

TKIP protsedurasini ishlatadigan shifrlash algoritmlarini endi WPA, CCMP protsedurasini ishlatadigan shifrlash algoritmlarini esa WPA2 deyish qabul qilingan, u holda aytish mumkinki, RSNani qanoatlantiradigan shifrlash usullari WPA-EAP (WPA-Enterprise), WPA-PSK (WPA-Preshared Key, WPA-Personal), WPA2-EAP (WPA2-Enterprise), WPA2-PSK (WPA2-Preshared Key, WPA2-Personal) hisoblanadi.

TKIP va CCMP algoritmlari uchun bog'lanishni o'rnatilishi va ma'lumotlarni almashlash protsedurasi bir xil. CCMP (Counter mode (CTR) with CBC-MAC (Cipher-Block Chaining (CBC) with Message Authentication Code (MAC) Protocol).

TKIP kabi CCMPning (Counter mode (CTR) with CBC-MAC (Cipher-Block Chaining (CBC) with Message Authentication Code (MAC) Protocol) o'zi konfidensialik, autentifikatsiyalash va qayta tiklashdan himoyalashni ta'minlashi kerak. Bu algoritm FIPS PUB 197 spetsifikatsiyada aniqlangan AES shifrlash CCM-algoritmiga asoslangan. CCMPda ishlatiladigan barcha AES-jarayonlar 128-bitli,

kalitli va 128-bitli o'ldamli blokli AESni ishlatadi.

Standartdagi oxirgi yangi joriy etish ulanish nuqtalari orasidagi PMK kalitni xeshlash protsedurasi va oldindan autentifikatsiyalashdan foydalanish bilan tezkor rouming texnologiyasini qo'llash hisoblanadi.

PMK kalitni xeshlash protsedurasi shundan iboratki, agar mijoz bir marta qandaydir ulanish nuqtasiga bog'lanishda to'liq autentifikatsiyalashdan o'tgan bo'lsa, u holda mijoz undan olgan PMK kalitni saqlaydi va bu ulanish nuqtasiga keyingi bog'lanishda haqiqiylikni tasdiqlash haqidagi so'rovga javob sifatida oldingi olingan PMK kalitni jo'natadi.

Oldindan autentifikatsiyalash protsedurasi shundan iboratki, mijoz ulanish nuqtasiga bog'langan va autentifikatsiyalashdan o'tganidan keyin, boshqa ulanish nuqtalariga (agar ularni "ko'rsa") parallel (oldindan) o'sha SSID bilan autentifikatsiyalashdan o'tishi, ya'ni ulardan oldindan PMK kalitni olishi mumkin. Va agar keyinchalik u bog'langan ulanish nuqtasi ishdan chiqsa yoki signal bunday tarmoq nomi bilan qandaydir ulanish nuqtasidagidan kuchsizroq bo'lsa, u holda mijoz xeshlangan PMK kalitli tezkor sxema bo'yicha qayta bog'lanishni amalga oshiradi.

Standartni ishlab chiquvchilar xavfsizlik mexanizmlarini takomillashtirguncha barrikadaning boshqa tomonidagilar ham jim turishmadi. Bu davrda WEPni etarlicha tez buzishga imkon beradigan yangi usullar paydo bo'ldi, binobarin, buzuvchilarning o'zidan ish sarflari endi minimal talab qilina boshlandi. Agar oldin barcha buzish vositalari faqat Unix-platformalarda ishlagan bo'lsa, endi ularda ko'pchiligi Windowsda, ayrimlari esa hatto MASda ishlashmoqda. Keyinchalik oddiy parolli jumalardan foydalanish bilan WPA-PSK va LEAPni birmuncha vaqtda buzishga imkon beradigan real ishlaydigan vositalar yaratildi. Simsiz tarmoqlar ham "Xizmat ko'rsatishni rad etish" turdagi hujumlardan himoyalangan bo'lib qolmoqda.

Uchta asosiy hujumlar guruhi mavjud:

Fizik darajada. Ulanish nuqtasining ishchi chastotasidagi quvvatli nurlanish manбайдan foydalanish (signalni bo'g'ish);

Xizmat freymlari qo'llaniladigan hujumlar. Xizmat freymlari uzatilganida ulanish nuqtasi va mijoz o'zaro autentifikatsiyalashni bajarmaydi, shuning uchun buzuvchi MAC-manzilni almashtirib qo'yishi va qonuniy mijoz nomidan freymlarni jo'natishi mumkin

Tarmoqning turiga bog‘liq ravishda turli xavfsizlikni ta‘minlash usullarining qo‘llanilishi

Tarmoq turi	Korporativ tarmoq	Hot-Spot tarmog‘i	Ko‘prikli bog‘lanish
WPA2ning ishlatilishi	+	–	–
WPA	+	–	–
802.1x	+	–	–
WEP	+	+	+
VPN	–	–	+
Ulanish nuqtasini brandmauerdan chiqarish	+	+	+
IDSdan foydalanish	+	+	+
Chegaraviy resursda autentifikatsiyalash	+	+	–
MAS-manzillar bo‘yicha filtrlash	+	–	+
SSID qayta tarqatishni uzilishi	+	–	+

IEEE 802.1x so‘rovlaridan foydalanish orqali hujumlar.
802.11i standarti autentifikatsiyalashga so‘rovlarni inkor etish mexanizmlariga ega emas, shuning uchun shunchalik ko‘p sonli bunday so‘rovlarni generatsiyalash mumkinki, ulanish nuqtasi ular bilash ishlay olmay qoladi.

Simsiz tarmoqning turiga bog‘liq ravishda himoyalash mumkin. Agar tarmoq unchalik katta bo‘lmagan nuqta–nuqta turidagi tarmoq bo‘lsa, WPA2dan foydalanish kerak. Agar infratuzilmali rejimda ishlaydigan korporativ tarmoq bo‘lsa, u holda barcha bo‘lishi mumkin himoyalash vositalari – SSIDni yashirish, MAS-manzillar asosida ulanish ro‘yxatlari va albatta WPA2-EAPni qo‘llash tavsiya etiladi. Korporativ tarmoq begona ulanish nuqtalaridan qanday himoyalanadi? Ulanish nuqtasi kompaniyaning lokal tarmog‘iga ulanmaganidagi variant qo‘rqinchli emas, chunki bunday hujumni amalga oshirilishi uchun dastlab WPA2ni buzish kerak bo‘ladi. Ulanishli variantdan turli

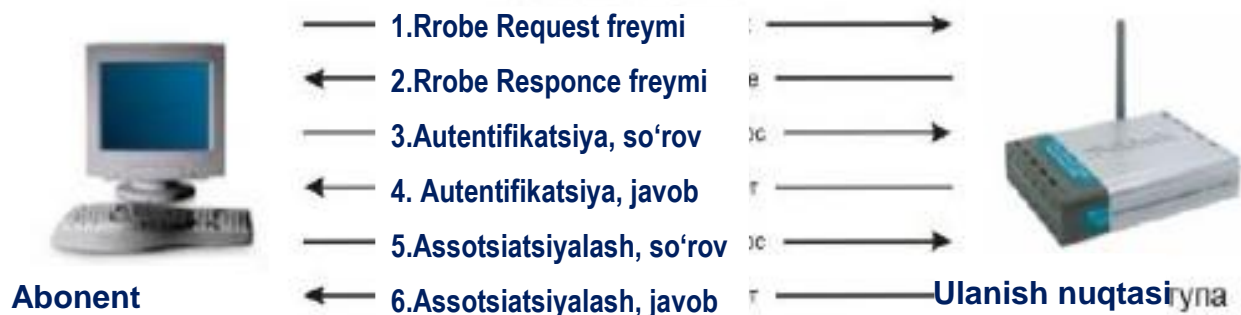
usullar orqali himoyalaniş mumkin:

- Kommutatordagi ishlatilmaydigan portlarni o‘chirish;
- Lokal tarmoqda IEEE 802.1x autentifikatsiyalashni ishlatish;
- Port Security funksiyasini qo‘llash (kommutatorda qaysi portlarga qanday MAS-manzillar ulanişhi mumkinligini ko‘rsatish);
- Simsiz ulaniş nuqtasini tarmoqlararo ekrandan tashqariga chiqarish yoki alohida virtual tarmoqqa chiqarish va bu tarmoq va boshqalar orasida trafikni nazorat qilish va cheklash qoidalarini sozlash;
- Suqulib kirishlarni aniqlash tizimlari (masalan simsiz tarmoqlar uchun Snort tizimi), tarmoqdagi “begona” qurilmalarni aniqlashga imkon beradigan maxsus simsiz kommutatorlar yoki ulaniş nuqtalaridan foydalanish.

4.8. IEEE802.11 standartida abonentni autentifikatsiyalash prinsipi

IEEE802.11 standartida abonentni autentifikatsiyalash aniq bir abonentni tarmoq resurslarining foydalanuvchisi emas, radioulaniş abonent qurilmasini autentifikatsiyalashga mo‘ljallangan. IEEE802.11 simsiz lokal tarmoq abonentini autentifikatsiyalash jarayoni quyidagi bosqichlardan tashkil topgan (4.20-rasm) [13]:

1. Abonent (Client) Probe Request freymni barcha radiokanallarga yuboradi.
2. Har bir radioulaniş nuqtasi (Access Point-AP) abonent joylashgan radio ko‘rinish zonasida Probe Responce javob freymini yuboradi.
3. Abonent o‘zi uchun afzal bo‘lgan radioulaniş nuqtasini tanlaydi va unga xizmat ko‘rsatadigan radiokanalga autentifikatsiyalashga (Authentication Request) so‘rovni yuboradi.
4. Radioulaniş nuqtasi autentifikatsiyalashning tasdiqlanishini (Authentication Reply) yuboradi.
5. Muvvafaqiyatli autentifikatsiya holatida abonent radioulaniş nuqtasiga assotsiatsiya freymini (Association Request) yuboradi.
6. Radioulaniş nuqtasi javobga assotsiatsiyani tasdiqlash freymini (Association Responce) yuboradi.
7. Abonent endi radioulaniş nuqtasi va simli tarmoq bilan foydalanish trafiklarini almashtirishni amalga oshirishi mumkin bo‘ladi.



4.20- rasm. 802 standart bo'yicha autentifikatsiyalash

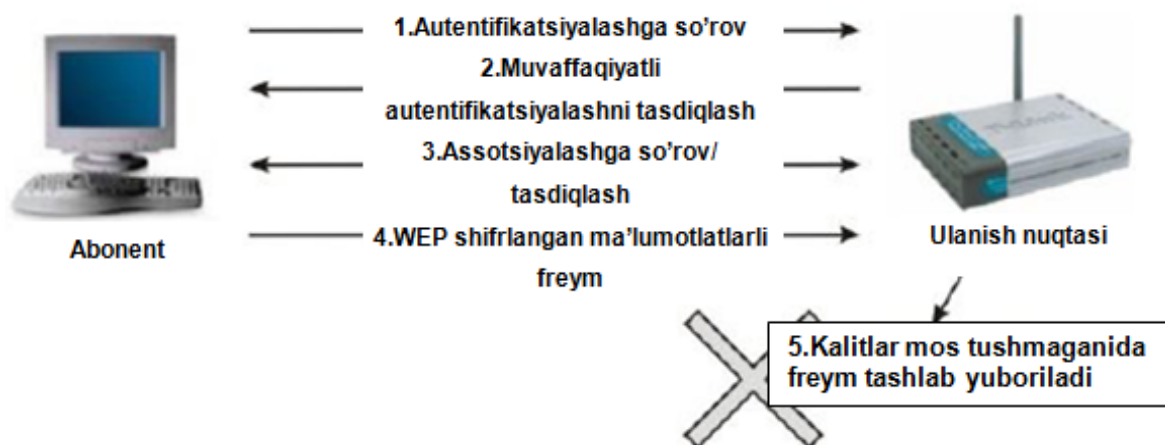
Aktivlashtirishda simsiz abonent o'z radio ko'rinish zonasida Probe Request boshqarish freymlari yordamida radioulanish nuqtalarini qidira boshlaydi. Probe Request freymlari mijozga zarur bo'lgan SSID identifikatorili barcha radioulanish nuqtalarini topish uchun abonent radiointerfeysini ishlata oladigan va radio almashtirish tezliklari bilan ishlay oladigan radiokanallardan har biriga yuboriladi. Abonent radio ko'rinish zonasida bo'lgan Probe Request freymida so'ralgan parametrlarni qoniqtiradigan radioulanish nuqtalaridan har biri sinxronlashtiruvchi axborotlar va radioulanish nuqtasining joriy yuklanishi haqida ma'lumotlardan iborat Probe Responce freymi bilan javob beradi. Abonent qaysi radioulanish nuqtasi bilan ishlashini ular ishlay oladigan radio almashtirish tezliklari va yuklanishlarini taqqoslash yo'li bilan aniqlaydi. Avzalloq radioulanish nuqtasi aniqlanganidan keyin abonent autentifikatsiyalash fazasiga o'tadi.

Ochiq autentifikatsiyalash. Ochiq autentifikatsiyalash birlamchi tushunishda autentifikatsiyalash algoritmi hisoblanmaydi. Radioulanish nuqtasidan foydalanish ochiq autentifikatsiyalashning barcha so'rovlarini qoniqtiradi. Bunday qaraganda bu algoritmdan foydalanish ma'nosiz ko'rinadi, lekin shuni e'tiborga olish kerakki, 1997 yilda yaratilgan IEEE802.11 autentifikatsiyalash usullari simsiz lokal tarmoqqa tezkor mantiqiy bog'lanishga mo'ljallangan. Bunga qo'shimcha ravishda ko'plab IEEE802.11-moslashuvchan qurilmalari (shtrix-kodlar skanerlari va boshqalar) autentifikatsiyalashning murakkab algoritmlarini ishlatilishi uchun zarur bo'lgan yetarlicha protsessorli quvvatga ega bo'lmagan portativ axborotlar yig'ish bloklaridan iborat bo'lgan.

Ochiq autentifikatsiyalash jarayonida quyidagi ikki turdagi xabarlarni almashtirilishi amalga oshadi:

- autentifikatsiyalashni so‘rash (Authentication Request);
- autentifikatsiyalashni tasdiqlash (Authentication Responce).

Shunday qilib, ochiq autentifikatsiyalashda simsiz lokal tarmoqqa istalgan abonentning ulanishi mumkin. Agar simsiz tarmoqda shifrlash ishlatilmasa, radioulanish nuqtasining SSID identifikatorini biladigan istalgan abonent tarmoqqa ulanishi mumkin. Radioulanish nuqtalari WEP shifrlashni ishlatganda shifrlash kalitlarining o‘zi ulanishni nazorat qilish vositasi bo‘lib qoladi. Agar abonent to‘g‘ri WEP-kalitga ega bo‘lmasa, u holda hatto muvaffaqiyatli autentifikatsiyalashda ham u radioulanish nuqtalari orqali ma’lumotlarni uzata olmaydi, radioulanish nuqtasidan uzatilgan ma’lumotlarni esa rasshifrovka qilolmaydi (4.21-rasm).



4.21- rasm. Ochiq autentifikatsiyalash

Umumiy kalitli autentifikatsiyalash. Umumiy kalitli autentifikatsiyalash IEEE802.11 standartining ikkinchi autentifikatsiyalash usuli hisoblanadi. Umumiy kalitli autentifikatsiyalash abonentda WEP shifrlash statik kalitini sozlanishini talab qiladi. Autentifikatsiyalash jarayoni 3.6-rasmda keltirilgan:

1. Abonent radioulanish nuqtasiga umumiy kalitli autentifikatsiyalashdan foydalanish zarurligini ko‘rsatish bilan autentifikatsiyalashga so‘rov yuboradi.

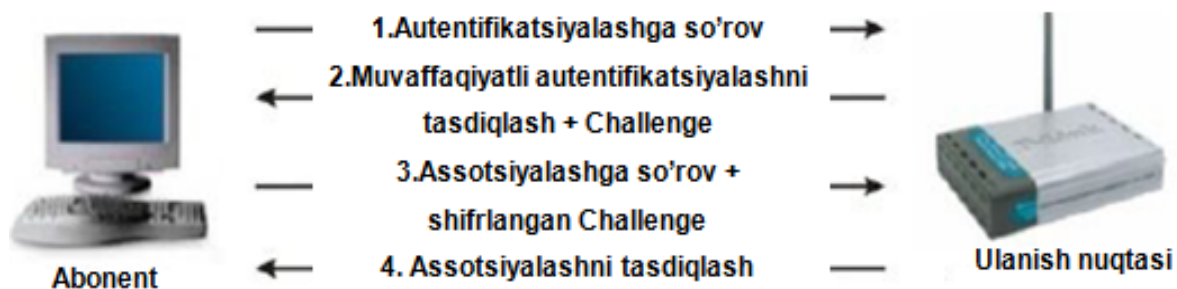
2. Radioulanish nuqtasi Challenge Textdan iborat autentifikatsiyalashni tasdiqlashni yuboradi.

3. Abonent o‘zining statik WEP-kaliti bilan Challenge Textni shifrlaydi va radioulanish nuqtasiga autentifikatsiyalashga so‘rov yuboradi.

4. Agar radioulanish nuqtasi autentifikatsiyalashga so'rovni va undagi Challenge Textni muvaffaqiyatli rasshifrovka qilish holatida bo'lsa, u autentifikatsiyalashga tasdiqlashni yuboradi, shunday qilib tarmoqqa ulanishni taqdim etadi.

MAC-manzil bo'yicha autentifikatsiyalash.

Uning MAC-manzili bo'yicha autentifikatsiyalash IEEE802.11 standartida ko'zda tutilmagan, lekin simsiz tarmoqlar uchun ko'plab qurilmalar, shu jumladan D-Link ishlab chiqaruvchilari tomonidan ishlatiladi.



4.22- rasm. Umumiy kalitli autentifikatsiyalash

MAC-manzil bo'yicha autentifikatsiyalashda abonentning MAC-manzili qonuniy abonentlar lokal saqlanadigan ruxsat etiladigan manzillar ro'yxati bilan yoki autentifikatsiyalashning tashqi serveri yordamida taqqoslash amalga oshadi (4.23- rasm).



4.23- rasm. Tashqi server yordamida autentifikatsiyalash

MAC-manzil bo'yicha autentifikatsiyalash begona abonentlarning ulanishi ehtimolligini kamaytirish uchun ochiq autentifikatsiyalashga va umumiy kalitli autentifikatsiyalashga qo'shimcha sifatida ishlatiladi.

802.11 autentifikatsiyalash mexanizmlarining zaifliklari

Simsiz LHT identifikatori muammosi. SSID identifikatori maxsus Veacon freymlarida radioulanish nuqtalaridan tez-tez uzatiladi. Tarmoqda bu freymlar faqat axborot rolini o'ynashiga, ya'ni

abonent uchun butkul ochiqligiga qaramasdan, tashqi kuzatuvchi 802.11 protokoli trafigi analizatori, masalan Sniffer Pro Wireless yordamida osonlikcha SSID identifikatorini aniqlashi mumkin. Ba'zi radioulanish nuqtalari, shu jumladan D-Link Veacon freymlari ichida SSID identifikatorini keng uzatilishini ma'muriy ta'qiqlashga imkon beradi. Lekin, bu holda ham SSID identifikatorini radioulanish nuqtalaridan yuboriladigan Rrobe Responce freymlarini qo'lga kiritish yo'li bilan osonlikcha aniqlash mumkin. SSID identifikatori xavfsizlikni ta'minlash mexanizmi sifatida ishlatilishi uchun ishlab chiqarilmagan. Bunga qo'shimcha ravishda radioulanish nuqtalaridan SSID identifikatorini keng uzatilishini uzilishi turli ishlab chiqaruvchilarning simsiz tarmoqlari qurilmalari bitta tarmoqda ishlatilganda moslashuvchanligiga ta'sir etishi mumkin.

Ochiq autentifikatsiyalashning zaifliklari. Ochiq autentifikatsiyalash radioulanish nuqtalariga abonent qonuniy yoki noqonuniyligini aniqlashga imkon bermaydi. Bu agar simsiz lokal tarmoqda WER shifrlash ishlatilmasa xavfsizlik tizimidagi bo'shliq bo'lib qoladi.

D-Link WER shifrlashsiz simsiz tarmoqlarni ishlatilishini tavsiya etmaydi. WER shifrlash talab qilinmaydigan yoki mumkin bo'lmagan hollarda (masalan, umumiy ulanishdagi simsiz lokal tarmoqlarda) yuqoriroq darajali autentifikatsiyalash usullari Internet-shlyuzlar orqali ishlatilishi mumkin.

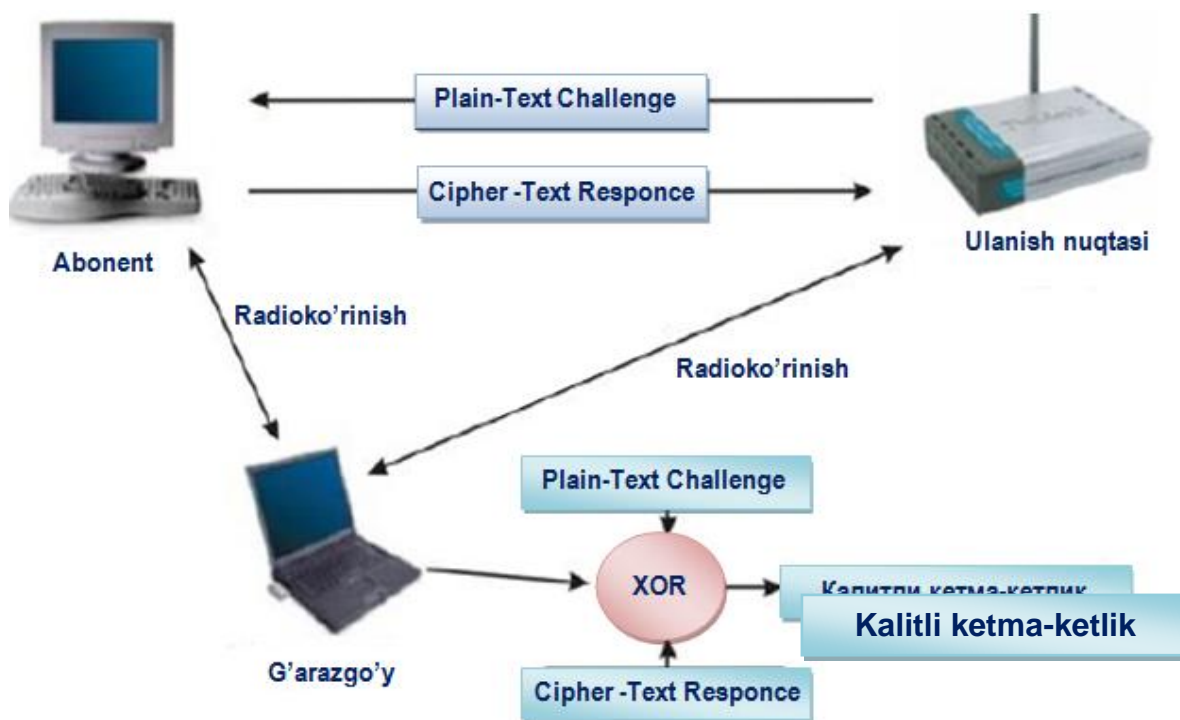
Umumiy kalitli autentifikatsiyalashning zaifliklari. Umumiy kalitli autentifikatsiyalash radioulanish nuqtasidan yuborilgan Challenge Textni shifrlash uchun abonentdan statik WER-kalitni sozlanishini talab qiladi (4.24-rasm).

Radioulanish nuqtasi abonentni uning Challengega javobini deshifrlash va uni yuborilgan asli bilan taqqoslash orqali autentifikatsiyalaydi. Challenge Textdagi freymlarni almashtirish ochiq radiokanal bo'yicha amalga oshadi, demak, kuzatuvchi tomonidan hujumlarga (Man in the middle Attack) duchor bo'ladi. Kuzatuvchi ham shifrlanmagan Challenge Textni, ham o'sha Challenge Textni, lekin endi shifrlangan ko'rinishda qabul qilishi mumkin. WER shifrlash xabar matni bilan XOR operatsiyaning bitlab bajarilishi va kalitli ketma-ketlik yo'li bilan amalga oshiriladi, buning natijasida shifrlangan xabar (Cipher-Text) olinadi. Tushunish muhimki, shifrlangan xabar bilan XOR operatsiyaning bitlab bajarilishi va kalitli ketma-ketlik natijasida biz dastlabki xabarning

matniga ega bo‘lamiz. Shunday qilib, kuzatuvchi abonentni autentifikatsiyalash jarayonida freymlarni tahlil qilish yo‘li bilan kalitli ketma-ketlik segmentini oson qo‘lga kiritishi mumkin.

MAS-manzil bo‘yicha autentifikatsiyalashning zaifliklari.

IEEE 802.11 standarti MAS-manzillarni uzatilishini va radioulanish nuqtasini ochiq ko‘rinishda bo‘lishini talab qiladi. Simsiz tarmoqda MAS-manzil bo‘yicha autentifikatsiyalashni ishlatilishi natijasida jinoyatchi autentifikatsiyalash usulini o‘z MAS-manzilini qonuniy MAS-manzil bilan almashtirishi bilan aldashi mumkin. MAS-manzilni almashtirilishi lokal ma‘murlashtiriladigan MAS-manzillardan foydalanishga ruxsat etadigan simsiz adapterlarda bo‘lishi mumkin. Jinoyatchi qonuniy abonentlarning MAS-manzillarini aniqlash uchun IEEE 802.11 protokoli trafigi analizatoridan foydalanishi mumkin.

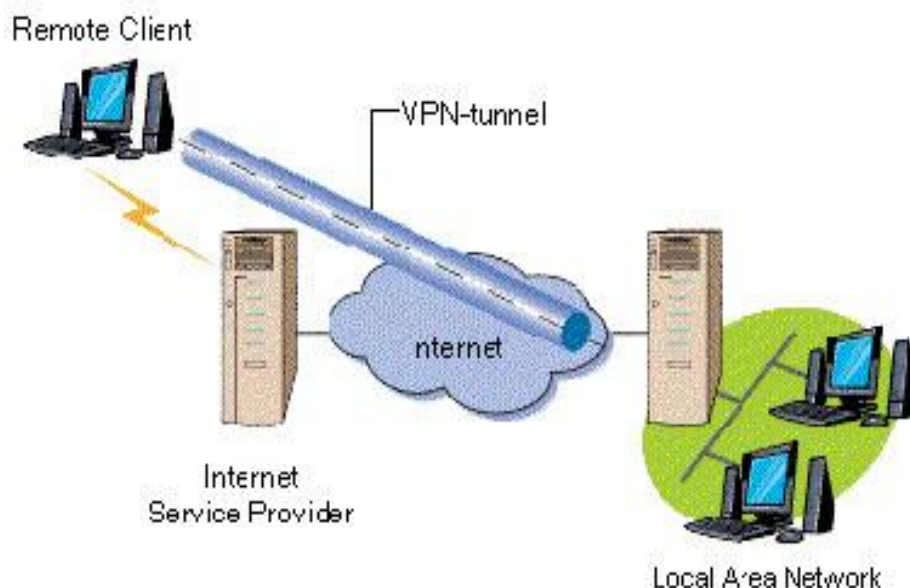


4.24- rasm. Umumiy kalitli autentifikatsiyalashning zaifligi

4.9. Virtual xususiy tarmoqlarni qurish

Virtual xususiy tarmoq (Virtual Private Network - VPN) – bu olisdagi foydalanuvchilar yoki alohida foydalanuvchilarga tashkilotning tarmog‘iga xavfsiz ulanish uchun umumiy foydalanishdagi telekommunikatsion infratuzilmadan, masalan,

Internetdan foydalanishga imkon beradigan usul hisoblanadi. Binobarin, 802.11 simsiz tarmoqlari litseziyalanmaydigan chastotalar dipazonida ishlaydi va yashirin eshinishi mumkin, aynan ularda VPNni qurish va xizmat ko'rsatish, agar ma'lumotlarni yuqori himoyalash darajasi talab qilinsa alohida ahamiyatga ega bo'ladi (4.25- rasm).

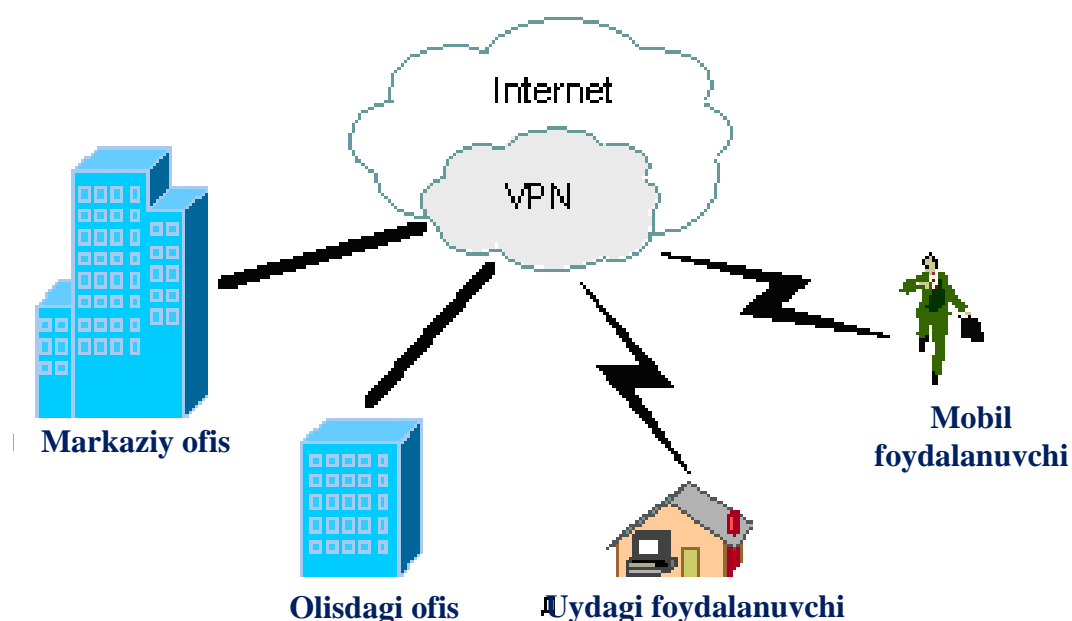


4.25- rasm. Olisidan foydalanuvchilar uchun VPN

Simsiz lokal tarmoqdagi ham xostlar orasidagi bog'lanishni, ham simsiz ko'priklar orasidagi ikki nuqtali kanallarni himoyalash kerak bo'ladi. O'ta maxfiy ma'lumotlarning xavfsizligini ta'minlash uchun qandaydir bitta himoyalash mexanizmini yoki tarmoqning faqat bitta darajasida himoyalashni ko'zda tutish mumkin emas. Ikki nuqtali tarmoqlar holida RADIUS-server va foydalanuvchilar haqidagi ma'lumotlar omboriga ega bo'lgan 802.11i standarti asosida himoyalashni amalga oshirishga qaraganda ikkita tarmoqlarni qamrab oladigan VPNni qurish oddiy va tejamli bo'ladi. Tarmoqlar orasidagi yuqori tezlikli kanal bo'lganida oldindan ajratigan kalitlar (PSK) va 802.1x protokoli asosidagi standartdan foydalanish eng xavfsiz usul hisoblanmaydi. VPN bu faqat bitta tashkilot tomonidan ishlatilishi mumkin bo'lgan o'z yoki ijaraga olingan liniyalari qimmat turadigan tizimning to'liq aksi hisoblanadi. VPNning vazifasi o'sha imkoniyatlarni, lekin ancha past narxlarda tashkilotga taqdim etish hisoblanadi. Buni qimmat ajratilgan liniyalari o'rniga ko'priqli ikki

nuqtali simsiz kanallar hisobiga aloqani ta'minlanishi bilan taqqoslang.

VPN va simsiz texnologiyalar raqobatlashmaydi, balki birbirlarini to'ldiradi (4.26-rasm). VPN ajratiladigan umumiy foydalanishdagi tarmoqlar ustidan ishlaydi, shu bilan bir vaqtda maxsus xavfsizlik choralari va kanal darajasidagi tunnel protokoli (Layer Two Tunneling Protocol - L2TP) kabi tunnel protokollarining qo'llanilishi hisobiga konfidensiallikni ta'minlaydi. Ularning mazmuni shundan iboratki, jo'natish uchida ma'lumotlarni shifrlash va qabul qilish uchida ularni deshifrlash bilan protokol kerakli tarzda shifrlanmagan ma'lumotlar tusha olmaydigan "tunnelni" tashkil etadi.



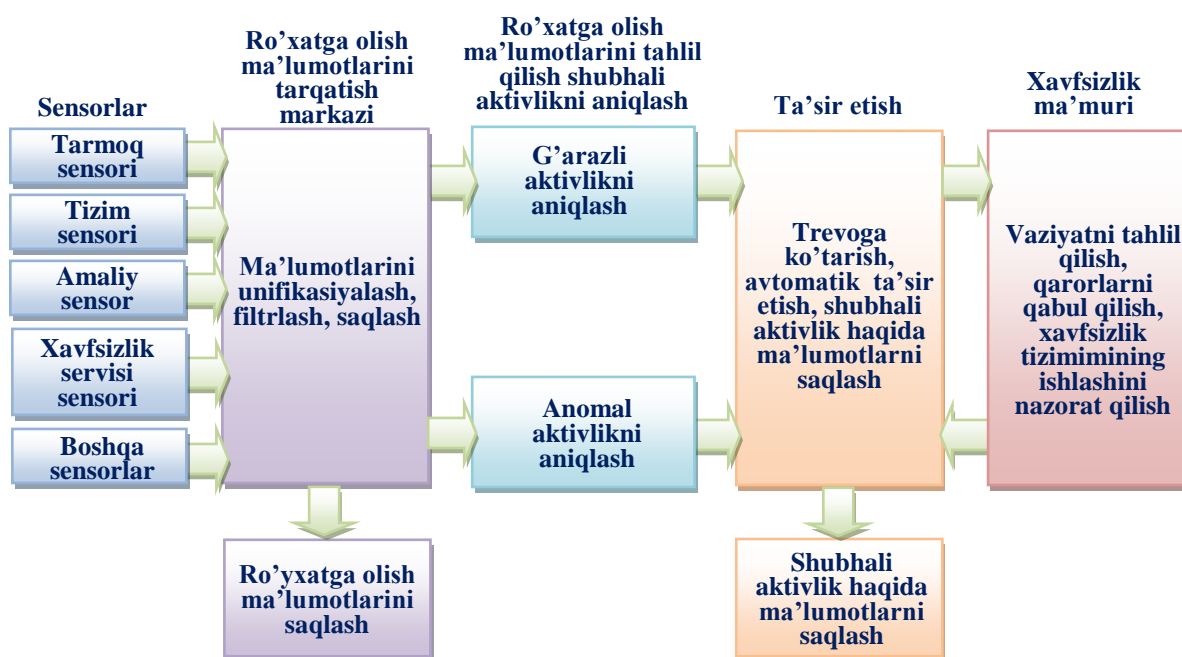
4.26- rasm. Virtual xususiy tarmoq

Nafaqat ma'lumotlarning o'zini, balki jo'natuvchi va oluvchining tarmoq manzillarini shifrlash qo'shimcha xavfsizlikni ta'minlashi mumkin. Simsiz lokal tarmoqni ajratiladigan umumiy foydalanishdagi tarmoqqa qiyoslash mumkin, ayrim hollarda esa (xot-spotlar, hamjamiyatga tegishli tugunlar) u shunday ham hisoblanadi.

VPN konfidensiallik, yaxlitlik va mumkinlik shartlariga javob beradi. Ta'kidlash kerakki, hech bir VPN DoS yoki DDoS-hujumlarga barqaror emas va o'zining virual tabiati va past turadigan protokollarga bog'liqligi tufayli fizik darajadaga mumkinlikni kafolatlay olmaydi.

VPNning ikkita muhim o‘ziga xos xususiyati, ayniqsa signalning tarqalishi ustidan cheklangan nazorat mavjud bo‘lgan simsiz muhitda yaxlitlik va ma’lumotlarning konfidensialligi hisoblanadi. G‘arazgo‘y WEP protokoli bo‘yicha shifrlashni yengib o‘tishga va simsiz lokal tarmoqqa ulanishga erishgan hayotiy vaziyatni olamiz. Agar VPN bo‘lmasa, u holda g‘arazgo‘y ma’lumotlarni yashirincha eshitishi va tarmoqning ishlashiga aralashishi mumkin. Lekin, agar paketlar autentifikatsiyalangan bo‘lsa, “o‘rtadagi shaxs” hujumi haligacha ma’lumotlarni qo‘lga kiritish oson bo‘lsada deyarli mumkin bo‘lmaydi. VPNga shifrlash elementlarining kiritilishi ma’lumotlarni qo‘lga kiritishning salbiy oqibatlarini kamaytiradi. VPNni tasniflashning ko‘plab usullari mavjud, lekin uchta asosiy turlari “tarmoq-tarmoq”, “xost-tarmoq” va “xost-xost” topologiyalardan iborat.

“Tarmoq-tarmoq” topologiyasi. Bu atama bilan ba’zan ikkita geografik ajratilgan xususiy tarmoqlar orasidagi VPN-tunnel tavsiflanadi (4.27-rasm).



4.27- rasm. “Tarmoq-tarmoq” topologiyasi

Bunday turdagi VPN odatda lokal tarmoqlarni umumiy foydalanishdagi tarmoq yordamida xuddi ular bitta bino ichidagidek birlashtirish kerak bo‘lganida qo‘llaniladi.

Bunday konfiguratsiyaning asosiy afzalligi shundan iboratki, tarmoqlar aralashdek ko‘rinadi, VPN-shlyuzlarning ishlashi uchun

foydalanuvchilar uchun ochiq bo‘ladi. Bu holda ham tunnellashtirish muhim, chunki xususiy tarmoqlarda odatda RFC 1918 hujjatda tavsiflangan zaxiralashtirilgan manzillar ishlatiladi, ular Internet orqali marshrutlashtirilishi mumkin emas. Shuning uchun muvaffaqiyatli o‘zaro ta’sirlashtirish uchun trafikni tunnelga inkapsulyatsiyalash zarur.

Bunday tarmoqqa oddiy misol bitta tashkilotning ikkita filiallarini ikki nuqtali simsiz kanal bo‘yicha bog‘lanishi bo‘lishi mumkin. Trafik tashkilotning ichki infratuzilmasi chegaralaridan chiqmasada, uning simsiz qismiga trafik umumiy foydalanishdagi tarmoq orqali marshrutlashtirilishidek diqqat bilan qarash kerak bo‘ladi. Bilamizki, WEP protokolini oson chetlab o‘tish mumkin va hatto TKIP ba’zan zaif bo‘ladi, shuning uchun hamma joyda qo‘shimcha shifrlash ishlatilishi tavsiya etiladi.

“Xost-tarmoq” topologiyasi. Bunday konfiguratsiyada olisdagi foydalanuvchilar korporativ tarmoqqa Internet tarmog‘i orqali ulanadi.

Dastlab mobil mijoz Internet bilan bog‘lanishni o‘rnatadi, keyin esa korporativ VPN-shlyuz bilan shifrlangan tunnelni tashkil etishga so‘rovni uyushtiradi. Muvaffaqiyatli autentifikatsiyalashdan keyin umumiy foydalanishdagi tarmoq ustidan tunnel hosil qilinadi va mijoz ichki tarmoqdagi oddiy yana bir mashina bo‘lib qoladi. Uyda bajariladigan ishlarning keng tarqalishi VPNning bunday qo‘llanilishini kuchaytiradi.

Qatnashchilar soni uncha katta bo‘lmagan “tarmoq-tarmoq” turdagi VPNdan farqli ravishda “xost-tarmoq” turdagi VPN juda katta o‘lchamlargacha ortishi mumkin. Shuning uchun tizim ma’muri masshtablanadigan mijozlarni autentifikatsiyalash va kalitlarni boshqarish mexnizmni oldindan o‘ylab ko‘rishi kerak bo‘ladi.

“Xost-xost” topologiyasi. Bunday topologiya juda kam uchraydi. Gap bir-birlari bilan shifrlangan va shifrlanmagan ma’lumotlarni almashadigan ikkita xostlar haqida bormoqda. Bunday konfiguratsiyada tunnel ikkita xostlar orasida tashkil etiladi va ular orasidagi butun trafik VPN ichida inkapsulyasiyalanadi. Bunday tarmoqlarda amaliy qo‘llanishlar kam, lekin misol sifatida geografik ajratilgan zahiralashtirish serverini aytish mumkin. Har ikkala xostlar Internetga ulangan va markaziy serverdan ma’lumotlar manzillashtirish serveriga simmetrik ko‘chiriladi. Masalan, “xost-xost” turdagi oddiy VPN tarmoqlar bitta darajali tarmoqlarni (Ad Hoc) himoyalash uchun ishlatilishi mumkin.

Tunnellash usuli bo'yicha ma'lumotlar paketi umumfoydalanuvchi tarmoq orqali xuddi oddiy ikki nuqtali ulanish bo'yicha uzatilganidek uzatiladi. Har bir "jo'natuvchi-qabul qiluvchi" juftligi orasiga bir protokol ma'lumotlarini boshqasining paketiga inkapsulyatsiyalashga imkon beruvchi o'ziga xos tunnel-mantiqiy ulanish o'rnatiladi.

Tunnellashga binoan, uzatiluvchi ma'lumotlar porsiyasi xizmatchi hoshiyalar bilan birga yangi "konvert"ga "joylash" amalga oshiriladi. Bunda pastroq satx protokoli paketi yuqoriroq yoki xuddi shunday sath protokoli paketi ma'lumotlari maydoniga joylashtiriladi.

Tunnellashdan paket tarkibini nafaqat konfidentsialligini, balki uning butunligini va autentiligini ta'minlashda foydalaniladi. Bunda elektron raqamli imzoni paketning barcha hoshiyalariga tarqatish mumkin.

Internet bilan bog'lanmagan lokal tarmoq yaratilganda kompaniya o'zining tarmoq qurilmalari va kompyuterlari uchun hohlagan IP-adresdan foydalanishi mumkin.

Tunnellash mexanizmi himoyalannuvchi kanalni shakllantiruvchi turli protokollarda keng qo'llaniladi. Odatda tunnel faqat ma'lumotlarning konfidentsialligi va yaxlitligining buzilishi xavfi mavjud bo'lgan ochiq tarmoq qismida, masalan, ochiq Internet va korporativ tarmoq kirish nuqtalari orasida yaratiladi.

Bunda tashqi paketlar uchun ushbu ikki nuqtada o'rnatilgan chegara marshrutizatorlarining adreslaridan foydalanilsa, oxirgi uzellarning ichki adreslari ichki dastlabki paketlarda ximoyalangan holda saqlanadi.

Tunnellash mexanizmini amalga oshirilishiga uch xil protokollar ishlatiladi:

- protokol- «yo'lovchi»;
- protokol eltuvchi;
- tunnellash.

Protokol - "yo'lovchi" sifatida bitta korxonada filiallarining lokal tarmoqlarida ma'lumotlarni tashuvchi transport protokoli IPX ishlatilishi mumkin. Eltuvchi protokolning eng ko'p tarqalgan varianti Internet tarmog'ining IP protokoli hisoblanadi.

Tunnellash protokoli sifatida kanal sathi protokollari PPTP va L2TP, xamda tarmoq satxi protokoli IPsec ishlatilishi mumkin. Tunnellash tufayli Internet infratuzilmasini VPN-illovalardan berkitish mumkin bo'ladi.

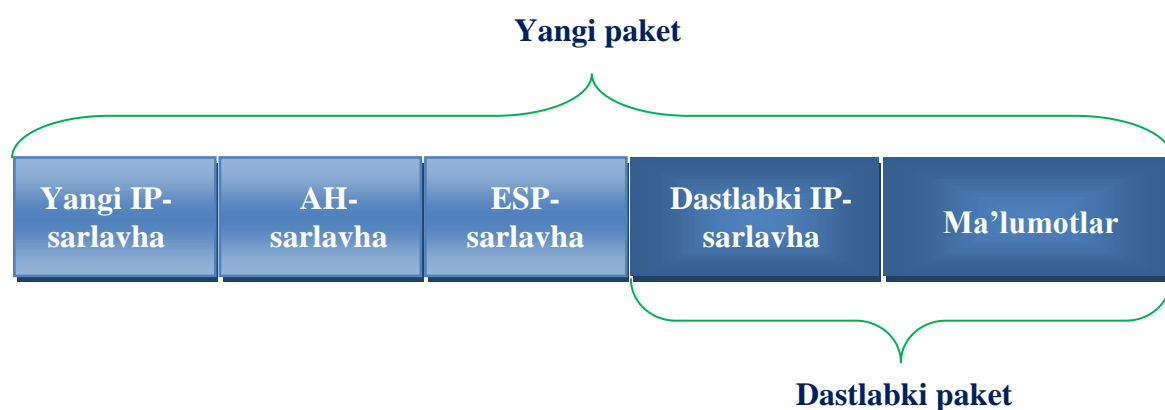
Tunnellashning o‘zi ma’lumotlarni ruxsatsiz foydalanishdan yoki buzishdan himoyalamaydi, ammo tunnellash tufayli inkapsulyasiyalanuvchi dastlabki paketlarni to‘la kriptografik himoyalash imkoniyati paydo bo‘ladi.

Uzatiluvchi ma’lumotlar konfidentsialligini ta’minlash maqsadida jo‘natuvchi dastlabki paketlarni shifrlaydi, ularni, yangi IP-sarlavxa bilan tashqi paketga joylaydi va tranzit tarmoq bo‘yicha jo‘natadi (4.28-rasm).

Ochiq tarmoq bo‘yicha ma’lumotlarni tashishda tashqi paket sarlavhasining ochiq kanallaridan foydalaniladi.

Inkapsulyasiya o‘z - o‘zidan tunnellashtiriladigan ma’lumotlarning konfidentsialligi va butunligi darajasini oshirmaydi.

Konfidentsiallik shifrlash yordamida ta’minlanadi. Ma’lumotlarni shifrlash usullarining ko‘pligi sababli, initsiator va tunnel terminatori bir xil usuldan foydalanishi muhim o‘rin tutadi. Bundan tashqari ma’lumotlarni muvaffaqiyatli shifrini yechish uchun initsiator va terminator kalitlar bilan almashish imkoniga ega bo‘lishlari kerak. Tunnellar faqat vakolatli foydalanuvchilar o‘rtasida yaratilishi uchun oxirgi nuqtalar identifikatsiya qilinishi kerak. Tunnellanadigan ma’lumotlarning butunligini xabarni tanlab olish shaklida yoki o‘zgartirish yoki yo‘q qilishni aniqlash uchun xesh-funksiya yordamida ta’minlash mumkin.



4.28- rasm. Tunnellashga tayyorlangan paket ko‘rinishi

Uchinchi satx (va undan ham yuqori sath) trafigini inkapsulyasiya qilishning unifikatsiya qilingan usulini Windows mijozlari va serverlarida amalga oshirish uchun Microsoft, Ascend Communications va 3Com kompaniyalari o‘zida RRR protokolining kengaytirilishini ifodalovchi ikki nuqta o‘rtasida ma’lumotlarni

yetakzib berilishini boshqarishning tunel protokolini (Point-to-Point Tunneling Protocol, RRTR) ishlab chiqdilar.

Cisco Systems kompaniyasi OSI (Layer-2 Forwarding, L2F) modelining ikkinchi sathida tarqatish protokolini ishlab chiqdilar, bu yordamida uzoq masofadagi mijozlar Internet provayderi kanallari bo‘ylab bog‘lanishlari va identifikatsyalanishlari mumkin.

Ushbu ikkita bir biri bilan chambarchas bog‘langan IETF protokollari birlashtirilgan bo‘lib va natijada eng yaxshi RRTR va L2Fni o‘z ichiga oluvchi protokol yuzaga keldi va u ikkinchi sath tunnellash protokoli (Layer-2 Tunneling Protocol, L2TP) deb nomlanadi. Uni Cisco, Microsoft, 3Com, Ascend kompaniyalari va bir qancha boshqa ishlab chiqaruvchilar qo‘llab quvvatladilar. Avval uchragan ikkinchi sath protokollari singari, L2TPning spetsifikatsiyasi identifikatsiya va shifrlash usullarini ta’riflamaydi.

VPNning barcha komponentlari uchun standart usullar tavsiflangan IETF spetsifikatsiyasi bo‘lib IPsec (Internet Protocol Security) protokoli hisoblanadi, ba’zida u uchinchi sath tunnellash (Layer-3 Tunneling) deb nomlanadi. IPsec protokoli tunnelni initsiatsiya qilishda foydalanuvchilarni yoki kompyuterlarni identifikatsiya qilishning standart usullarini, tunnelning oxirgi nuqtalari tomonidan shifrlashdan foydalanishning standart usullarini, shuningdek, oxirgi nuqtalar o‘rtasida shifrlash kalitlarini almashish va boshqarishning standart usullarini ko‘zda tutadi.

IPsec protokoli L2TP bilan birgalikda ishlashi mumkin, natijada ushbu ikkita protokol o‘ta ishonchli identifikatsiyani, standartlashtirilgan shifrlashni va ma’lumotlarning butunligini ta’minlaydi.

Initsiator va tunnel terminatori o‘rtasida uzatiladigan axborotning shifrlanishi, ko‘pincha transport sathi muxofazasi (Transport Layer Security, TLS) yordamida amalga oshiriladi. IETF brandmauerlar orqali autentifikatsiyalangan o‘tishni standartlashtirish uchun SOCKS nomli protokolni belgiladi va hozirgi vaqtda SOCKS 5 kanal vositachilarini standartlashtirilgan tarzda amalga oshirilishi uchun foydalanilmoqda.

Boshqa istalgan hisoblash funksiyasi kabi VPN tarmoqlarini yaratish ishlari dasturiy ta’minot yordamida o‘tkaziladi. VPNning yaratilishi uchun dasturiy ta’minot turli apparat platformalarida bajarilishi mumkin. VPN funksiyalari marshrutizatorlarni (OSI modelining uchinchi sathida), kommutatorlarni (OSI modelining

ikkinchi sathida), apparat va dasturiy amalga oshiriladigan brandmauerlarni qo‘llab-quvvatlashi mumkin.

4.10. Simsiz tarmoqlarda qo‘llaniladigan RADIUS va TACACS+ protokollarini taqqoslash

Uzoq masofadagi foydalanuvchilarning MUTdan foydalana olishini nazorat qilishning eng keng tarqalgan protokollariga RADIUS (Remote Authentication Dial-In User Service – foydalanuvchilarni bog‘lanadigan liniyalar bo‘yicha masofadan autentifikatsiyalash tizimi) va TACACS+ (Terminal Access Controller Access Control System - masofadan foydalanishni markazlashtirilgan nazorat qilish tizimi) protokollari kiradi [12].

RADIUS o‘z asosida UDP (User Data Protocol – foydalanuvchining ma’lumotlarini uzatish) protokolini ishlatadi, shuning uchun u nisbatan tez ishlaydi, mualliflashtirish jarayoni autentifikatsiyalash jarayoni kontekstida bo‘lib o‘tadi. RADIUS va serverning ishlatilishi mijozlarga bir jarayonli xizmat ko‘rsatishga (ko‘p jarayonli bo‘lishi mumkin bo‘lsada), yetarlicha cheklangan autentifikatsiyalash turlari sonini qo‘llab-quvvatlaydi va o‘rtacha muhofazalanganlik darajasiga ega.

TACACS+ protokoli TSR (Transport Control Protocol – uzatishlarni boshqarish) protokolini ishlatilishiga asoslangan, shuning uchun RADIUS protokolidan sekin ishlaydi, lekin jarayonlarni multi jarayonli qayta ishlashni (vaqtning har bir momentida bir nechta foydalanuvchilarga xizmat ko‘rsatilishi mumkin) olib borishga imkon beradi va yuqori muhofazalanganlik darajasiga ega (paketning butun tanasi shifrlangan).

RADIUS protokoli yo‘qotiladigan paketlar 5...10% dan kam bo‘ladigan tarmoqlarda samarador bo‘ladi, boshqa tarmoqlarda TACACS+ protokoli ishlatilishi yaxshi bo‘ladi.

Qandaydir serverdan foydalana olish uchun RADIUS protokoli bitta so‘rovni qayta ishlaydi (autentifikatsiyalash – so‘rov, javob), TACACS+ protokoli esa ikkita so‘rovni qayta ishlaydi (autentifikatsiyalash va mualliflashtirish), lekin bunda TACACS+ protokoli ishlatilganida boshqa serverdan foydalana olish imkoniyati mavjud.

Shifrlashda RADIUS protokoli parolda faqat clear text shifrlanadi, qolgan butun paket “ochiq” qoladi (xavfsizlik nuqtai

nazaridan hatto foydalanuvchining nomi juda muhim parametr bo'lsada).

TACACS+ protokolida paketning faqat sarlavhasi ochiq (hech qanday qimmatli axborotni tashimaydigan) qoladi, paketning butun tanasi esa shifrlanadi.

Biroq, TACACS+ protokolida uncha katta bo'lmagan zaiflik ham bor: TACACS+ protokoli hujjatlashtirishda outbound (ya'ni tashqi) deyiladigan mualliflashtirishni qo'llab-quvvatlaydi, ya'ni foydalanuvchini autentifikatsiyalash kerakmi yoki kerak emasmi qarorini mijozning o'zi qabul qiladi.

TACACS+ protokolida so'rovni qayta yo'naltirish imkoniyati yo'q. RADIUS protokoli esa bunday imkoniyatga ega. RADIUS-server so'rovni boshqa RADIUS-serverga qayta yo'naltirishni biladi. Shunday qilib, RADIUS protokoli ixcham taqsimlangan tizimni loyihalashtirishga imkon beradi.

RADIUS va TACACS+ protokollari taqdim etadigan imkoniyatlar 4.2- jadvalda keltirilgan.

4.2- jadval

RADIUS va TACACS+ protokollarini taqqoslash

	RADIUS	TACACS+
Bazaviy protokol	UDP	TCP
Ishlatiladigan servislar	Autentifikatsiyalash, mualliflashtirish va hisobga olish birlashtirilgan	Autentifikatsiyalash, mualliflashtirish va hisobga olish alohida
Xavfsizlik	Faqat parollar shifrlanadi. Ma'lumotlar bazasidagi parollar ochiq ko'rinishda saqlanadi	Serverlar va mijozlar orasidagi barcha paketlar shifrlanadi. Ma'lumotlar bazasidagi parollar shifrlanishi mumkin
So'rovni qayta yo'naltirish imkoniyati	Bor	Yo'q

Ko‘rib chiqilgan protokollarning samaradorliklarini nisbiy tahlil qilish maqsadida REUdan muhofaza qilish vositasining dasturini deshifrlash uchun buzg‘unchiga zarur bo‘ladigan o‘rtacha vaqtni baholashga bog‘liq bo‘lgan hisoblashlar amalga oshirilgan.

Dasturni deshifrlash uchun T o‘rtacha vaqt quyidagicha aniqlanadi [3,4]:

$$T = 3 \times n \times \frac{N^2 \times \log_2 \eta}{4 \times S}, \quad (4.1)$$

bu yerda n – tizim ishlatadigan serverlar soni;

N – qandaydir tilda yozilgan dastur matnining uzunligi, bit;

η - dastur matni tilining alfaviti;

S – Straud soni (sekundiga $S=4 \div 20$ operatsiyalar), buzg‘unchi bir vaqtda ish olib borishi mumkin bo‘lgan ob’ektlar sonini xarakterlaydi.

RADIUS uchun:

$$T = 3 \times \frac{10000^2 \times \log_2 256}{4 \times 20} = 30000000c \approx 347 \text{ кун}$$

TACACS+ uchun:

$$T = 3 \times \frac{10500^2 \times \log_2 256}{4 \times 20} = 33075000c \approx 383 \text{ кун}$$

Demak, axborotlarni himoyalash vositasining dasturini rasshifrovka qilib bo‘lmaslik ehtimolliligini quyidagi formula bo‘yicha hisoblash mumkin:

$$P = \frac{\beta}{\beta + \frac{1}{T}}, \quad (4.2)$$

Bu yerda β – Puasson qonuni bilan tavsiflanadigan 0,001 ga teng bo‘lgan parametr.

Axborotlarni muhofaza qilish vositasining dasturini ochib bo‘lmaslik ehtimolliligini hisoblaymiz:

RADIUS uchun:

$$P = \frac{0,001}{0,001 + \frac{1}{30000000}} = 0,999967$$

TACACS+ uchun:

$$P = \frac{0,001}{0,001 + \frac{1}{33075000}} = 0,99997$$

Himoya qilish vositasining dasturini deshifrlash uchun buzg'unchiga zarur bo'ladigan o'rtacha vaqtning bog'liqlik tahlili ko'rsatdiki, buzg'unchiga ochish qilish uchun o'rtacha bir yil zarur bo'ladi.

Uzoq masofadan foydalana olish protokollarining nisbiy taqqoslash natijasi shuni ko'rsatadiki, TACACS+ protokoli RADIUS protokoliga qaraganda kengroq imkoniyatlar to'plamiga va yuqori muhofazalanganlik darajasiga ega. Lekin, RADIUS protokoli qulayligi va tez ishlashi sababli simsiz aloqa tarmoqlarida keng qo'llaniladi.

4.11. Uzatiladigan ma'lumotlarning yaxlitligi va konfidensialligi

Tarmoq kompyuterlariga olisdan kirish imkoniyati keltirib chiqaradigan muammolardan tashqari, tarmoqlar o'z tabiati bo'yicha yana bir xavf turi bo'lgan tarmoq bo'yicha uzatiladigan xabarlarni qo'lga kiritish va tahlil qilish, shuningdek "soxta" trafikni yaratilishiga uchraydi [13]. Tarmoq xavfsizligini ta'minlash vositalarining katta qismi aynan bu turdagi buzishlarni oldini olishga yo'naltirilgan.

Axborot xavfsizligi sohasidagi asosiy xarakteristikalar:

1. Ma'lumotlarning konfidensialligi;
2. Ma'lumotlarning yaxlitligi;
3. Ma'lumotlarning mumkinligi hisoblanadi.

Ma'lumotlarning konfidensialligi bu ma'lumotlarga ulanishga ega bo'lgan shaxslar doirasiga ma'lum cheklashlarni kiritilishini ko'zda tutadi. Konfidensiallik darajasi oshkora qilinmaydigan, cheklangan shaxslar doirasiga mo'ljallangan, sir hisoblanadigan ma'lumotlarni bo'lishiga bog'liq ravishda ma'lumotlarning egasi tomonidan sub'ektiv aniqlanadigan qandaydir shartli xarakteristika (o'ta muhimlik, mutlaqo maxfiy, maxfiy, xizmat manfaatlari uchun, bosish uchun emas va h.k.) orqali ifodalanadi. Tabiiyki, o'rnatilgan ma'lumotlar konfidensialligi darajasi ularni aborot tizimlarida ishlov berilishida va simsiz tarmoq bo'yicha uzatilishida saqlanishi kerak.

Simsiz aloqa tarmoqlari axborot xavfsizligini ta'minlash maqsadida xalqaro tashkilotlarning standartlari va tavsiyalarini tahlil qilish asosida simsiz aloqa tarmoqlari operatorlari uchun shart hisoblanadigan axborot xavfsizligining umumiy talablarini ishlab chiqish zarur. Bunda umumiy talablarni ishlab chiqish simsiz aloqa

tarmoqlarining zaifliklarini va xavfsizlikka xavf va bo'lishi mumkin zarar nuqtai nazaridan buzuvchining bo'lishi mumkin ta'sir etishlarini tahlil qilish asosida olingan axborot xavfsizligiga eng xavfli tahdidlardan kelib chiqishi kerak.

Simsiz aloqa tarmoqlari axborot xavfsizligi bo'yicha talablarning bajarilishi tarmoqning xarakteristikalariga ikki tomonlama ta'sir qiladi. Bir tomondan tarmoqning himoyalanganligi ortadi, boshqa tomondan esa qo'shimcha qurilmalarning hajmi ortadi, bu o'z navbatida ishonchlilikni, unumdorlikni kamayishiga olib keladi va foydalanuvchilarning foydalanishiga vaqtini oshiradi. Bunda tarmoq komponentlarining funksional parametrlarini xavfsizlikka talablar bilan birga ko'rib chiqish zarur, chunki xavfsizlik bo'yicha qo'shimcha talablarning ishlatilishi tizimning unumdorligi va ishonchliligini kamayishiga, tarmoqning qator ekspluatatsion xarakteristikalarini o'zgarishiga olib keladi.

Xavfsizlikka talablar funksional talablarga (ishlash qulayligi, tezkor ishlash va boshqalar) qarama-qarshi bo'ladi, moslashuvchanlikka cheklashlarni qo'yadi va juda keng tarqalgan, lekin himoyalangan amaliy dasturiy vositalarni rad etishga majburlaydi.

Rivojlangan mamlakatlarning xalqaro tajribasi ko'rsatadiki, simsiz aloqa tarmoqlari axborot xavfsizligi muammosining yechimi mos qonunlar, standartlar va me'yoriy-uslubiy hujjatlar ko'rsatmalari va talablariga asoslanishi kerak.

Qonunchilik talablarining so'zsiz bajarilishi va simsiz aloqa tarmoqlari axborot xavfsizligi sohasidagi zarur me'yoriy-huquqiy hujjatlarni o'z vaqtida ishlab chiqish va qabul qilish axborot xavfsizligini buzilishini oldini olishning kuchli qonuniy-huquqiy chorasi hisoblanadi, shuning uchun bugungi kunda axborot xavfsizligini ta'minlashning turli jihatlarining ichidan eng muhimi va dolzarbi axborot xavfsizligining me'yoriy-huquqiy ta'minlanishi masalasi hisoblanadi.

Simsiz aloqa tarmoqlarining axborot xavfsizligiga umumiy talablar tarmoq egasi yoki bu tarmoqda aylanadigan ma'lumotlar egasi tomonidan axborot xavfsizligi tashkil etuvchilari – konfidensiallik, yaxlitlik va foydalanishga olishganliklarning har birini buzilishlari oqibatlarining jiddiyligini tahlil qilish asosida shakllantirilishi va o'rnatilishi kerak. O'z navbatida, umumiy talablar simsiz aloqa tarmog'idagi funksiyalari va ular yechadigan masalalarga muvofiq

dasturiy texnik vositalarga va protokollarga majburiy talablarga transformatsiyalanadi.

Zamonaviy simsiz aloqa tarmoqlarini qurishda vujudga keladigan muhim muammo ishonchliligi, yashovchanligi va barqarorligi bilan bir qatorda ularning axborot xavfsizligini ta'minlash hisoblanadi. Ishlardagi muhim yo'nalish axborot xavfsizligining o'ziga tizimli yondashish hisoblanadi. U simsiz aloqa tarmoqlari hayot siklining barcha loyihalashtirish, qurish va ishlatish bosqichlarida axborot xavfsizligini ta'minlashning mos choralarini va mexanizmlarini yaratilishini ko'zda tutadi. Xalqaro tajriba ko'rsatadiki, simsiz aloqa tarmoqlarining axborot sohasiga buzuvchining ta'sir etishi ularning hayot siklining texnologik va ekspluatatsiya qilish bosqichlarida amalga oshirilishi mumkin, shuning uchun ularning axborot xavfsizligini ta'minlash muammosida ikkita texnologik va ekspluatatsion jihatlarni ajratish zarur. Tarmoqlarning texnologik xavfsizligi apparatlar vositalari va DT ning jinoyatkorona texnik va dasturiy nuqsonlarga ("qo'yilmalar, "troya otlari" va h.k.), ya'ni noxush oqibatlarga olib keladigan ma'lum vaqt tugashi bo'yicha yoki tashqi komanda bo'yicha ruxsat etilmagan ta'sir etishlarni amalga oshirishga qodir bo'lgan vositalarga ega bo'lmaslik xossalari xarakterlaydi.

Axborot xavfsizligining boshqa xarakteristikasi ma'lumotlarning yaxlitligi, ya'ni ma'lumotlarni ruxsat etilmagan buzilishi va soxtalashtirilishini oldini olish ta'minlanadigan ma'lumotlarning holati hisoblanadi.

Shuningdek, foydalanuvchilarga ular uchun mo'ljallangan ma'lumotlarni to'siqlarsiz va o'z vaqtida olish uchun ta'minlanadigan ma'lumotlarning mumkinligi – ma'lumotlar va ularni tashuvchining holati ham muhim rol o'ynaydi.

Ma'lumotlarga ruxsat etilmagan shaxslarni ularga ulanishi, operatorlar, foydalanuvchilar yoki dasturlarning atayin yoki atayin bo'lmagan xatoliklari, qurilmalarning uzilishlari tufayli ma'lumotlarning noto'g'ri o'zgartirilishi bu ma'lumotlarning eng muhim xususiyatlarini buzilishiga olib keladi va ularni yaroqsiz va hatto xavfli qiladi. Uning ishlatilishi moddiy va ma'naviy zararga olib kelishi mumkin, shuning uchun ma'lumotlarni himoyalash tizimini yaratilishi dolzarb masala bo'lib qoladi. Ma'lumotlarning xavfsizligi deganda ma'lumotlarni keraksiz oshkora qilinishidan (konfidensiallikni buzilishidan), buzilishidan (yaxlitlikni

buzilishidan), yo‘qotilishidan va mumkinlik darajasini kamayishidan, shuningdek ularning noqonuniy ko‘paytirilishidan ma’lumotlarning himoyalanganligi tushuniladi.

Ma’lumotlarning konfidensialligi ularni ruxsat etilmagan ochilishidan himoyalashni ta’minlaydi va quyidagi shakllardan tashkil topishi mumkin:

1. Bog‘lanishning konfidensialligi n-nchi bog‘lanish bo‘yicha uzatishda n-nchi foydalanuvchining barcha ma’lumotlarining konfidensialligini ta’minlaydi;

2. Bog‘lanishsiz konfidensiallik bog‘lanish o‘rnatilishsiz n-nchi daraja xizmatlarining bitta ma’lumotlar blokida uzatiladigan n-foydalanuvchining barcha ma’lumotlarining konfidensialligini ta’minlaydi;

3. Tanlanma maydonlarning konfidensialligi bog‘lanish o‘rnatilishsiz n-nchi daraja xizmatlarining bitta ma’lumotlar blokida yoki n-nchi bog‘lanish bo‘yicha uzatilishida n-foydalanuvchining tanlanma maydonlarining konfidensialligini ta’minlaydi;

4. Ma’lumotlar oqimining konfidensialligi ma’lumotlar oqimini tahlil qilishda olinadigan ma’lumotlarning konfidensialligini ta’minlaydi;

5. Qayta tiklanishli bog‘lanishning yaxlitligi istalgan modifikatsiyalash, qo‘yilmalar, butun ma’lumotlar bloklari ketma-ketligidagi istalgan ma’lumotlarning yo‘qotilishi va takrorlanishlari va qayta tiklanishi imkoniyatlari aniqlanadigan n-nchi bog‘lanish bo‘yicha n-foydalanuvchining barcha ma’lumotlarining yaxlitligini saqlanishiga yo‘naltirilgan;

6. Qayta tiklanishsiz bog‘lanishning yaxlitligi qayta tiklanishli bog‘lanishning yaxlitligiga o‘xshash, lekin qayta tiklash protsedurasiga ega bo‘lmaydi;

7. Bog‘lanish tanlanma maydonlarining yaxlitligi n-nchi bog‘lanish bo‘yicha uzatishda n-nchi xizmatlarning ma’lumotlar blokida n-foydalanuvchining ma’lumotlari tanlanma maydonlarining yaxlitligini ta’minlaydi;

8. Bog‘lanishsiz yaxlitlik bog‘lanishsiz n-nchi xizmatlarning bitta ma’lumotlar blokining yaxlitligini ta’minlaydi va modifikatsiyalash dalilini aniqlash shaklini qabul qiladi;

9. Bog‘lanishsiz tanlanma maydonlarning yaxlitligi bog‘lanishsiz uzatiladigan xizmatlarning bitta ma’lumotlar blokidagi tanlanma maydonlarning yaxlitligini ta’minlaydi;

10. Manba tasdiqlanadigan rad etishlarda himoyalash oluvchini jo‘natuvchining ma’lumotlarni jo‘natilishi dalilini yoki ularning tarkibini xato rad etishga urnishlari qarshi himoyalaydigan ma’lumotlarni kelib chiqishining zarur isbotlari bilan ta’minlaydi;

11. Yetkazish tasdiqlanadigan rad etishlarda himoyalash jo‘natuvchini oluvchining ma’lumotlarni olinishi dalilini yoki ularning tarkibini xato rad etishga urnishlari qarshi himoyalaydigan ma’lumotlarni yetkazilishining zarur isbotlari bilan ta’minlaydi.

Ma’lumotlarni almashlash seansida himoyalashga, shu jumladan ma’lumotlarning konfidensialligiga, yaxlitlik va autentifikatsiyalashga maxsus talablarning aniqlanishi himoyalash ma’muriy boshqaruvi yoki amaliy daraja ma’muriy boshqaruvi orqali amaliy daraja beradigan ma’lumotlar asosida amalga oshirilishi mumkin.

Axborot xavfsizligini ta’minlash bir martalik ish bo‘lmazligi kerak. Bu himoyalash tizimini takomillashtirish va rivojlantirishning eng oqilona usullari va yo‘llarini asoslash va ishlatishdan, uning holatini uzluksiz nazorat qilishdan, uning zaif va kuchsiz joylari va qonunga qarshi harakatlarni aniqlashdan iborat bo‘lgan uzluksiz jarayon hisoblanadi.

Simsiz aloqa tarmoqlari axborot xavfsizligining asosiy tashkil etuvchilari quyidagilar hisoblanadi:

- konfidensiallik, ya’ni axborotlarni ruxsat etilmagan olinishidan himoya qilish;
- yaxlitlik, ya’ni axborotlarni va resurslarni ruxsat etilmagan buzilishidan himoya qilish;
- foydalana olishlik, ya’ni axborotlarni va resurslarni ruxsat etilmagan blokirovkalanishidan (to‘silishidan) himoya qilish.

Simsiz aloqa tarmoqlarining axborot xavfsizligiga tahdidlarning o‘tib borishi sharoitlarida bo‘lishi mumkin xavfsizlikning buzilishlarni aks ettiradigan va buzuvchilarni aniqlaydigan axborot xavfsizligini boshqarish jarayonlarini mos tadqiq qilish va ishlab chiqish zarur.

Simsiz aloqa tarmoqlari axborot xavfsizligining zamonaviy holati uchun tez yechilishini talab qiladigan quyidagi muammolar xarakterli hisoblanadi:

- turli simsiz aloqa tarmoqlari uchun axborot xavfsizligini ta’minlashning o‘zaro muvofiqligining, shu jumladan standartlar, protokollar, axborot resurslarining mavjud emasligi;

– e’lon qilinmagan imkoniyatlarga (“qo’yilmalar” va boshqalar) potensial bo’lgan xorijiy ishlab chiqarish texnik vositalaridan keng foydalanish;

– huquqbuzarlikning asosli bazasini yaratish uchun zarur bo’ladigan simsiz aloqa tarmoqlarining ishlatilishini hujjatlashtirilishi uslubiyatini yetarli darajada ishlab chiqilmaganligi;

– simsiz aloqa tarmoqlarining umumiy foydalanishdagi telekommunikatsiya tarmoqlariga ulanishida va o’zaro ishlashida axborot xavfsizligini ta’minlash bo’yicha kompleks yechimlarning mavjud emasligi;

– e’lon qilinmagan funksiyalarni ishlatadigan va tarmoqlarning normal ishlashini buzadigan komponentlar va dasturlarning joriy etilishi imkoniyati;

– tarmoq ishlatilgan muhofaza qilish mexanizmlari tomonidan axborot xavfsizligini ta’minlash jarayoniga berilgan talablarni bajarilmasligi;

– xavfsizlik talablariga muvofiq sertifikatlanmagan texnik vositalarning ishlatilishi.

802.11 standartda ma’lumotlarning konfidensialligi

802.11 standartda ma’lumotlarning konfidensiallik radiointerfeys uchun kriptografik usuldan foydalanish orqali ta’minlanadi. WEPda konfidensiallikni ta’minlanishi uchun psevdotasodifiy kalitli ketma-ketlikni generatsiyalaydigan simmetrik RC4 oqimli shifrlash algoritmi ishlatiladi. Bu asosiy oqim uzatiladigan ma’lumotlarga oddiy 2 modul (XOR) bo’yicha qo’shiladi. WEP usuli bo’yicha ma’lumotlar radiokanal bo’yicha uzatilishida ochilishidan himoyalaniishi mumkin. WEP TCP/IP, IPX, HTTP va boshqalar trafiklarini himoyalash uchun 802.11 WLAN darajalardan yuqorida joylashgan barcha ma’lumotlarga qo’llaniladi.

802.11 standartida faqat 40-bitli kalitlarni qo’llash tavsiya etilgan. Shunga qaramay, bir necha ishlab chiqaruvchilar WEPning standartlashtirilmagan kengaytirishlarini taklif etishgan, ular 40 dan 128 bitgacha kalitlar uzunliklarini qo’llaydi.

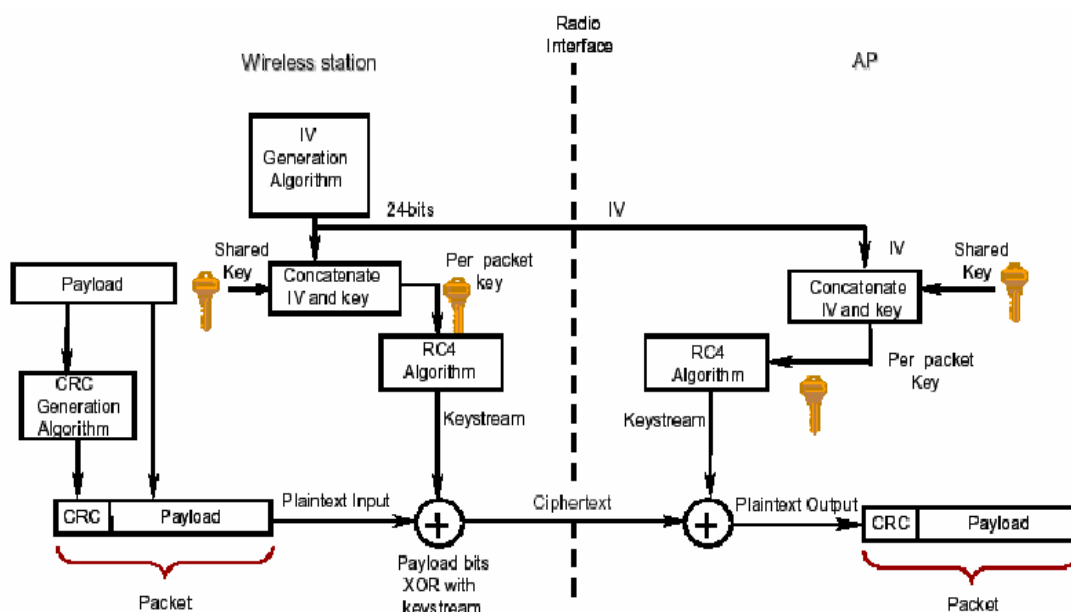
Konseptual jihatdan algoritm 4.29-rasmda tasvirlangan.

802.11 standartda ma’lumotlarning yaxlitligi

IEEE 802.11 spetsifikatsiyasi radiomijozlar va ulanish nuqtalari orasidagi uzatiladigan ma’lumotlar yaxlitligini ta’minlash vositalarini tavsiflaydi. Bu xavfsizlik chorasi radiokanal bo’yicha uzatilishi vaqtida buzuvchi orqali buzilgan istalgan xabarlarini inkor qilish uchun

qoʻllaniladi. Bu usul ortiqcha siklli kodlar yordamida nazorat qilishni ishlatadi. 4.29-rasmda tasvirlanganidek, CRC-32 (yoki FCS kadrni tekshirish ketma-ketligi) uzatishdan oldi foydali maʼlumotlarning har bir kadri uchun hisoblanadi.

Bunday tarzda yigʻilgan paket keyin RC4 kalit oqimidan foydalanish bilan shifrlanadi. Qabullash tomonida deshifrlash bajariladi va yana CRC hisoblanadi, u keyin xabar bilan birga kelgan CRC bilan taqqoslanadi. Bu ikkita CRClar bir-birlariga teng boʻlmasa, u holda bu yaxlitlikni buzilganligini bildiradi va paket yoʻqotiladi.



4.29-rasm. 802.11 standartida faqat 40-bitli kalitlarni qoʻllash agoritmi

Konfidensiallikni taʼminlash bilan holdagi kabi 802.11 standartdagi yaxlitlik kalitning uzunligiga bogʻliq boʻlmagan holda ayrim hujumlar turlariga nisbatan zaif. WEPda yaxlitlikni taʼminlash sxemasidagi fundamental kamchilik shu hisoblanadiki, oddiy CRC, masalan, xesh-funksiya kabi kriptografik xavfsiz mexanizm hisoblanmaydi.

4.12. WiMAX tarmoqlarida axborot xavfsizligi masalalari

IEEE 802.16 standartiga asoslangan WiMAX simsiz keng polosali ulanish tarmoqlari bugungi kunda istiqbolli, tez rivojlanayotgan aloqa texnologiyasi hisoblanadi [16]. Ularda Wi-Fi

(IEEE 802.11 standart) tarmoqlaridagi kabi simli tarmoqlardagiga qaraganda nisbatan oson hujum qilinishi sababli axborot xavfsizligi masalasi o'tkir bo'lib turibdi. Shuning uchun WiMAX tizimlarida xavfsizlik masalalari va ularni mumkin yechimlarini aniqlash oldindan birinchi darajada turdi. Wi-Fi tarmoqlarini ishlatishdan tajribalaridan olingan saboqlar IEEE 802.16 standartida hisobga olindi.

Axborot xavfsizligi deganda axborot munosabatlari sub'ektlariga, shu jumladan, axborotlar egalariga va foydalanuvchilarga, qo'llab-quvvatlovchi infratuzilmaga tuzatib bo'lmas zarar yetkazishi mumkin bo'lgan tabiiy yoki sun'iy xarakterdagi o'ylangan va tasodifiy ta'sirlardan axborotlarning va quvvatlovchi infratuzilma himoyalanganligi tushuniladi.

Qanday tarmoqda bo'lsa ham axborot xavfsizligi tizimini rejali tashkil etish uchun xavfsizlik mezonlarini aniqlash zarur. Bu mezonlar risklar va tahdidlar asosida, shuningdek ham tarmoq operatorlari, ham foydalanuvchilarining xavfsizligi talablarini hisobga olib aniqlanadi. Axborot tizimlaridan foydalanishga bog'liq sub'ektlar manfaatlari spektrini umumiy ko'rishda quyidagi toifalarga bo'lish mumkin: yetishlikni (dostupnost) ta'minlash, axborot resurslarining va qo'llab-quvvatlovchi infratuzilmaning butunligi va konfidensialligi.

- Yetishlik bu ma'qul vaqtda talab qilinadigan axborot xizmatini olish imkoniyati.

- Butunlik deganda axborotning aktualligi va zidma-zid emasligi, buzilishdan va sanksiyalanmagan o'zgartirishdan himoyalanganligi tushuniladi.

- Konfidensiallik bu axborotga sanksiyalanmagan ulanishdan himoya.

Xususiy holda tarmoq operatori shunga amin bo'lishni istaydiki, uning tarmog'iga ulangan foydalanuvchilar va qurilmalar, haqiqatan ham, ularni (to'g'ri hujumlarni yoki foydalanuvchilarning almashtirilishini oldini olish uchun); abonentlar ruxsat etilgan o'sha servislarga ulanib olishyapti; ular ishlatgan xizmatga o'rnatilgan haqni to'layaptimi va hokazo. O'z navbatida, foydalanuvchi esa shunga amin bo'lishni istaydiki, uning xususiy axboroti himoyalangan; u qabul qilayotgan va uzatayotgan ma'lumotlarning butunligi buzilmagan; u yozilgan servislarga doimo ulanishni olishi mumkin va hokazo.

Shuningdek, tarmoqning xavfsizligi uchun risklar va tahdidlar tuzilmasini tushunish, xavfsizlik tizimini adekvat shakllantirish va

yangi risklar va tahdidlardan bu tizimni nazorat qilish va koreksiyalash bo'yicha tadbirlarni rejalashtirish uchun tarmoqning zaifligini o'z vaqtida topish juda muhim. Xavfsizlik dasturi va siyosatini ishlab chiqish risklarni tahlil qilishdan boshlanadi, o'z navbatida, uning birinchi bosqichi eng ko'p tarqalgan hujumlar va tahdidlar bilan tanishish hisoblanadi.

4.12.1. IEEE 802.16. standartidagi zaifliklar va hujumlar turlari

Simsiz WiMAX tarmoqlarida tarmoqqa turli hujumlar bo'lishi mumkin va turli zaifliklar aniqlangan bo'lib, ularning quyidagi guruhlarga birlashtirish mumkin [17]:

- Radiosignalni bo'g'ilishi kabi fizik darajadagi hujumlar ulanishni buzilishiga (ingl. *Denial of Service*) yoki kadrlarni ko'chkisimon chaplanishiga (ingl. *Flooding*) olib keladi va AQ akkumulyatorining resursini tugatish maqsadiga ega bo'ladi. Bunday hujumlarga qarshi turish juda qiyin va bugungi kunga kelib bunday hujumlar bilan samarali kurash usullari o'ylab chiqilmagan.

- "Kishi o'rtada" (ingl. *Man In The Middle, MITM*) turidagi hujumlarga kiradigan bazaviy stansiyaning almashtirilishi. Zaiflik telekommunikatsiya tarmoqlari uchun an'anaviy bo'lgan Autentifikatsiya protsedurasining assimetrikligiga bog'liq (ya'ni, BS ni emas abonentni Autentifikatsiyalash bajariladi).

- Mualliflashtirish kalitlarini generatsiyalashning tasodifiy bo'lmagan xarakteri.

- Shifrlash kalitlarining takroran ishlatilishi imkoniyati. Bu hujum shifrlash kalitining indeksini maydonining kichik o'lchamiga asoslangan.

- Shifrlashning kuchsiz algoritmlaridan (DES kabi) foydalanish. Kalit hayotining yetarlicha katta vaqtida va xabarlar intensiv almashtirilganda shifrnı buzish mumkin bo'lib qoladi va xavfsizlikka real tahdid bo'ladi.

4.12.2. IEEE 802.16 standartida xavfsizlik tizimini tashkil etish

Axborot xavfsizligi tizimini tashkil etish masalasini tarmoqning turli darajalarida ko'rib chiqamiz. Tarmoqning xavfsizligi funksiyasi 4.3-jadvalda keltirganidek, turli MVOS modellari darajalariga kiritilishi mumkin [17].

IEEE 802.16e aniqlagan xavfsizlik nimdarajasi faqat kanalli darajada mavjud. Kanalli darajani Autentifikatsiyalash va mualliflashtirish tarmoqqa faqat qonuniy huquqi bor abonentlarga ulanishni ta'minlaydi. Kanalli darajani shifrlash xususiy axborotni butunligini va konfidensialligini ta'minlaydi va trafikni ushlab olinishidan himoya qiladi

Tarmoq darajasi vositalari tarmoq filtrlari (ya'ni, fayrvollar) va AAA-serverlardan foydalanish orqali himoyani ta'minlaydi. AAA funksiyalari uchun eng keng qo'llaniladigan protokol RADIUS protokoli hisoblanadi. WiMAX tarmoq arxitekturasida bu texnologiyalar rouming funksiyasini ishlatish uchun foydalaniladi.

4.3- jadval

OTO' M modelining turli darajalarida xavfsizlik funksiyalari

OTO' M darajasi	Xavfsizlik funksiyalari
Ilovalar darajasi	Raqamli imzolar, raqamli sertifikatlar, «p2p» skvoz shifrlash
Transport darajasi	TLS protokollar
Tarmoq darajasi	IPSec, AAA, RADIUS infratuzilmalar
Kanal darajasi	AES, PKI, X.509
Fizik daraja	WiMAX PHY

Transport darajasi va ilovalar darajasi tarmoq operatori, servis-provayder yoki oxirgi foydalanuvchini o'zining istagiga ko'ra qo'shimcha himoya choralarini ta'minlaydi.

WiMAX tizimi kanalli darajasida va qisqacha tarmoq darajasida bajariladigan xavfsizlik funksiyalarini atroflicha ko'rib chiqamiz.

Kanal darajasida xavfsizlik funksiyalari

Kanalli daraja xavfsizligi algoritmlari AQ va BS orasida IEEE 801.16e interfeysi orqali amalga oshiriladigan muhim Autentifikatsiyalash, mualliflashtirish va shifrlash funksiyalarini bajaradi. Bu funksiyalarni xavfsizlik uyushmasidan (assotsiatsiyasidan) tushunchasini tushuntirishdan boshlab atroflicha ko'rib chiqamiz.

Xavfsizlik uyushmasi

Xavfsizlik uyushmasi - SA (ingl. *Security Association*) WiMAX radio ulanish tarmog'i orqali himoyalangan ulanishni ushlab turish

uchun BS va unga ulangan bir yoki bir necha AQLar orasida ajratilgan himoyalangan axborotlar to'plami sifatida aniqlanadi.

SA xavfsizlik uyushmasi ikki turga bo'linadi:

I. ASA (ingl. *Authorization Security Association*) - mualliflashtirish uchun xavfsizlik uyushmasi.

II. DSA (ingl. *Data Security Association*) – ma'lumotlar uchun xavfsizlik uyushmasi.

I. ASA mualliflashtirish uchun xavfsizlik uyushmasi BS va AQ uchun bir vaqtda ishlatiladi, ya'ni BS va AQni bir ASA ajratib turadi. BS ASAni keyingi DSAni kofiguratsiyalash uchun ishlatadi.

II. DSA ma'lumotlar uchun xavfsizlik uyushmasi uch turga bo'linadi:

- birlamchi DSA (ingl. *Primary DSA*);
- statik DSA (ingl. *Static DSA*);
- dinamik DSA (ingl. *Dynamic DSA*).

Birlamchi DSA AQ ga initsializatsiya protsedurasi vaqtida (ya'ni, birlamchi Autentifikatsiyalash va muallifirishda) o'rnatiladi. Abonent qurilmasi muvaffaqiyatli initsializiyalangandan keyin BS unga statik DSA ni taqdim etadi. Dinamik DSA ma'lumotlar oqimlari uchun zarurat bo'yicha o'rnatiladi va o'chiriladi. Har bir AQ har bir vaqt davrida bir necha ma'lumotlar oqimlariga va mos ravishda bir necha dinamik DSAlarga ega bo'lishi mumkin. AQni mualliflashtirishda bazaviy stansiya mos DSAlar so'raladigan servislar turlari bilan mosligiga ishonadi.

Autentifikatsiyalash

Autentifikatsiya axborotni jo'natuvchi va oluvchining shaxsini tasdiqlash vositasi sifatida xizmat qiladi. IEEE 802.16e standartida PKM (ingl. *Privacy and Key Management*) kalitlarni boshqarish va konfidensialligi protokoli qo'llangan. U quyidagi uchta turdagi autentifikatsiyani qo'llaydi:

- RSA (yaratuvchilarning inglizcha familiyalaridan *Rivest, Shamir i Adleman*) ochiq kalitli kriptografik algoritmiga asoslangan autentifikatsiya, raqamli sertifikatlarni, X.509 protokolni va bevosita RSA- shifrlashni ishlatadi;

- kengaytiriladigan EAP (ingl. *Extensible Authentication Protocol*) protokolga asoslangan autentifikatsiya. Opsional qo'llaniladi:

- EAP protokoli qo'llanilganidan keyin RSA algoritmi ishlatilishiga asoslangan autentifikatsiya.

PKM protokoli mualliflashtirish kaliti (MK) deyiladigan umumiy kalitni BS va AQ orasiga o‘rnatadi. BS va AQ orasida umumiy MK o‘rnatilishi bilanoq, kalitlarni shifrlash kaliti (KShK) foydalanishdan chiqariladi va trafikni shifrlash kalitlarini (TShK) keyingi almashtirilishida shifrlash uchun qo‘llaniladi. Autentifikatsiya ochiq kalitlarni almashtirish protokolidan foydalanish yo‘li bilan ishlatiladi, bunda faqat autentifikatsiya emas, shifrlash kalitlarini yaratish ham ta‘minlanadi. Ochiq kalitlarni almashtirish sxemalarida har bir qatnashuvchi ochiq va xususiy (yopiq) kalitlarga ega bo‘lishi kerak. Ochiq kalit barchaga ma‘lum, xususiy kalit esa maxfiy saqlanadi.

RSA algoritmgiga asoslangan autentifikatsiyada BS AQni uni ishlab chiqaruvchisi yaratgan X.509 protokoli ulkan raqamli sertifikat bo‘yicha autentifikatsiyalaydi. Bu sertifikat AQ ochiq kaliti va uning MAS-manzilidan tashkil topgan. MKga zarurat bo‘lganda AQ o‘z raqamli sertifikatini BS ga yuboradi, BS sertifikatni tekshiradi va haqiqiyliги tasdiqlansa, MK ni shifrlash uchun tekshirilgan ochiq kalitni qayta AQga uzatadi. RSA-autentifikatsiyadan foydalanadigan barcha bazaviy stansiyalar zavodda o‘rnatilgan xususiy/ochiq kalitlar juftligiga (yoki bu kalitlarni dinamik generatsiyalash uchun algoritmgaga) va X.509 raqamli sertifikatga ega bo‘ladi.

EAP protokoliga asoslangan autentifikatsiyadan foydalanishda AQ operator ulkan faktori (omili), masalan SIM-karta orqali yoki yuqorida bayon etilganidek, X.509 raqamli sertifikat orqali autentifikatsiyalanadi. EAP autentifikatsiyalash protokoli simsiz tarmoq infratuzilmasi elementlarini va foydalanuvchilarini shifrlash kalitlarini dinamik generatsiyalash imkoniyatili markazlashtirilgan autentifikatsiyani qo‘llaydi.

Autentifikatsiyalashtirish usulini tanlash quyidagi tarzda operator tomonidan EAP protokolini tanlashga bog‘liq:

- EAP-AKA (ingl. *Authentication and Key Agreement*) – kalitlarni autentifikatsiyalash va moslashtirish, SIM-kartalardan foydalanishga asoslangan;

- EAP-TLS (ingl. *Transport Layer Security*) – transport darajasidagi xavfsizlik, X.509 raqamli sertifikatlari asosida autentifikatsiyalash uchun foydalaniladi;

- EAP-TTLS (ingl. *Tunneled Transport Layer Security*) – transport darajasidagi tunellashtirilishli xavfsizlik, MS-CHAPv2 (ingl. *Microsoft-Challenge Handshake Authentication Protocol*) protokolidan foydalanishga asoslangan.

Keyin BS mos abonentga (va AQga) xizmatlarni qo‘yadi va mos ravishda abonentga ruxsat etilgan xizmatlar ro‘yxatini aniqlaydi. Shunday qilib, KA orqali almashtirish bilan BS abonentni va uning uchun ruxsat etilgan xizmatlarni identifikatsiyalaydi.

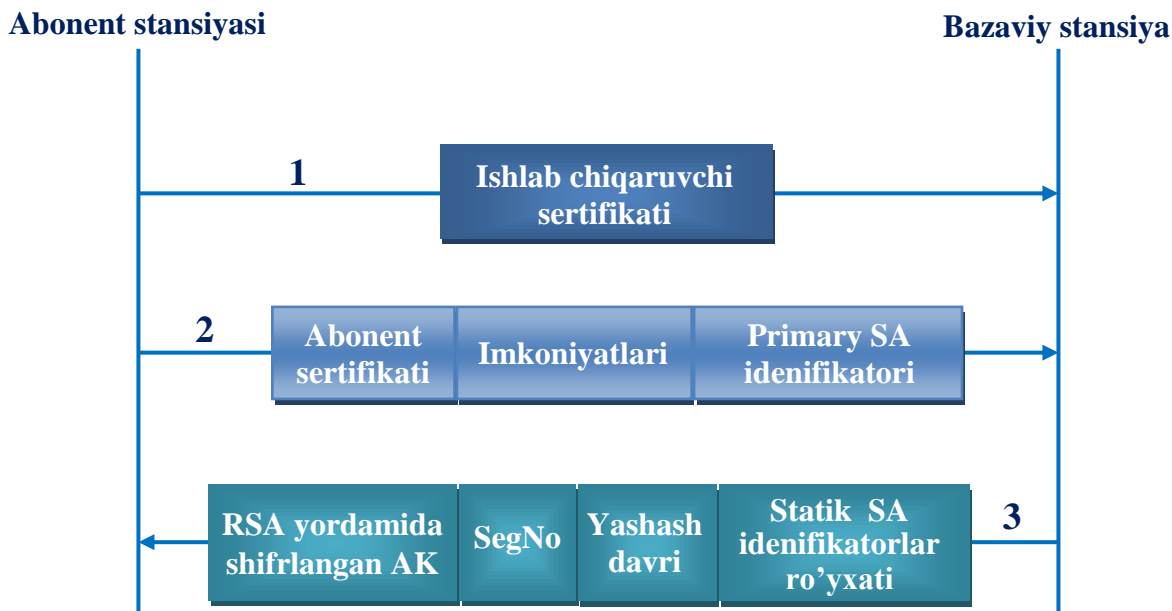
Autentifikatsiyalash ikki turda mavjud:

- bir tomonlama autentifikatsiya, bunda BS faqat AQni autentifikatsiyalaydi;
- ikki tomonlama autentifikatsiya, ham BS, ham AQ bir-birlarini autentifikatsiyalaydi.

WiMAX tizimlari uchun majburiy talab bir tomonlama autentifikatsiyani ishlatish hisoblanadi. Lekin, bunda tajribalar shuni ko‘rsatdiki, ikki tomonlama autentifikatsiya tarmoq xavfsizligi darajasini sezilarli oshiradi.

Mualliflashtirish

Autentifikatsiyalash bosqichidan keyin mualliflashtirish bosqichi boshlanadi. AQ bazaviy stansiyaga mualliflashtirishga so‘rov (ingl. *Authorisation Request*) jo‘natadi. U MK mualliflashtirish kaliti yoki SAID (ingl. *SA Identification*) xavfsizlik uyushmasini identifikatsiyalashga so‘rov bo‘lishi mumkin (4.30-rasm).



4.30- rasm. IEEE 802.16 standartidagi mualliflashtirish protsedurasi

1. AQ uni ishlab chiqaruvchining X.509-sertifikatiga ega so‘rovni jo‘natadi. Odatda bu sertifikat faqat ishonchli ishlab

chiqaruvchilar AQLarini mualliflashtirish uchun BS ni sozlash mumkin bo'lsada, u hech qanaqasiga ishlatilmayapti.

2. Birinchi xabardan keyin, AQ o'zining X.509-sertifikati, uning kriptografik imkoniyatlari va birlamchi DSA indikatoridan tashkil topgan xabarni jo'natadi.

BS AQning sertifikati bo'yicha mos servislarni taqdim etish uchun mualliflashtirilganligini aniqlaydi (AAA serverni so'rash bilan). Musbat natija bo'lganida BS AQga mualliflashtirish javobini (ingl. *Authorization Reply*) yuboradi. Bu javob shifrlangan MK, bu MK ning ketma-ket nomeri (ingl. *SeqNo*), uning hayot vaqti, shuningdek, abonent mualliflashtirilgan statik DSA (SAID) identifikatorlar ro'yxatidan tashkil topadi.

Binobarin, birinchi mualliflashtirish protsedurasidan keyin AAA-server BS orqali davriy ravishda AQni takroriy mualliflashtirish protsedurasini o'tkazadi.

Autentifikatsiyalash va mualliflashtirish jarayonlari uzunligi 160 bitga teng bo'lgan MK mualliflashtirish kalitidan foydalanadi.

Kalitni shifrlash kaliti (KShK) bevosita MKdan shakllantiriladi, uning uzunligi 128 bitni tashkil etadi va u faqat MKni shifrlangan uzatish uchun foydalaniladi. Trafikni shifrlash uchun trafikni shifrlash kaliti (TShK) talab qilinadi, u shifrlash kaliti sifatida KShK ishlatiladigan TShKni shifrlash algoritmidan foydalanishli tasodifiy ketma-ketlik sifatida BSga generatsiyalanadi.

Trafikni shifrlash

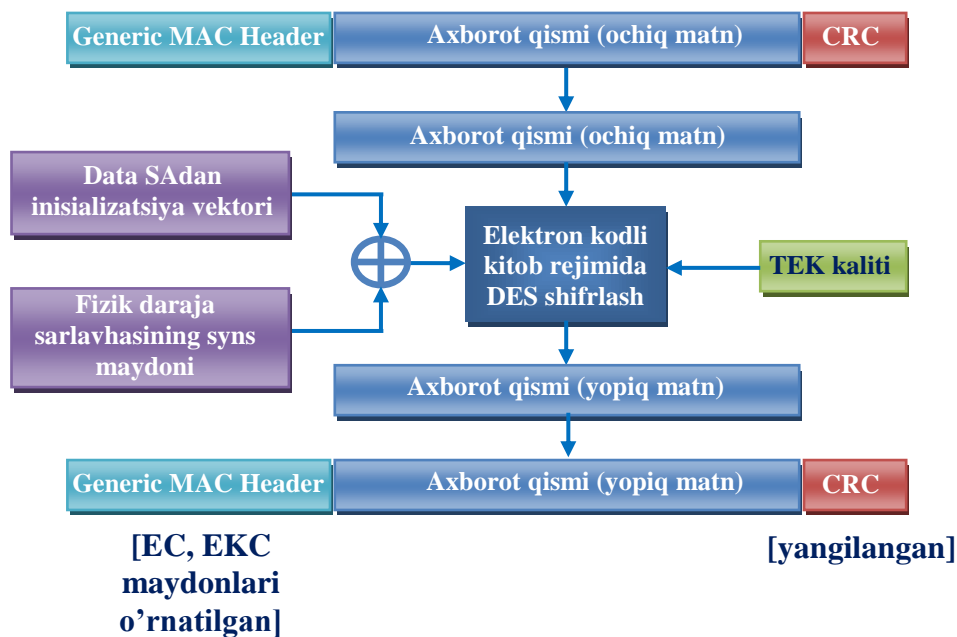
Trafikni shifrlash uchun IEEE 802.16 standarti ma'lumotlar blokli shifrlar bloki ulanish rejimida DES algoritmidan foydalanadi. Lekin ta'kidlaymizki, hozirgi vaqtda DES algoritmi yetarli xavfsiz hisoblanmaydi va shuning uchun IEEE 802.16e standartiga AES algoritmi qo'shilgan. Bu algoritmlarni atroflicha ko'rib chiqamiz.

DES shifrlash algoritmi

DES (ingl. *Data Encryption Standard*) – IBM kompaniyasi tomonidan ishlab chiqilgan va AQSh hukumati tomonidan 1977 yilda rasmiy standart (FIPS 46-3) sifatida tasdiqlangan blok shifrlash simmetrik algoritmi. DES algoritmi 64 bitdan bitdan bloklarni va Feystel tarmog'ining 16-siklli tuzilmasidan foydalanadi. Shifrlash uchun 56 bit uzunlikdagi kalit ishlatiladi. Agar xabarning hajmi 64 bitdan ortiq bo'lsa (odatda bo'lib turadi), unda u 64 bitdan bloklarga bo'linadi, keyin esa ma'lum tarzda birlashtiriladi. Bunday birlashtirish quyidagi to'rtta usullardan biri orqali amalga oshiriladi:

- Elektron kodli kitob usuli (ingl. *Electronic Code Book, ECB*);
- Shifrlar blokining ulanish usuli (ingl. *Cipher Block Chaining, CBC*);
- x -bitli shifrlangan teskari aloqa usuli (ingl. *Cipher FeedBack, CFB-x*);
- chiqish teskari aloqa usuli (ingl. *Output FeedBack, OFB*).

DESda ma'lumotlarni shifrlash protsedurasini quyidagi tarzda bo'lib o'tadi (4.31- rasm).



4.31- rasm. DES da ma'lumotlarni shifrlash protsedurasini

DSA xavfsizlik uyushmasidan initsializatsiyalash vektori (ingl. *Initialization Vector, IV*) va PHY-kadr sarlavhasining sinxronlashtirish maydoni 2 modul bo'yicha (inkor qiluvchi "YoKI" operatsiyasi (ingl. *XOR*)) bitlab qo'shiladi va SVS shifrlar bloki ulanish rejimida DES algoritmini initsializatsiyalash uchun uzatiladi. Shuningdek, DES sxemasi kirishiga TShK kalit (ingl. *TEK*) va xabarning ochiq matni beriladi. Bunda MAC-daraja sarlavhasida (ingl. *Generic MAC Header, GMH*) ES maydonda (ingl. *Encryption Control*) bir o'rnatiladi, chunki ma'lumotlar shifrlangan, ikki bitli EKS (ingl. *Encryption Key Sequence*) maydonda esa bunda foydalanilgan TShK kalit turadi. CRC kadri tugaganidan keyin, agar u bo'lsa, shifrlangan matn ostida o'zgaradi.

AES shifrlash algoritmi

AES (ingl. *Advanced Encryption Standard*) – 128 bit o‘lchamli bloklar va 128/192/256 bit uzunlikdagi kalitlardan foydalanadigan, shuningdek, Reyndal (*Rijndael*) algoritmi sifatida ma’lum bo‘lgan blokli shifrlashning simmetrik algoritmi [1]. AES algoritmi yaxshi testlangan va hozirgi vaqtda simmetrik shifrlashning eng keng tarqalgan algoritmlaridan biri hisoblanadi. Misol uchun, algoritm AQSh hukumati tomonidan shifrlash standarti sifatida qabul qilingan va Intel kompaniyasi tomonidan Intel® Core™ protsessorlar oilasiga kiritilgan.

802.16e standarti quyidagi to‘rtta usullardan biri qo‘llaniladigan AES algoritmidan foydalanishni aniqlaydi:

- shifrlar blokining ulanish usuli – CBC;
- hisoblagichning shifrlash usuli (ingl. *Counter Encryption, CTR*);
- CCM (ingl. *Counter Encryption with Cipher Block Chaining message authentication code*) shifrlar blokining ulanish usuli orqali olingan Autentifikatsiya kodi bilan hisoblagichning shifrlash usuli. CTR usulidan farqli ravishda bu yerda shifrlangan xabarning haqiqiylikini tekshirish imkoniyati mavjud.

- TShK trafikning kalitlarini shifrlash uchun foydalaniladigan ECB elektron kodli kitob usuli.

Takomillashtirilganroq sifatida SSM usuli qo‘llaniladigan AES rejimini ko‘rib chiqamiz. Shifrlash protsedurasi bir necha bosqichlarda bo‘lib o‘tadi. Foydali axborotni shifrlash uchun dastlab uzatuvchi stansiya har bir paketga 12-baytli *Nonce* ketma-ketligini generatsiyalaydi (4.32-rasm).

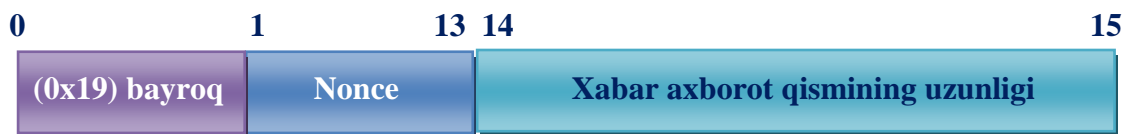


4.32- rasm. Nonce ketma-ketligi

Nonce ketma-ketligining birinchi 5 ta bayti GMH kadrining boshlanishi hisoblanadi. Keyin nolli qiymatlarga ega bo‘lgan 4 ta zaxiralangan bayt keladi. Keyin bu DSA xavfsizlik uyushmasida PN paketning 4 baytli nomeri (ingl. *Packet Number*) keladi. PN qiymat yangi DSA yoki yangi TShK o‘rnatilganda 1 ga teng qo‘yiladi.

Keyin *Nonce* ketma-ketligi qo‘llanilib, CBC va CTR bloklar shakllantiriladi. CBC bloki 0001100 qiymatga ega bo‘lgan bir baytli

bayroqchaga, *Nonce* ketma-ketligiga va xabarning axborot qismining uzunligini ko'rsatadigan maydondan tashkil topgan (4.33- rasm).



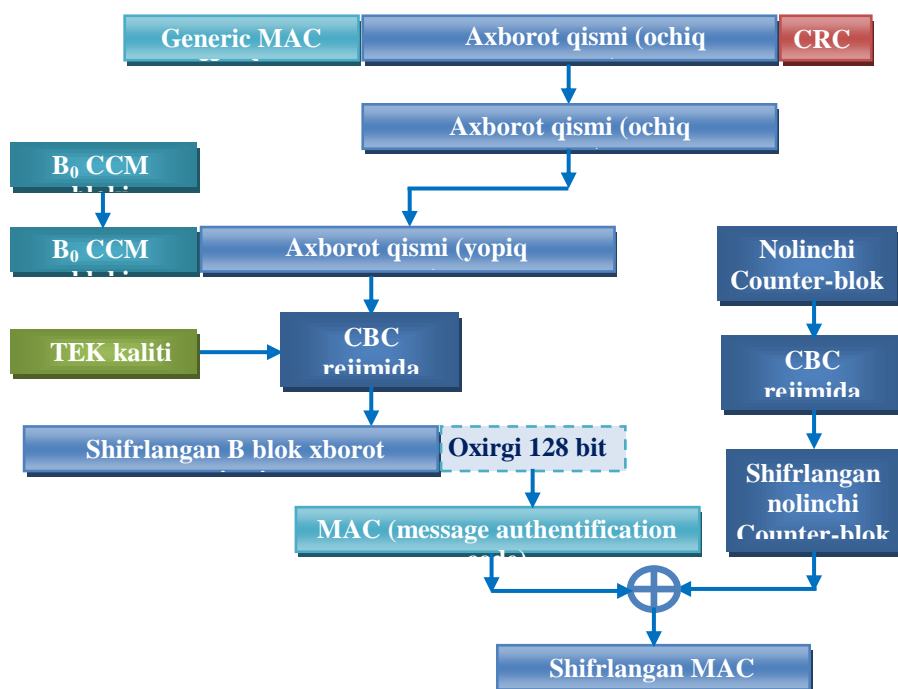
4.33- rasm. CBC bloki

CTR bloki 0000001 qiymatga ega bo'lgan bir baytli bayroqchaga, *Nonce* ketma-ketligiga va CTR blokning *i* nomeridan iborat maydondan tashkil topgan (4.34- rasm).



4.34- rasm. CBR bloki

Keyin MAS-kod yaratiladi, buning uchun xabarning axborot qismi boshlanishiga *IV* initsializatsiyalash vektori o'rniga boshlang'ich (nolinchi) SVS blok qo'yiladigan modifikatsiyalangan SVS usulidan foydalaniladi (4.35-rasm).

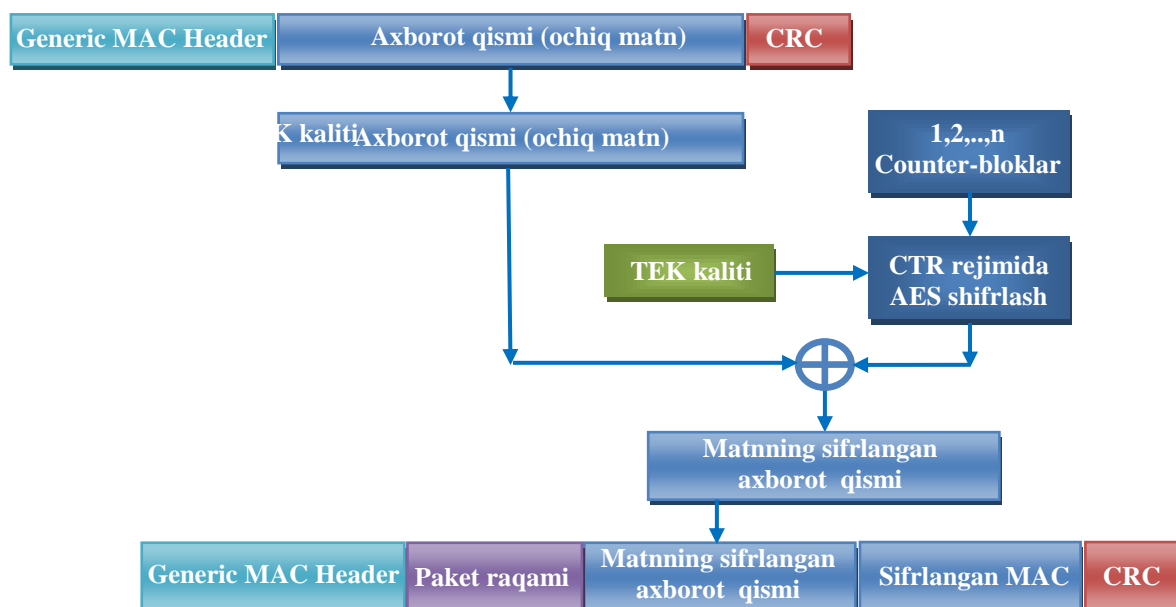


4.35- rasm. AES - CCM rejimida MAS-kod yaratish va shifrlash

Keyin bu juftlik SVS usuli va TShK kaliti qo‘llaniladigan AES algoritmi bilan shifrlanadi. Shifrlangan matnning oxirgi 128 biti MAS-kod sifatida olinadi. Keyin MAS-kod AES-CTR rejimda shifrlangan boshlang‘ich (nolinchi) CTR blok bilan (yoki Counter-blok bilan) “XOR” qo‘shishga olib kelinadi.

Yakunda qolgan CTR bloklardan har bir n bloklar (nolinchi MAS-kodni shifrlashda ishlatilgan) TShK kalit qo‘llaniladigan AES-CTR rejimda shifrlanadi. Keyin natija xabarning axborot qismidan “XOR” operatsiyada qo‘shiladi (4.36-rasm).

Shifrlangan MAS-kodli, ma‘lumotlar paketi nomerili, GMH sarlavhali va CRC nazorat yig‘indili shifrlangan matn PHY fizik darajaga jo‘natiladi. Bunda DESdagi kabi GMH sarlavhada ES maydonda 1 o‘rnatiladi, EKS maydonda esa foydalanilgan TShK kalitning (ingl. *TEK*) indeksi ko‘rsatiladi.



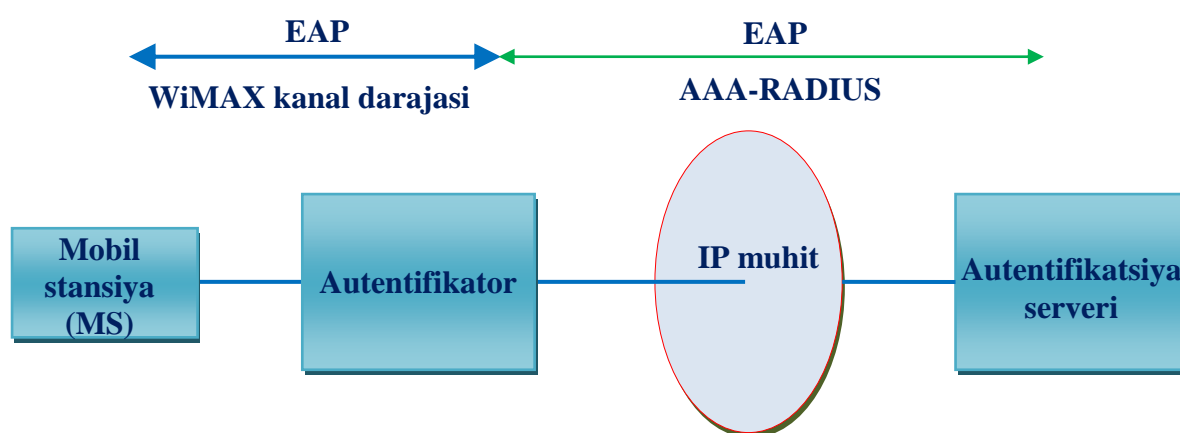
4.36- rasm. Xabarni axborot qismini shifrlash

Xavfsizlikning tarmoq jihatlari

Tarmoq darajasida bo‘lib o‘tadigan xavfsizlik funksiyalarini ko‘rib chiqamiz. 4.37-rasmda ulanishni nazorat qilishning arxitekturasi keltirilgan

EAP kengaytirilgan autentifikatsiyalash protokoli oxirgi foydalanuvchi va Autentifikator orasida murakkab autentifikatsiya protokollarini almashtirishga imkon beradigan ixcham karkas hisoblanadi. WiMAX (IEEE 802.16e) tizimlarida BS va AQ orasida EAP protokol PKMv2 protokolidan foydalanish bilan PHY va MAC

darajalarning ustida ishlaydi. Agar autentifikatsiyalash funksiyasi BSning o‘zida ko‘zda tutilmagan bo‘lsa, unda BS autentifikatsiyalash protokolini Autentifikatorga (ASN-shlyuzga) qayta yuboradi. Autentifikator EAP protokoli RADIUS protokoli bo‘yicha autentifikatsiyalash serveriga uzatiladi. RADIUS protokoli keng foydalaniladigan standart hisoblanadi, «klient-server» arxitekturaga ega va UDP protokoldan foydalanadi. Shunday qilib, autentifikatsiyalash serveri RADIUS-server hisoblanadi, Autentifikator esa RADIUS-klient rolini bajaradi. Autentifikatsiyalashga qo‘shimcha ravishda RADIUS-server mualliflashtirish va hisobga olish funksiyalarini qo‘llab-quvvatlaydi.



4.37- rasm. Ulanishni nazorat qilishning arxitekturasi

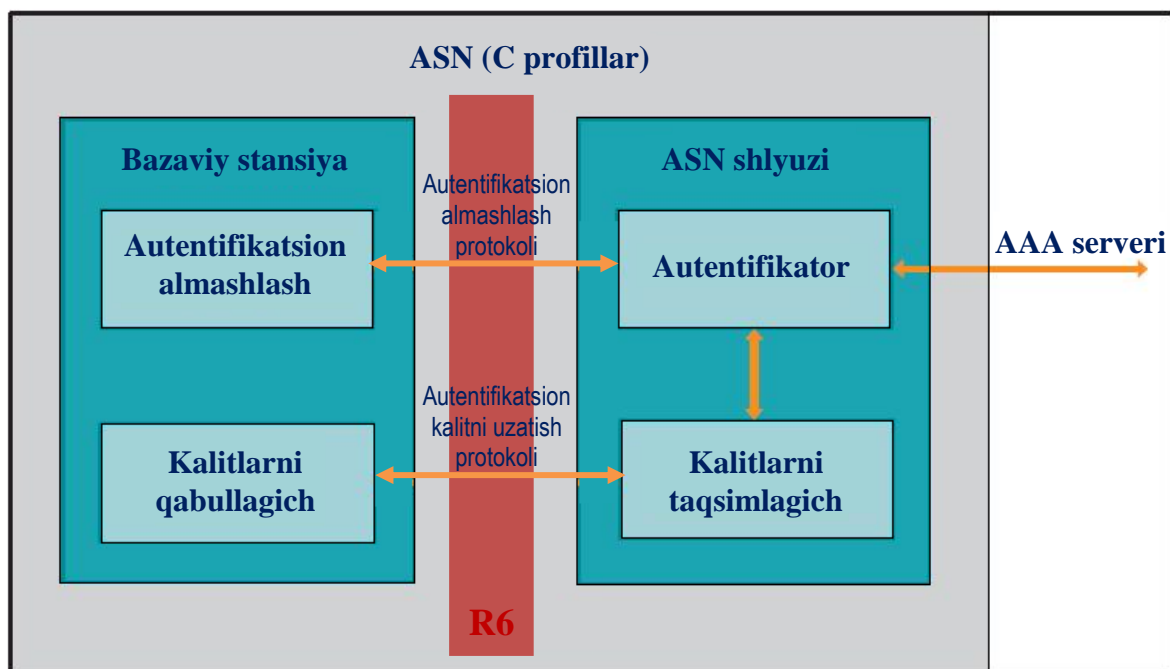
ASN profillari i xavfsizlik

NWG tarmog‘ini tashkil etish bo‘yicha ishchi guruh tomonidan mos ravishda *A*, *B* va *S* deyiladigan ASN ulanish tarmog‘ining uchta profili aniqlandi. Qurilmalar ishlab chiqaruvchilari va xizmatlar provayderlari bu profillardan birini tanlashi mumkin. *A* va *S* profillar markazlashtirilgan ASN-shlyuzlardan foydalanadi, bunda *S* profilda bazaviy stansiyalar RRM radioresurslarni boshqarish va «xendover» funksiyalarini ishlatilishiga bevosita javobgar hisoblanadi. *B* profil bazaviy stansiyalar darajasida ASN tarmog‘ining kalit funksionalligini bajaradi, bu markazlashtirilgan ASN-shlyuzning zaruratini olib tashlaydi. Shuningdek, ta’kidlaymizki, so‘ngi vaqtlarda faqat *V* va *S* profillarni qo‘llash bilan *A* profildan foydalanish ko‘pincha inkor qilinmoqda.

S profil qo‘llaniladigan xavfsizlik funksiyalarini bajarilishini ko‘rib chiqamiz.

4.4- jadvalda S profil ishlatilganda BS va ASN-shlyuz orasida ASN tarmog‘i funksiyalarining (xavfsizlik funksiyasi qo‘shilganda) bo‘linishi keltirilgan.

S profil uchun ASN tarmog‘i xavfsizligi arxitekturasi 4.38-rasmida ko‘rsatilganidek, bazaviy stansiya va ASN-shlyuz orasida R6 tayanch nuqtasi orqali o‘zaro ta’sirlashishga asoslangan.



4.38- rasm. S profili uchun ASN tarmog‘i xavfsizligi arxitekturasi

4.4- jadval

S profil ishlatilganda ASN tarmog‘i funksiyalarining bo‘linishi

Toifa	Funksiya	ASN tarmog‘i – C profili	
		BS	ASN-shlyuz
Xavfsizlik	Autentifikator		+
	Autentifikatsiyani kechiktirish	+	
	Kalitlar taqsimlagichi		+
	Kalitlar oluvchisi	+	
Foydalanuvchi bazaviy stansiyalar	Ma’lumotlar yo‘llari funksiyasi	+	+

orasida harakatlanganida boshqarish, «xendover»	Harakatda nazorat qilish	+	
	Kontekst serveri va klienti	+	+
	Begona Mobile IP agenti		+
Radioresurslarni boshqarish	Radioresurslar kontrolleri	+	
	Radioresurslar agenti	+	
Peydjing	Peydjing kontrolleri	+	
	Peydjing agenti		+
Xizmat ko'rsatish sifati	SF-mualliflashtirish		+
	SF-menejer	+	

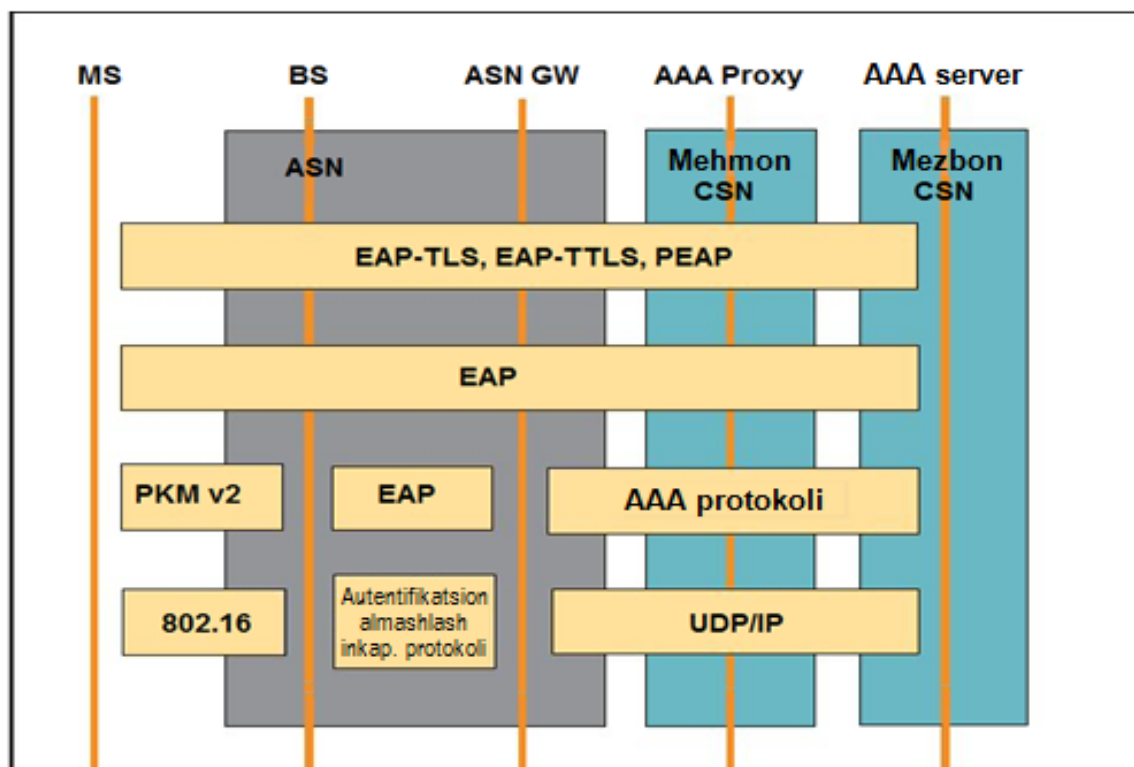
Yuqorida bayon etilganidek, CSN kommutatsiya tarmog'i WiMAX tarmog'i yadrosi hisoblanadi va ASN tarmog'ini boshqaradi va AAA, DHCP-server va boshqa funksiyalarni bajaradi. CSN shuningdek, boshqa operatorlar tarmoqlari bilan ulanishga, shuningdek, operator tarmog'i ichida va turli operatorlar tarmoqlari orasida roumingni ta'minlashga javobgar.

4.39-rasmda WiMAX tarmog'ida AAA funksiyalarni bajarilishi uchun protokollar steki keltirilgan. EAP protokoli R1/R3/R5 tayanch nuqtalari ustida, AKA i TLS/TTLS kabi EAP protokollari esa R2 tayanch nuqtasi ustida ishlaydi.

Ham AQni, ham foydalanuvchining o'zini autentifikatsiyalash talab qilingan hollarda va bunda autentifikatsiya AAA-serverga bog'langan bo'lsa, bir necha PKMv2 usullari o'zaro autentifikatsiyalashdan mustaqil ravishda EAP-TTLS dan foydalanadi. Ikkilangan autentifikatsiyada oldin AQ autentifikatsiyalanadi, keyin foydalanuvchini EAP-autentifikatsiyalash bo'lib o'tadi, undan keyin AQ IP-xizmatlarga ulanishni oladi. EAP-TTLS autentifikatsiyada ikkilangan autentifikatsiya mos AAA-serverga tunnellashtirishsiz bo'lib o'tadi (har ikkala holda o'sha bir AAA-serverdan foydalaniladi), buning natijasida autentifikatsiya jarayoni tezlashadi.

Servis oqimlarga qo‘llaniladigan boshqarish va mualliflashtirish funksiyalari

SFM (ingl. *Service Flow Management*) servis oqimlarni boshqarish va SFA (ingl. *Service Flow Authorisation*) servis oqimlarni mualliflashtirish bu QoS xizmat ko‘rsatish sifati bog‘liq va ASN tarmog‘ida joylashgan mantiqiy funksiyalardir. ASN tarmog‘ining S profili BSda SFM funksiyani, SFM funksiya esa ASN-shlyuzda bajarilishini reglamentlaydi.



4.39- rasm. WiMAX tizimida AAA uchun protokollar steki

SFM tuguni IEEE 802.16e standarti servis oqimlarini yaratish, ulanish, aktivlashtirish, modifikatsiyalash va o‘chirishga javobgar. U AC (ingl. *Admission Control*) ulanishni nazorat qilish funksiyasi, ma‘lumotlar yo‘llari funksiyalari va uyushtirilgan lokal resurslar haqida axborotlardan iborat.

SFM tuguni abonent QoS profiliga nisbatan istalgan servis so‘rovlarini baholashga javobgar. Agar abonent QoS profili mavjud bo‘lsa, SFA ularga baholash uchun foydalaniladi. Agar abonent QoS profili mavjud bo‘lmasa, u holda SFA qaror qabul qilish uchun siyosat funksiyasiga (ingl. *Policy Function, PF*) so‘rov jo‘natadi. Siyosat funksiyasi WIMAX tarmog‘i taqdim etadigan turli xizmatlar uchun

ilovalarning bajarilishi ssenariylaridan iborat ma'lumotlar bazasi hisoblanadi. Siyosat funksiyasi va unga mos baza CSN da ham uy tarmog'i, ham mehmon tarmog'i uchun qo'llab-quvvatlanadi.

WiMAX tarmoqlarida axborot xavfsizligi masalalariga bag'ishlangan nimsarlavhaga yakun yasab, yagona 4.5-jadvalga IEEE 802.16 standartida foydalaniladigan axborot xavfsizligi bo'yicha qo'yiladigan talablarni qoniqtirish uchun usullarni kiritamiz.

Ta'kidlaymizki, WiMAX katta imkoniyatlarni, yuqori aloqa sifatini va xavfsiz ulanishni taqdim etishga qodir simsiz keng polosali ulanishning to'laqonli vakili hisoblanadi. Bularning barchasi bu standartning keyingi rivojlanishini va uning amalda keng tarqalishini ko'zda tutishga asos bo'ladi.

4.5- jadval

IEEE802.16. standartida xavfsizlik talablarini ta'minlash

Ishtirokchi	Xavfsizlik aspekti	Sharhlar	WiMAX tizimida qo'llanilgan usul
Tarmoq abONENTI	Xususiy ma'lumotlarning daxlsizligi	“Eshitishga” hujumdan himoya	RSA, EAP-TLS shifrlash, PKM protokol
	Ma'lumotlarning butunligi	Uzatish jarayonida ma'lumotlarni almashtirishdan himoya	RSA, EAP-TLS shifrlash, PKM protokol
	Etishlik	Abonent aniq huquqlarga ega	X.509, EAP
	Ko'rsatilgan xizmatlarga to'g'ri hisob	Aniq va samarali qayd etish	AAA-funksiyalar arxitekturasi
Tarmoq operatori	Foydalanuvchilarni autentifikatsiyalash	Abonentning haqiqiylikini tekshirish	X.509, EAP-TTLS
	Qurilmani autentifikatsiyalash	AQning haqiqiylikini tekshirish	X.509, EAP-TTLS

	Mualliflashtirish	Servislarni olish uchun abonengtlarni obuna qilish	RSA,EAP shifrlash, PKMv2 protokol
	Ulanishni nazorat qilish	Faqat mualliflashtirilgan abonentlarga ulanishni taqdim etish	RSA, EAP shifrlash, PKMv2 protokol

Nazorat savollari

1. Simsiz tarmoqlar xavfsizligiga tahdidlarni sanang.
2. Simsiz tarmoqlarda signalli darajadagi tahdidlarning turlari va manbalarinitushuntiring
3. Simsiz tarmoqlarda axborotli darajadagi tahdidlarning turlari va manbalarinitushuntiring
4. Xavfsizlikka tahdidlar turlarining tahlil qilish nimadan iborat?
5. WEP shifrlash mexanizmi nima uchun ishlatiladi?
6. WEP-protokolning o'ziga xos xususiyatlarini tushuntiring.
7. Oqimli shifrlash va inisializatsiya vektori nima uchun ishlatiladi?
8. WPA spesifikatsiyasini tushuntiring
9. 802.1x: ishlash prinsipini tushuntiring
10. Axborot xavfsizligi sohasidagi asosiy xarakteristikalarini tushuntiring

5- BOB. NFC TEXNOLOGIYALARINING QO'LLANILISHI ISTIQBOLLARI

5.1. NFC texnologiyasi spetsifikatsiyasi

Near Field Communication, NFC («yaqin maydon kommunikatsiyasi») - 10-20 santimetrlar (4-8 dyuymlar atrofida) masofalarda joylashgan qurilmalar orasida ma'lumotlarni almashtirish imkoniyatini beradigan kichik ishlash radiusili simsiz yuqori chastotali aloqa texnologiyasi hisoblanadi. Bu texnologiya – smart karta va o'qish qurilmasi interfeyslarini yagona qurilmaga birlashtiradigan kontaktsiz kartalar standartining (ISO 14443) oddiy kengaytirilishi hisoblanadi [23].

ISO 14443 standarti amplitudaviy modulyatsiyali va magnit bog'langan induktivliklardagi 850 kGs deviasiyasili bo'sh (litsenziyalanmagan) 13,56 MGs chastotalar diapazonidan foydalanishni aniqlaydi. Kartalar va o'qish qurilmalaridan o'qishning uzq masofaliligi 5-15 sm. Almashtirish tezligi 106 dan 848 kbit/s gachani tashkil etadi [23].

NFC qurilmasi ISO 14443 standartining mavjud smartkalari va o'qish qurilmalari va boshqa NFC qurilmalar bilan aloqa qilishi mumkin va shunday qilib jamoat transportida va to'lov tizimlaridagi mavjud ishlatilayotgan kontaktsiz kartalar mavjud infratuzilmalari bilan moslashadi. NFC, avvalo mobil telefonlarda foydalanish maqsadiga yo'naltirilgan.

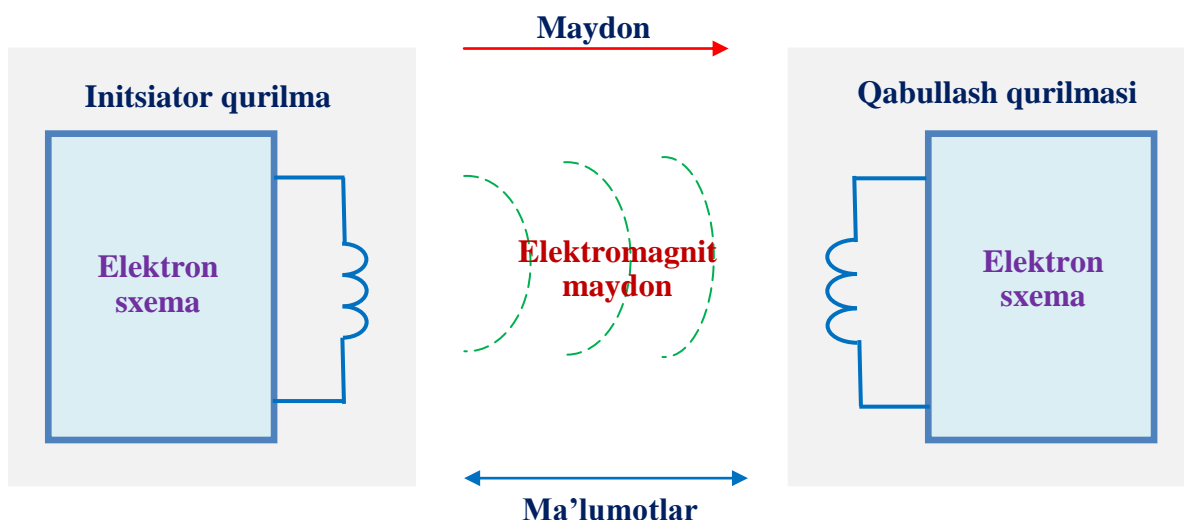
ISO 14443 standartidagi kabi NFC da aloqa magnit maydon induksiyasi orqali amlga oshiriladi, bu yerda ikkita ramkali antennalar havo o'zagili transformatorni samarali shakllantirishi bilan birbirlariga yaqin maydonlar chegaralariga joylashtiriladi. Bu standart umumiy mumkin bo'lgan va litsenziyalanmagan, deyarli 2 MGs o'tkazish polosasi kengligi 13,56 MGs atrofidagi ISM band (ingl. Industrial, Scientific and Medical radio Bands – sanoat, ilmiy va meditsina radiochastotalari) radiochastotalar chegaralarida ishlaydi.

Ishchi masofasi: 20 sm gacha.

106, 212 yoki 424 kbod ma'lumotlarni uzatish tezliklarida ishlaydi.

NFC asosida induktiv aloqa yotadi (5.1-rasm). Ishlash chastotasi 13,56 MGs ni, uzatish tezligi 106 kbit/s ni (212 kbit/s va 424 kbit/s bo'lishi mumkin) tashkil etadi. Signal turli 100% yoki 10% foizlik

chuqurikli ASK (Amplitude Shift Keying) amplitudaviy manipulyasiyalanadi yoki BPSK fazaviy manipulyasiyalanadi.



5.1- rasm. NFC ning ishlash prinsipi

Ma'lumotlarni uzatish uchun NFC ikkita turli kodlashtirishni ishlatadi. Agar aktiv qurilma ma'lumotlarni 106 kbod tezlikda uzatsa, u holda 100 % modulyatsiyali modifikatsiyalangan Miller coding ishlatiladi. Qolgan barcha hollarda 10 % modulyatsiya koeffitsientili Manchester coding ishlatiladi.

NFC qurilmasi bir vaqtda ma'lumotlarni uzatish va qabul qilish holatida bo'ladi. Shunday qilib, ular radiochastotali maydonni nazorat qilishi va agar olingan signal uzatilgan signalga mos kelmaslik zidligini aniqlashi (5.1- jadval) mumkin [24].

5.1- jadval

NFCning ish rejimlari

Tezlik	Aktiv qurilma	Passiv qurilma
424 kbod	Manchester, 10 % ASK	Manchester, 10 % ASK
212 kbod	Manchester, 10 % ASK	Manchester, 10 % ASK
106 kbod	Modified Miller, 100 % ASK	Manchester, 10 % ASK

5.2. NFC texnologiyasini standartlashtirish va sanoat loyihalari

Standartlar. NFC 2003 yilning 8 dekabrda ISO/IEC standarti sifatida va keyin ECMA standarti sifatida ma'qullangan [23], [24].

NFC ECMA-340 va ISO/IEC 18092 ga standartlashtirilgan ochiq platformali texnologiya hisoblanadi. Bu standartlar modulyatsiyalash sxemalarini, kodlashni, uzatish tezligini va NFC qurilmalarining interfeyslari radiochastotali tuzilmasini, shuningdek NFC ning ham passiv, ham aktiv rejimlari uchun initsializatsiya vaqtida bahsli vaziyatlarni nazorat qilish uchun talab qilinadigan initsializatsiya sxemalari va shartlarini aniqlaydi. Bundan tashqari, ular aktivlashtirish protokoli va ma'lumotlarni almashtirish usullarini qo'shganda uzatish protokolini aniqlaydi.

NFC uchun radiointerfeys standartlashtirilgan:

- ISO/IEC 18092 / ECMA-340: Near Field Communication Interface and Protocol-1 (NFCIP-1).

- ISO/IEC 21481 / ECMA-352: Near Field Communication Interface and Protocol-2 (NFCIP-2).

NFC ISO 14443, ISO 15693 larni qo'shganda ko'plab oldingi mavjud standartlarni birlashtiradi. Shunday qilib, NFC bilan jihozlangan telefonlar o'qish qurilmalarining oldingi mavjud tuzilmalari bilan o'zaro ta'sirlasha oladi. Ayniqsa, "kartani emulyatsiyalash rejimida" NFC qurilmasi kamida oldin mavjud bo'lgan o'qish qurilmasiga unikal identifikatsion nomerni uzatishi kerak.

Bundan tashqari, NFC Forum NDEF deyiladigan ma'lumotlarning umumiy formatini aniqladi. U istalgan MIME-typed ob'ekti chegaralaridan URL kabi ultra qisqa RTD-hujjatlarga ma'lumotlarning turli elementlarini saqlash va uzatish uchun ishlatilishi mumkin.

NDEF konseptual jihatdan MIME ga juda ham o'xshaydi. Bu "yozuvlar" deyiladigan ikkilik format hisblanadi, ularda har bir yozuv ob'ektning turli sinflarini saqlashi mumkin. Kelishuvga muvofiq birinchi hisobot turi butun xabarning kontekstini aniqlaydi.

NFC Forum. NFC Forum maishiy elektronikada, mobil qurilmalarda va personal kompyuterlarda NFC dan foydalanishni ilgari surish uchun NXP Semiconductors, Sony va Nokia kompaniyalari tomonidan 2004 yilning 18 martida asoslangan notijorat uyushmasi hisoblanadi. NFC Forum qurilmalar va xizmatlar orasida o'zaro ta'sirlashishi qobiliyatini kafolatlash uchun NFC texnologiyasini ishlatish va standartlashtirishga ko'maklashadi. 2007 yilning sentyabrida NFC Forum a'zolari 130 tadan ortdi.

2010 yilning oktyabrida i-Free kompaniyasi xalqaro NFC Forum tashkilotiga qo'shildi. i-Free NFC Forum ga qo'shilgan birinchi Rossiya kompaniyasi bo'ldi. i-Free da ishlatilgan NFC bazasidagi loyihalardan NFC-yechimlar sinov zonasining qurilishini ajratish mumkin. Bu loyihaning test sinovlari Sankt-Peterburgda muvaffaqiyatli o'tdi.

2011 yilning martida NFC Forum ga yetakchi qatnashuvchi (Principal Member) sifatida Google qo'shildi. Bu kattaligi bo'yicha NFC Forum ning ikkinchi roli bo'ldi. U NFC Forum standartlariga muvofiq o'z laboratoriyalarida ishlab chiqariladigan qurilmalarning tijorat sirlarini oshkor qilmasdan qurilmalarni testlashni o'tkazishga imkon beradi.

GSMA assotsiatsiyasi. GSM Association (GSMA) jahonning 218 ta davlatlaridagi 700 ta aloqa operatorlaridan iborat global savdo uyushmasi hisoblanadi.

GSMA assotsiatsiyasi ikkita tashabbusni (Mobile NFC initiative) berdi: NFC da ishlaydigan o'n to'rtta mobil tarmoqlar operatorlari mobil aloqa global bozorining 40 foizini beradi va NFC uchun ilovalarni rivojlantirish uchun hamkorlik qiladi (Bouygues Telecom, China Mobile, AT&T, KPN, Mobilkom Austria, Orange, SFR, SK Telecom, Telefonica Moviles Espana, Telenor, TeliaSonera, Telecom Italia Mobile (TIM), Vodafone and 3 (telecommunications)).

2007 yilning 13 fevralida NFC ekotizimiga mobil aloqa tizimlarining nuqtai nazarlarini berish uchun NFCning texnik tavsifini nashr etdi.

«Pay buy mobile initiative» tashabbusi mobil qurilmalarni to'lov va kontakt tizimlar bilan bog'lash uchun Near Field Communications (NFC) texnologiyasidan foydalanishga umumiy global yondashuvni aniqlashga intildi. Hozirgi vaqtgacha 30 dan ortiq mobil aloqa operatorlari bu tashabbusga qo'shildi.

StoLPaN konsorsiumi. StoLPaN (Store Logistics and Payment with NFC) European Commission's va Information Society Technologies dasturlari tomonidan qo'llab-quvvatlanadigan Yevropa konsorsiumi hisoblanadi. StoLPaN lokal simsiz interfeyslar, NFC va mobil aloqaning yangi turlarini moslashtirish maqsadida hali ishlatilmagan potensialni tadqiq qiladi.

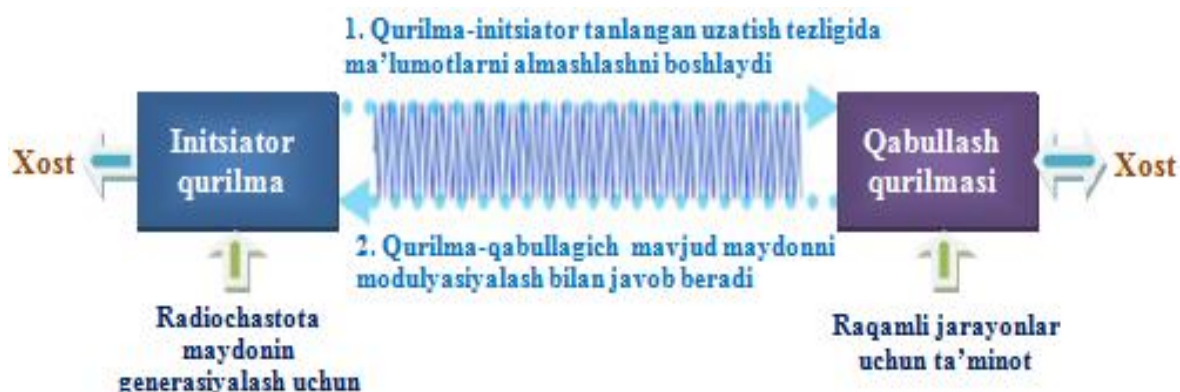
Boshqa standartlar. NFCga jalb qilingan boshqa standartlar quyidagilarni o'z ichiga oladi:

- SIM-karta va NFC mikrosxemalari to‘plami orasidagi aloqani o‘rnatish uchun ETSI / SCP (smart-kartlar platformasi);
- Single Wire Protocol — SIM-karta va NFC fizik darajasi mikrosxemasi almashtirish protokolidagi ETSI standarti;
- himoyalangan mikrosemaning ko‘p amaliy arxitekturasini aniqlash uchun GlobalPlatform;
- EMV to‘lov ilovalariga ta’sir etish uchun EMVCo.

5.3. NFC aloqa rejimlari

NFC da ikkita aktiv va passiv aloqa rejimlari mavjud [23].

Passiv aloqa rejimi. Qurilma-initsiator tashuvchi maydonni va mavjud maydonni modulyatsiyalash bilan maqsadli qurilmaga javoblarni ta’minlaydi (5.2- rasm). Bu rejimda maqsadli qurilma o‘z ishchi quvvatini initsiator taqdim etgan elektromagnit maydondan tortib oladi va bu bilan u retranslyator bo‘ladi.

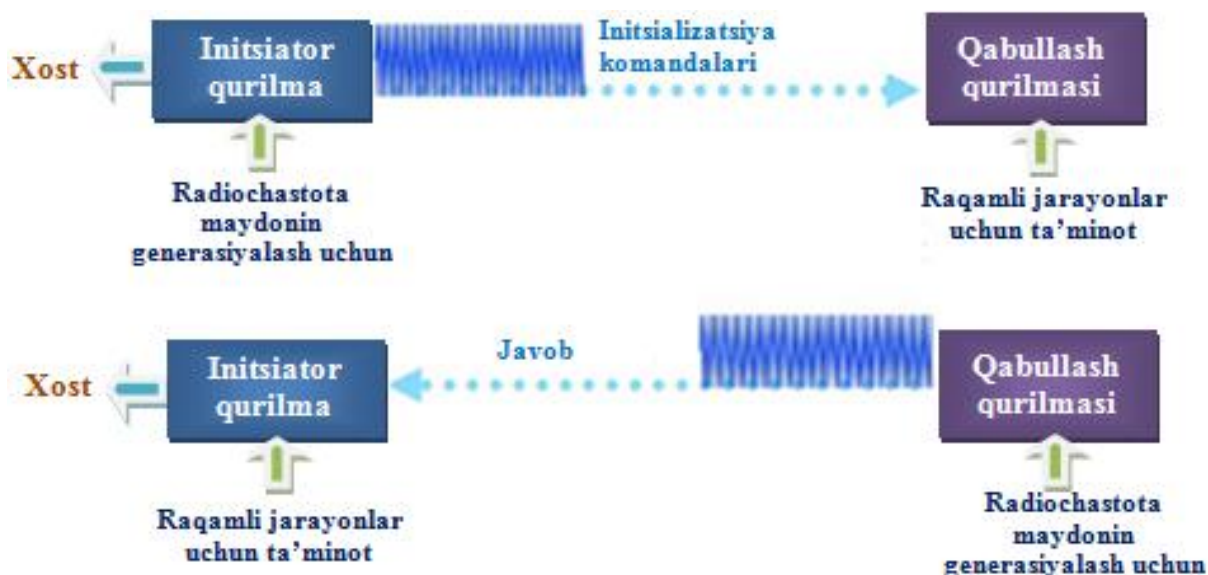


5.2- rasm. NFC passiv aloqa rejimi

Aktiv aloqa rejimi. Ham initsiator, ham maqsadli qurilma o‘z maydonlarini navbatma-navbat yaratish yo‘li bilan o‘zaro ta’sirlashishadi (5.3- rasm). Qurilma ma’lumotlarni kutayotgan vaqtda o‘z radiochastota maydonlarini aktivlashtirishdan chiqaradi. Bu rejimda har ikkala qurilmalarda elektr ta’minoti bo‘lishi kerak.

Ma’lumotlarni uzatish uchun NFC ikkita turli kodlashtirishni ishlatadi. Agar aktiv qurilma ma’lumotlarni 106 kbod tezlikda uzatsa, u holda 100 % modulyatsiyali modifikatsiyalangan Miller coding ishlatiladi. Qolgan barcha hollarda 10 % modulyatsiya koeffitsientili Manchester coding ishlatiladi.

NFC qurilmasi bir vaqtda ma'lumotlarni uzatish va qabul qilish holatida bo'ladi. Shunday qilib, ular radiochastotali maydonni nazorat qilishi va agar olingan signal uzatilgan signalga mos kelmaslik zidligini aniqlashi mumkin.



5.3- rasm. NFC aktiv aloqa rejimi

Har bir rejimda uchta NFC-A (14443 A), NFC-B (14443 V), NFC-F (JIS X 6319-4) usullardan biri qo'llanilishi mumkin. Uzatish usulini tanish uchun initsializatsiyalovchi qurilma so'rov yuboradi. Kodlash va modulyatsiya rejimlarining xarakteristikalari 5.2- jadvalda berilgan [232].

5.2- jadval

NFC rejimlari xarakteristikalari

Standart	Qurilma turi	Kodlash	Modulyatsiya	Uzatish tezligi, kb/s	Tashuvchi, MGs
NFC-A	So'rovchi	Millerning modifikatsiyalangan kodi	ASK 100%	106	13,56
	Eshituvchi	Manchester	Yuklamaning modulyatsiyasi (ASK)	106	13,56 ± 848 kGs
NFC-B	So'rovchi	NRZ-L	ASK 10%	106	13,56
	Eshituvchi	NRZ-L	Yuklamaning modulyatsiyasi	106	13,56± 848 kGs

			(BPSK)		
NFC-F	So‘rovchi	Manchester	ASK 10%	212/424	13,56
	Eshituvchi	Manchester	Yuklamaning modulyatsiyasi (ASK)	212/424	13,56 (nimtashuvchisiz)

Passiv rejimda aktiv NFC-qurilmalar bilan almashinuv uchun mo‘ljallangan NFC belgilar – passiv qurilmalar ishlatiladi. RFID belgilar kabi NFC belgilar uncha katta bo‘lmagan ma’lumotlar miqdorini saqlash uchun qo‘llaniladi. Jami 4 ta belgilar turlari aniqlangan (5.3- jadval).

5.3- jadval

Belgilar turlari

Turi	1	2	3	4
Standart	14443 A	14443 V	JIS 6319-4	14443 A/V
Qo‘shma mahsulot	Innovision Topaz	NXP Mifare	Sony FeliCa	NXP DESFire, SmartMX-JCOP, dr.
Uzatish tezligi, kb/s	106	106	212, 424	106, 212, 424
Xotira hajmi	96 b, 2 kb gacha kengaytirish	48 b, 2 kb gacha kengaytirish	1 Mb gacha	32 kb gacha
Kolliziyalardan himoyalash	Yo‘q	Yo‘q	Yo‘q	Yo‘q

5.4- jadvalda NFC texnologiyaning boshqa kommunikatsion texnologiyalar bilan taqqoslash keltirilgan.

NFC texnologiyaning boshqa kommunikatsion texnologiyalar bilan taqqoslash ko‘rsatdiki, bu insonga mo‘ljallangan eng qisqa diapazoni texnologiya hisoblanadi. Boshqa texnologiyalar, masalan RFID (Radio Frequency IDentification) o‘xshash parametrlarga ega bo‘ladi, lekin boshqalariga nisbatan to‘ldiruvchi hisoblanadi. Bunday texnologiyalarga Bluetooth va IrDa larni (Infrared Data Association – ma’lumotlarni uzatish infraqizil porti) kiritish mumkin.

NFC texnologiyaning boshqa kommunikatsion texnologiyalar
bilan taqqoslash

	NFC	RFID	IrDa	Bluetooth
Aloqaning o‘rnatilishi vaqti	0,1 ms dan kam emas	0,1 ms dan kam emas	~ 0,5 s	~ 6 s
Ta’sir etish masofasi	20 sm gacha	3 m gacha	5 m gacha	25-30 m gacha
Ishlatilishi qulaylik	Insonga mo‘ljallangan, engillik, intuitivlik, tezkorlik	Elementga mo‘ljallangan, engillik	Ma’lum otlarga mo‘ljallangan, engillik	Insonga mo‘ljallangan, o‘rtacha
Tanlovc hanligi	Yuqori, ma’lumotlarni uzatish, xavfsizlik	Qisman ulanish	Nurning yo‘nalishi burchagiga bog‘liq	“Men kim?” so‘rash prinsipi
Qo‘llanilishi hollari	To‘lov, ulanishni olish, initsializatsiya xizmati, oson o‘rnatish	Elementni kuzatish	Ma’lum otlarni almashtirish va boshqarish	Ma’lum otlarni almashtirish uchun tarmoq, simsiz garnitura

5.4. NFC texnologiyasining qo‘llanilishi sohalari

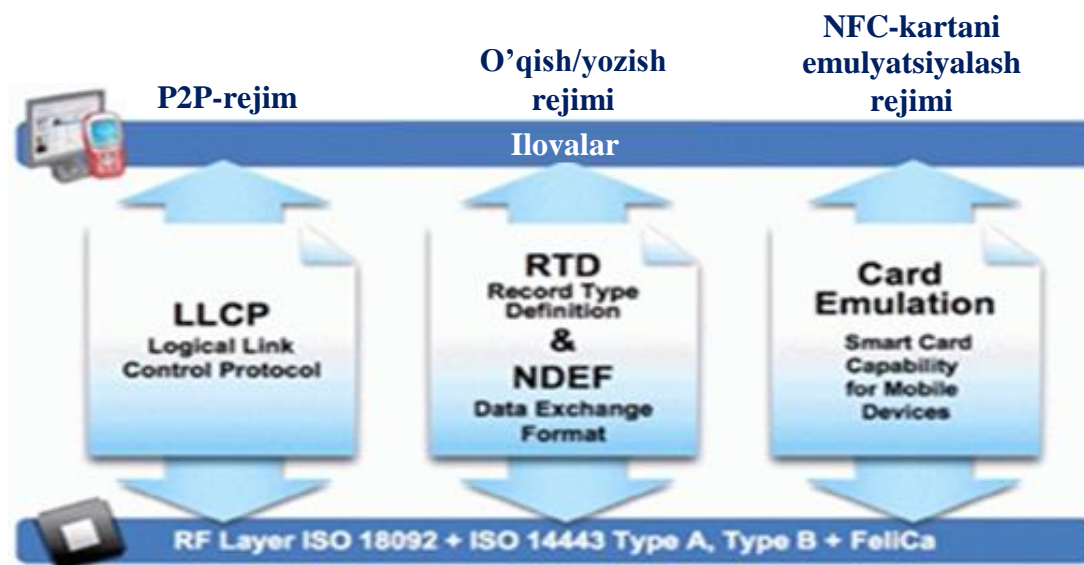
NFC texnologiyasi hozirgi vaqtda, asosan, mobil telefonlarda foydalanish maqsadlariga yo‘naltirilgan. NFC ni qo‘llanilishining uchta asosiy sohasi mavjud (5.4-rasm) [23]:

1. Peer-to-Peer rejimi qurilma-qurilma kommunikatsiyalari uchun aniqlangan. Uning yordamida smartfonlar orasidagi kontaktlarni, WiFi-routerdan i mobil qurilmalarga sozlanishlarni oniy uzatish mumkin. Shuningdek bu rejimda smartfonlarni multipleyer o‘yinlari uchun birlashtirish mumkin.

2. O‘qish/yozish rejimi ilovalarga NFC-xabarlarini almashtirishga imkon beradi. Bu rejimda telefon o‘qish qurilmasi sifatida ishlaydi.

Uni shtrix-kodlar skaneri analogi sifatida ishlatish mumkin. Faqat shtrix-kodlar o‘rniga predmetlar o‘rniga qo‘shimcha ma’lumotlarli NFC-belgilar ishlatiladi.

3. NFC-kartani emulyatsiyalash rejimi NFC-telefon garniturasiga standart smart-karta sifatida ishlashga imkon beradi. Aynan bu rejim ko‘pincha NFC texnologiyasi bilan assotsiyalanadi. U tufayli smartfon bank kartasi yoki metroga yo‘l chiptasi bo‘lishi bilan bu buyumlarni olib yurish zaruratidan foydalanuvchini xalos qiladi.



5.4- rasm. NFCning qo‘llanilishi sohalari

NFCning bo‘lishi mumkin qo‘llanilishlari:

Jamoat transportida mobil sotib olish – mavjud kontaktsiz infratuzilmani kengaytirish.

Mobil to‘lovlar – qurilma to‘lov kartasi sifatida ishlaydi.

Elektron doska – mobil telefon yurayotganda ma’lumotlarni olish uchun ko‘cha e’lonlar taxtalaridan RFID-belgilarni o‘qish uchun ishlatiladi [24].

5.5- 5.8- rasmlarda NFC ning qo‘llanilishiga misollar keltirilgan.

Bluetoothlarni juftlashtirish – kelajakda NFC da ishlaydigan Bluetooth 2.1 undan yuqori qurilmalarni bog‘lanishi uchun ularni yaqinlashtirish va bog‘lanishni qabul qilish yetarli bo‘ladi. Har ikkala tomonlarni aktivlashtirish jarayoni, qidirish, kutish, bog‘lanish va mualliflashtirish telefonlarning oddiy tekkizish bilan almashtiriladi.



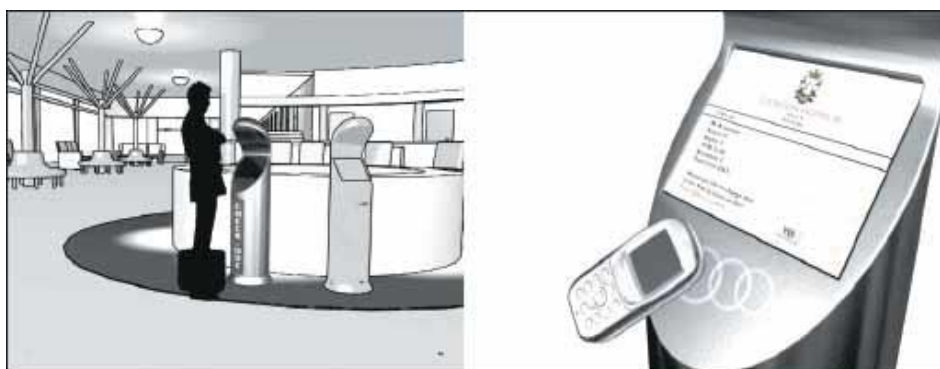
5.5- rasm. Ofisdan yoki uydan chiptalarga va mehmonxonalar joylariga buyurtma berish



5.6- rasm. Reysga ro'yxatdan o'tish



5.7- rasm. Mehmonxonada ro'yxatdan o'tish



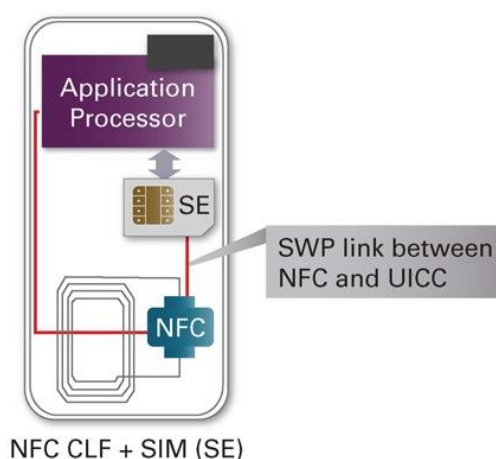
5.8- rasm. Mehmonxonadan jo'nash

Boshqa qo‘llanilishlar quyidagilarni o‘z ichiga olishi mumkin:

- chiptalarni elektron sotib olish (aviachiptalar, konsertlarga chiptalar va boshqalar);
- elektron pullar;
- sayohatchi xaritasi;
- shaxsni tasdiqlash guvohnomalari;
- mobil savdo;
- elektron kalitlar – mashina, uy va ofis, mehmonxona nomeri va boshqalar kalitlari;
- Bluetooth, Wi-Fi yoki Ultra-wideband kabi boshqa simsiz bog‘lanishlarni konfiguratsiyalash va initsializatsiyalash uchun;
- hozirgi vaqtda mustaqil filial Dolby Laboratories bo‘lgan Via Licensing Corporation da ishlab chiqilayotgan NFC uchun patentni litsenziyalash dasturi.

5.9- rasmda NFC ning telefonda ishlatilishi imkoniyatlaridan biri tasvirlangan.

NFC Renesas RF21 kontroller kabi kontaktsiz mijoz qismi (CLF) radiochastotali ulanishni qayta ishlaydi va telefonning ilovalari protsessori va abonentni identifikatsiyalash moduli bilan (SIM-karta bilan) o‘zaro ta’sirlashishadi [23].



5.9- rasm. Ssenariylardan birida telefon abonentni identifikatsiyalash moduli ulanadigan mijoz qismidan (CLF) foydalanishli yaqindan ta’sir qilish aloqasiga integratsiyalanishi mumkin

5.5. NFC texnologiyalarining jahon mamlakatlarida joriy etilishi

Kontaktsiz to‘lov tizimlari eng keng tarqalgan davlatlarga Yaponiya kiradi, bu yerda Sony kompaniyasi tomonidan ishlab

chiqilgan NFCga yaqin bo'lgan FeliCa tizimi ishlatiladi [23]. Osaifu-Keitai brendi ostidagi servislar elektron pullarni, identifikatsiyalash va to'g'rilik kartalarini, yo'l haqi to'lovlari kartalarini, kredit kartalarini va boshqalarni o'z ichiga oladi. 2011 yilning oxirida mobil aloqa yapon operatorlari Felica texnologiyasining NFCga bosqichma-bosqich o'tishi rejalarini e'lon qildi.

2011 yilning o'rtalarida Janubiy Koreyaning mobil operatorlari, plastik kartalar emitentlari, maishiy elektronika ishlab chiqaruvchilari va hukumat tashkilotlari Grand NFC Korea Alliance ni ta'sis etdi, uning asosiy maqsadi \$1 mlrd. hajmli yangi bozorni va 5 mingdan ortiq yangi ish joylarini yaratish bo'ldi [23].

Buyuk britaniyada pochta xizmati butun mamlakat bo'yicha 11,5 mingta pochta xizmati bo'limlarida 30 mingta NFC-terminallarini o'rnatishni rejalashtirmoqda. Foydalanuvchilar xizmatlarga to'lovlarni Mastercard PayPass yoki Visa PayWave kontaktsiz kartalari orqali va NFC texnologiyasida ishlaydigan smartfonlar yordamida amalga oshirishi mumkin.

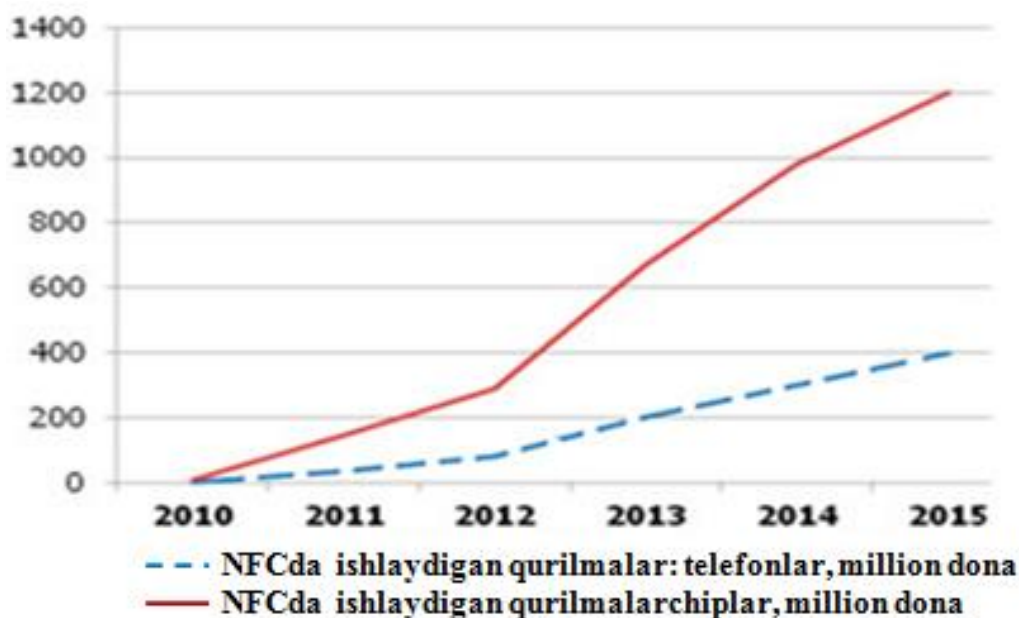
2011 yilning yozida Fransiya hukumati NFC bazasidagi xizmatlarni ilgari surish uchun €20 mln. investitsiyalashga tayyorligini e'lon qildi. To'rtta mobil operator va to'rtta bank 2012 yilda milliy ko'lamda NFC-servislarini ishga tushirish bo'yicha o'z rejalarini e'lon qildi.

2011 yilning boshida transport kompaniyalari bo'lgan Deutsche Bahn (DB) nemis temir yo'l operatori va RMV kompaniyasi Germaniyada chiplarni sotish milliy NFC-tizimini yaratishda hamkorlikni boshlashdi.

Xalqaro to'lov tizimlaridagi yirik NFC loyihalar Mastercard PayPass va Visa PayWave hisoblanadi. Parallel ravishda muqobil Google Wallet, Isis va boshqa yechimlar rivojlanmoqda. Qatar milliy banki Katara (Qatar National Bank, QNB) Qtel mobil operatori bilan hamkorlikda mijozlarga NFC yordamida to'lovlar uchun hisobni aktivlashtirishda va bitta tranzaksiyani amalga oshirishda 100 qatar realligacha (\$27,5 atrofida) pulli bonuslarni taklif qilmoqda.

Jahon NFC bozori bo'yicha ma'lumotlar va taxminlar bu segmentning yuqori potentsiali haqida guvohlik beradi. Masalan, Berg Insight taxminlari bo'yicha NFC smartfonlarning sotilishi yaqin 5 yilda o'rtacha yillik o'sish jadalligida 87,8% ga ortadi, bu tufayli 2016 yilda bozorga 700 millionta NFC smartfonlar yetkazib beriladi. 2011 yil yakunlari bo'yicha 30 millionta NFC da ishlaydigan mobil

telefonlar sotilgan va 40 dan kam bo‘lmagan NFC-modellari ishlab chiqarilgan. IMS Research taxminlari bo‘yicha 2012 yilda jahonda 80 millionta NFC da ishlaydigan mobil telefonlar va 300 millionta atrofida NFC-chipsetlar sotiladi, 2015 yilga kelib esa bu ko‘rsakichlar mos ravishda 400 va 1200 milliontaga yetadi (5.10-rasm) [23].



5.10- rasm. NFCda ishlaydigan qurilmalar

5.6. O‘zbekistonda NFC-texnologiyalardan foydalanish istiqbollari

O‘zbekistonda SMS-To‘lov tizimi bazasida tovarlar va xizmatlarga kontaktsiz to‘lov texnologiyasini joriy etish bo‘yicha ishlar olib borilmoqda [20]. O‘zbekiston savdo-sanoat palatasi O‘zbekiston Milliy banki, O‘zbekiston banklar Uyushmasi, Davlat soliq qo‘mitasi, O‘zbekiston Respublikasialoqa, axborotlashtirish va telekommunikatsion texnologiyalar Davlat qo‘mitasi, Uzkart tizimi va boshqa davlat organlari bilan birga O‘zbekistonda NFC ni joriy etish bo‘yicha ishlamoqda [21].

Hozirgi momentda Ucell va Beeline sotali kompaniyalari bilan barcha shartlar kelishilgan, ular testli ishlashlar uchun 1 000 tadan sim-kartalarni taqdim etishga rozi bo‘lishgan.

Oddiy SIM-karta 125 kb dan ortiq bo‘lmagan sezilarsiz xotiraga ega, bu kontaktlarni saqlashga yetadi, lekin multimediyali fayllarni

saqlashga yetarli emas. Ustida ishlar olib borilayotgan NFC li SIM-kartalar 500 Mb gacha xotiraga ega, bu unga har qanday xarakterdagi ma'lumotlarni yozishga imkon beradi.

NFCning joriy etilishi birinchi navbatda mahsulotlarga va xizmatlarga qulay va tezkor to'lashga imkon beradi.

O'zbekistonda hozir SMS-To'lov protsessingli to'lov tizimi ishlarida, u orqali tovarlar va xizmatlarga onlayn to'lovlar amalga oshirilmoqda. Ilovadan tijorat bankiga bir marta pasport va mobil telefon bilan kelish va "SMS-TO'LOV" tizimida ro'yxatdan o'tish bilan foydalanishni boshlash mumkin. Keyinchalik ilovada NFC bo'limi paydo bo'ladi.

Offline plastik kartalari o'rniga online-kartalarining joriy etilishi mobil to'lovlarning rivojlanishiga olib keladi, bu kartalar endi mobil to'lovlarda ishlaydi.

NFC texnologiyalardan foydalanish uchun quyidagi sohalar taklif etilmoqda:

1. Magazinlarda sotib olishlarni amalga oshirish. NFCli telefon orqali tovarlarga qo'yilgan maxsus stikerlar bo'yicha amalga oshiriladi. Kassaning yonida terminalga telefon yaqinlashtiriladi, to'lov amalga oshiriladi. To'lov vaqti bir necha sekundlarga qisqaradi.

2. NFC joriy etilishi bilan vokzallardagi, aeroportlardagi va avtobuslar to'xtash joylaridagi ma'lumotlar pannolariga zarurat yo'qoladi. Telefoni NFC-belgiga yaqinlashtirish kifoya bo'ladi va telefonda marshrutlar, narxlar, kelish va ketish vaqtlari bo'yicha ma'lumotlar paydo bo'ladi.

3. Avto yonilg'i quyish stansiyalari hollarida hozirda bajarilayotgan plastik karta orqali chiqish, kassaga borish va to'lash kerak emas. Faqat avtomobildan qo'lni chiqarish va telefoni maxsus terminalga yaqinlashtirish yetarli bo'ladi. Bularning barchasi 5 sekundni oladi.

4. NFC joriy etilishi bilan har xil turlardagi plastik kartalar egalari vaziyatlari yengillashadi, chunki hamma joylarda ma'lum kartalar bilan emas, to'g'ridan-to'g'ri pul vositalari bilan ishlaydigan bir xil NFC terminallari bo'ladi.

Nazorat savollari

1. NFC texnologiyasi spetsifikatsiyasi nimadan iborat?
2. NFC texnologiyasining ahamiyati bormi?

3. NFC texnologiyasining standartlashtirishini tushuntiring.
4. NFC texnologiyasining sanoat loyihalarini tushuntiring.
5. NFC aloqa rejimlari qaysilar?
6. NFC texnologiyasi qanday sohalarda qoʻllaniladi?
7. NFC texnologiyalarining jahon mamlakatlarida joriy etilishini tushuntiring.
8. Oʻzbekistonda NFC texnologiyalardan foydalanish istiqbollarini tushuntiring.

6- BOB. ZIGBEE TEXNOLOGIYASINING QO'LLANILISHI

6.1. Zigbee texnologiyasining tavsifi

Ma'lumotlarni to'plash va boshqarish tizimlarida ishlatish uchun mo'ljallangan simsiz texnologiya hisoblanadi [21]. U past energiya iste'moliga, ma'lumotlarni uzatish ishonchliligiga va ma'lumotlarni himoyalashga ega, turli ishlab chiqaruvchilar qurilmalari bilan moslashuvchan. ZigBee ma'lumotlarni uzatishda kechikishlarga qat'iy talablar qo'yilmaydigan tizimlarda ma'lumotlarni uzatilishiga yo'naltirilgan. Bu texnologiya binolar va ko'p sonli tugunlarli (standart bo'yicha 65 mingtagacha) boshqa yirik ob'ektlarni yagona simsiz tarmoq bilan qamrab olishga imkon beradi. Bularning barchasiga xabarlarni marshrutlashtirishning murakkab mexanizmlarini qo'llanilishi hisobiga erishiladi, bu tarmoqning oxirgi nuqtasiga o'nlab oraliq tugunlar orqali ma'lumotlarni uzatilishiga imkon beradi.

2002 yilda Invensys, Mitsubishi Electric, Philips Semiconductors va Motorola kompaniyalari ZigBee (shuningdek HomeRF lite, Firefly va RF-EasyLink sifatida ma'lum bo'lgan) nomini olgan yangi simsiz aloqa standartini ilgari surish bo'yicha uyushma tashki etishdi. Bugungi kunda ZigBee nomi ostida deyarli IEEE 802.15.4 standartiga protokollar va kengaytmalar to'plami yashiringan bo'lib, u tufayli turli ishlab chiqaruvchilar qurilmalarining moslashuvchanligi ta'minlanadi.

IEEE 802.15.4 standarti ZigBee tarmog'ining radiochastotaviy qismi – modulyatsiyalash turi (BPSK va O-QFSK), chastotalar diapazonlari va ularga mos uzatish tezliklari tavsifiga ega. ZigBee spetsifikatsiyasi 10 dan 75 metrlargacha radiusda 250 kbit/s maksimal tezlikda ma'lumotlarni uzatilishini ko'zda tutadi. Lekin uncha yuqori bo'lmagan o'tkazish qobiliyati o'ta past energiya iste'moli bilan kompensatsiyalanadi, chunki standart apparatura faqat kam vaqtda efirni eshitishi bilan vaqtning katta qismida uxlash rejimida bo'lishi hisobiga qurilmalarning maksimal past energiya iste'molini ko'zda tutadi. ZigBee standartiga uchta 2,4 GGs (16 ta kanallar), 915 MGs (10 ta kanallar) va 868 MGs (1 ta kanal) chastotalar diapzonlaridagi 27 ta kanallar birlashtirilgan. Bu efir diapazonlari uchun maksimal ma'lumotlarni uzatish tezliklari mos ravishda 250 kbit/s, 40 kbit/s va 20 kbit/s larni tashkil etadi. Kanalga ulanish tashuvchini nazorat qilish (Carrier Sense, Multiple Access, CSMA) bo'yicha amalga oshiriladi,

ya'ni qurilma dastlab efir band emasligini tekshiradi va faqat bundan keyin uzatishni boshlaydi. 128 bitli kalit uzunligili AES algoritmi bo'yicha shifrlash qo'llanadi. 802.15.4 standarti MAS darajadagi noyob 64-bitli manzilning bo'lishini, shuningdek bu qurilmaning u yoki bu WPANga (Wireless Personal Area Network) tegishlilikini aniqlash uchun qo'shimcha 16-bitli tarmoq manzilini (PAN-ID) bo'lishini ko'zda tutadi.

6.2. Zigbee tarmog'ini qurishning afzalligi

Istalgan standart, ma'lumotlarni simli almashlash interfeysi yoki simsiz aloqa bo'lsin, o'z masalalari doirasini yechish uchun yaratiladi. Misol uchun WiFi video va audioni uzatishga imkon berish bilan o'rtacha masofalarda nisbatan katta ma'lumotlarni uzatish tezliklarida bog'lanishga imkon beradi. WiFi simsiz qurilmalarni korporativ tarmoqlar va Internetga ulanishi uchun qo'llashga mo'ljallangan. Shuningdek, Bluetooth standarti kichik masofalarda ma'lumotlarni uzatishga mo'ljallangan. Bluetooth tezlikda WiFiga sezilarli yutqazadi. U oqimli audio yoki videoni, masalan uy komponentlari orasida uzatishga ideal to'g'ri keladi. ZigBee yordamida hal etiladigan asosiy masala bu uncha katta bo'lmagan ma'lumotlar hajmini o'rta masofalarga uzatish hisoblanadi. ZigBeeni vazifasining o'ziga xosligi shundan iboratki, bu standartning qabullash-uzatish qurilmalari minimal energiya iste'moliga ega bo'lishi kerak. IEEE 802.15.4 va ZigBee orqali yuqori aniqlikdagi sifatli oqimli audio yoki videoni uzatish mumkin emas, biroq murakkab monitoring qilish sxemalarini amalga oshirish mumkin [21].

Alyansning asosiy maqsadi turli ilovalar xavfsizlik funksiyalari va moslashuvchan profillarili turli "yulduz", "klasteri daraxt", "ko'p yacheykali tarmoq" tarmoqlar topologiyalarini qo'llaydigan ZigBee protokollari dasturiy stekining yagona spetsifikatsiyasini ishlab chiqish hisoblanadi. ZigBee spetsifikatsiyasi 250 Kbit/sgacha uzatish tezliklari, o'ta past energiya iste'moli qo'llanadigan va ma'lumotlarni himoyalash va tizimning ishonchliligini ta'minlaydigan yagona global standartga asoslangan simsiz tarmoq yechimini ishlatishga imkon beradi.

ZigBee 802.15.4 standarti darajalari ustidan qo'shimcha tarmoq qatlami dasturiy ta'minotini ishlab chiqayotgan kompaniyalar alyansi hisoblanadi. Alyansning a'zolari moslashuvchan simsiz tarmoqlarning

yangi bozorini aniqlaydi. Konsorsiumda qatnashish tufayli uning barcha faol a'zolari ZigBee texnologiyasi bo'yicha barcha texnik ma'lumotlarga to'liq mumkinlikka va ZigBee spetsifikatsiyasiga ta'sir etish imkoniyatiga ega.

ZigBee texnologiyasi yuqori texnik xarakteristikalarli va mos ravishda qimmat qurilmalar va texnologiyalar yoki qat'iy standartlashtirilgan asosga ega bo'lmagan elektron komponentlar turli ishlab chiqaruvchilaridan radiotransiverlar alohida mikrosxemalariga asoslanadigan yechimlar to'ldirgan radiointerfeyslarning oldin bo'shagan joyini egalladi.

Ishlab chiquvchilar oddiy masalalarni yechishda oshirilgan xarajatlarga borishga yoki personal lokal tarmoqlarni yaratish uchun o'z uzatish protokollari va dasturiy steklarini yaratishga majbur bo'lishdi, bu ham yakuniy jihozning narxiga va tayyor mahsulotni bozorga chiqishi muddatlariga ta'sir qildi. Natijada ko'pincha mahsulotning yangiligiga va unga bozorning qiziqishi yo'qotildi.

ZigBee/802.15.4 dastlab tijorat, sanoat va uy avtomatikasida ishlatiladigan quyidagi monitoring va nazorat qilish ilovalari, taqsimlangan xabarlagichlar tarmoqlari, kam energiya iste'mol qiladigan tizimlar uchun simsiz axborot tarmoqlarini qurishga mo'ljallangan yagona standartlashtirilgan simsiz texnologiya hisoblanadi:

- yoritishni boshqarish tizimlari (sanoat, munitsipal va uy);
- sanoat va uy avtomatikasi va boshqarish (isitish, ventilyatsiya va konditsionirlash (IVK), yordamchi qurilmalar va vositalar);
- iste'mol elektronikasi (multimediya/ko'ngilochar vositalari, portative elektronika), maishiy texnika;
- PK periferiya qurilmalari: sichqoncha, klaviatura, o'yin qurilmalari, joystiklar;
- signalizatsiya va xavfsizlik, avariya dan ogohlantirish tizimlari, ulanishni nazorat qilish tizimlari, kontaktsiz kalitlar, tutun, gaz, harakat, olov, harorat, bosim xabarlagichlari va boshqalar;
- bemorni tibbiy diagnostika qilish qurilmalari, sportchilarning holatini monitoring qilish, bioxabarlagichlar va tibbiyot jihozlari;
- texnologik jarayonlarni olisdan boshqarish va nazorat qilish, harakatlanadigan apparatlar, dastgohlar, sanoat qurilmalari, sovutish qurilmalari, masofadan ma'lumotlarni to'plash qurilmalarini boshqarish, telemetriya;
- sanoat va portaktivlarini monitoring qilish, logistika ;

– suv, gaz va issiqlik ta’minoti tizimlari, elektr energiyasini boshqarish va instrumental nazorat qilish tizimlari, turar-joy kommunal (TJK) xo‘jaligi tizimlarini monitoring qilish;

– ma’lumotlarni simsiz almashlash qurilmalari, radiomodemlar, radiouzatish;;

– avtomobil elektronikasi (shinalardagi bosimni nazorat qilish tizimlari, olib qochishga qarshi tizimlar, identifikatsiyalash va diagnostika qilish tizimlari) va h.k..

ZigBee/802.15.4 standartining asosiy afzalliklaridan biri bunday qurilmalarni o‘rnatilishi va xizmat ko‘rsatilishi oddiyligi hisoblanadi. ZigBee spetsifikatsiyasining o‘ziga xos xususiyatlari oson simsiz personal tarmoqlarni qurishga imkon beradi. “Siz qurilmani qutidan olasiz, batareyani qo‘yasiz va tugmachaning bosilishiga o‘xshash oddiy operatsiyani amalga oshirasiz – ikkita qurilmalarni bir-birlariga yaqinlashtirasiz, tugmachani bosasiz va yashil yorug‘lik diodlari yonguncha tutib turasiz”. Shunday qilib, ikkita qurilmalarni tarmoqqa birlashtirish yoki bog‘lanish, masalan yoritishni uzgichni ma’lum lampaga bog‘lanishi bo‘lib o‘tadi. Bu prinsipning amalga oshirilishi ham uncha katta bo‘lmagan binolarda (uy va ofis), g‘am korxonalarida (sanoat zonasi, zavodlar) barcha yangi asboblar va tizimlarga ZigBee-modullarni joriy etilishini ko‘zda tutadi [1].

ZigBee-qurilmalar uchun boshqa ko‘plab qo‘llanilish sohalari ham topiladi. Istiqbolda ZigBee simsiz tarmoqlari Bluetooth texnologiyasiga jiddiy raqobatni hosil qilishi kerak. 6.1- jadvalda ZigBee aloqaning asosiy texnik parametrlari keltirilgan.

6.1- jadval

ZigBee aloqaning asosiy texnik parametrlari

Xususiyatlari/Funksiya	Xarakteristika
Aloqa turi	Radioto‘lqinlar
Chastotalar diapazoni	868,902 va 2400 MGs
Kanallar soni	2,4 GGs (16 ta kanallar), 915 MGs (10 ta kanallar) va 868 MGs (1ta kanal)
Batareyaning xizmat ko‘rsatish muddati	100 dan 1000 gacha va undan ortiq kunlar
Uzatish usuli	Direct Sequence Spread Spectrum (DSSS) to‘g‘ri ketma-ketlik usulida spektrni kengaytirish
Ulanish vaqti	30 ms
Uzatish quvvati	1 mVt

Ma'lumotlarni uzatish tezligi	250 Kbit/sgacha
Ishlash masofasi	70 mgacha
Tarmoqdagi tugunlar soni	65 536 (64-bitli manzillar), 264 (16-bitli manzillar)
Ma'lumotlarni himoyalash	128 bitli kalit uzunligili AES algoritmi bo'yicha shifrlash
Manzillashtirish	MAS darajadagi noyob 64-bitli manzil, qo'shimcha 16-bitli manzil (PAN-ID)

6.3. WPAN tarmoqlar va IEEE 802.15.4 standartlari

Bugungi kunga kelib quyidagi uchta standartlar oilasi simsiz hisoblash tarmoqlari uchun keng qo'llaniladi [21]:

– IEEE 802.11 – Wireless Local Area Network (WLAN — simsiz lokal hisoblash tarmoqlari);

– IEEE 802.15 – Wireless Personal Area Network (WPAN — simsiz personal hisoblash tarmoqlari);

– IEEE 802.16 – Broadband Wireless Access (BWA — simsiz keng polosali ulanish).

WPAN simsiz personal hisoblash tarmog'i odatda 15...20 metrdan oshmaydigan kichik ishlash radiusili lokal tarmoq hisoblanadi va personal kompyuterlar orasida kabelli bog'lanishlarni almashtirish uchun, shuningdek turli xil periferiyalar va multimediya qurilmalari (ChPK, printerlar, fakslar, skanerlar, stereotizimlar va h.k.) bilan aloqa uchun mo'ljallangan. Biroq ayrim WPAN-tarmoqlar 100 metrlargacha (ZigBee, Bluetooth) masofalarda ishlay oladi. Bu masalalarni yecha oladigan birinchi standart IEEE 802.15.1 bo'ldi. Standart Bluetooth v1.x spetsifikatsiyalariga asoslanadi va fizik daraja (PHY layer) va muhitga ulanishi darajasini (MAC layer) aniqlaydi. IEEE 802.15.1 oilasini kengaytirishdagi keyingi qadam 802.11 va 802.15 sinflar qurilmalari orasida o'zaro ta'sirlashishni ta'minlaydigan standartni yaratilishi bo'ldi. Tez orada WPAN-tarmoqlar zonasida ishlaydigan qurilmalar uchun Bluetooth ta'minlaydigan tezliklar yetarli bo'lmay qoldi. O'nlab va yuzlab Mbit/s o'tkazish qobiliyatili simsiz kanalni yaratishga imkon beradigan standartni (IEEE 802.15.3) ishlab chiqishga zarurat yuzaga keldi. Yuqorida sanab o'tilgan standartlar katta ma'lumotlar

hajmlarini (ovoz, ma'lumotlar, video) yuqori tezliklarda (1 ... 200 Mbit/s) uzatish uchun juda yaxshi to'g'ri keladi. Ular asosidagi qurilmalar 10 ... 100 metrlar uzatish masofalarida avtonom rejimda (akkumulyatorlar batareyalaridan) ishlay oladi. Bu standartlar biz har kuni ishlaydigan qurilmalar (kompyuterlar, hisoblash tarmoqlari) bilan simli bog'lanishlarni almashtirishga imkon beradi. Lekin bir qarashda o'ziga xoslikka ega bo'lgan juda ko'plab sezilmas tizimlar (turli xil xabarlagichlar, ma'lumotlarni to'plash tizimlari va h.k.) borki, buning natijasida bunday turdagi ilovalar aytib o'tilgan texnologiyalarni yuz foizda samarali ishlatish mumkin bo'lmaydi. Bunday masalalarni amalga oshirish uchun past tezlikli WPAN-tarmoqlar uchun IEEE 802.15.4 (ZigBee) standarti ishlab chiqilgan.

Ravshanki, qisqa ishlash radiusli simsiz tarmoqlar o'zaro ta'sirlashishadi. Turli simsiz tarmoqlar orasida shlyuz vazifasini bajaradigan qurilmalarni ishlab chiqish rejalashtirilmoqda. Agar ZigBee asosida qurilgan xavfsizlik tizimi buzuvchini aniqlasa, u bu haqda kompyuterni ogohlantirish uchun IEEE 802.11 tarmog'i bilan bog'lanadi, u esa, o'z navbatida, egasining mobil telefoniga SMS xabarni jo'natadi yoki qo'riqlash xizmatiga signal beradi. 802.15 va 802.11b standartlari oilalarining nisbiy xarakteristikalarini 6.2-jadvalda keltirilgan.

Keltirilgan xarakteristiklardan kelib chiqqanda, yaqin raqobatchilar Bluetooth va ZigBee texnologiyalari hisoblanadi. Mos ravishda, ularning qo'llanilish sohalari ham o'xshash – uy va sanoat yo'nalishidagi, shu jumladan masofadan boshqarish tizimlari, kompyuter periferiyasi va boshqalar simsiz qurilmalari hisoblanadi. Lekin Bluetooth texnologiyasidan farqli ravishda ZigBee asosiy talablardan biri past energiya iste'moli hisoblanadigan ilovalar uchun ishlab chiqilgan. ZigBee texnologiyasi qurilgan qurilmalarning aktivlik davrlari juda kam bo'lishi mumkin, bu batareyalarning uzoq muddatli xizmat ko'rsatishini ta'minlaydi. Bundan tashqari, Wi-Fi va Bluetooth mikrosxemalari ular asosida korxonalar va ofis binolari ko'lamlarida turli qurilmalar yirik tarmoqlarini tashkil etish uchun juda qimmat, 802.15.4/ZigBee standarti esa minimal xarajatlari simsiz interfeyslarni ishlab chiqishga imkon beradi, bu sxemotexnikaning oddiyligi, tashqi passiv elementlarning minimal soni, unga ajratilgan xotirani yuqori samaradorlikda ishlatadigan stek dasturiy ta'minoti orqali ta'minlanadi (6.2-jadvalga qarang). Standart ko'p yacheykali tarmoqni yaratishga, bu bilan kuchaytirish

qurilmalariga qo‘shimcha xarajatlarsiz juda ko‘p sonli tugunlarga xizmat ko‘rsatish va aloqa masofasini oshirishga imkon beradi.

6.2- jadval

802.15 va 802.11b standartlari oilalarining nisbiy xarakteristikalari

Standart	802.15.4 Zigbee			802.15.1 Bluetooth	802.11b Wi-Fi
Ilova	Monitoring qilish, boshqarish			Ovoz, ma'lumotlar	Ma'lumotlar, video
Chastota, GGs	0.868	0.915	2.4		
Afzalliklari	Narx, energiya tejamkorligi, o'lchamlari			Narx, ovozni uzatish	Tezlik, tez moslashuvchanlik
Maksimal tezlik	20 kbit/s	40 kbit/s	250 kbit/s	1 mbit/s	11 mbit/s i bolee
Masofa, m	10-100, 1000			100	100
Sezgirlik, dBm (o'rtacha)	-92			-70	-76
Stek o'lchami, kBayt				>250	>1000
Batareyalar xizmat qilish muddati, kunlar	100-1000			1-7	0,5-1

ZigBee texnologiyasi Wi-Fi yoki Bluetooth kabi katta ma'lumotlar hajmlarini uzatish uchun mo'ljallanmagan. Lekin, masalan, hajmi o'nlab kilobaytlardan oshmaydigan xabarlagichlar ko'rsatkichlarini uzatish uchun yuqori talablar talab qilinmaydi, bu holda energiya iste'moli, narx va ishonchlilik bo'yicha yuqori ko'rsatkichlar kerak bo'ladi.

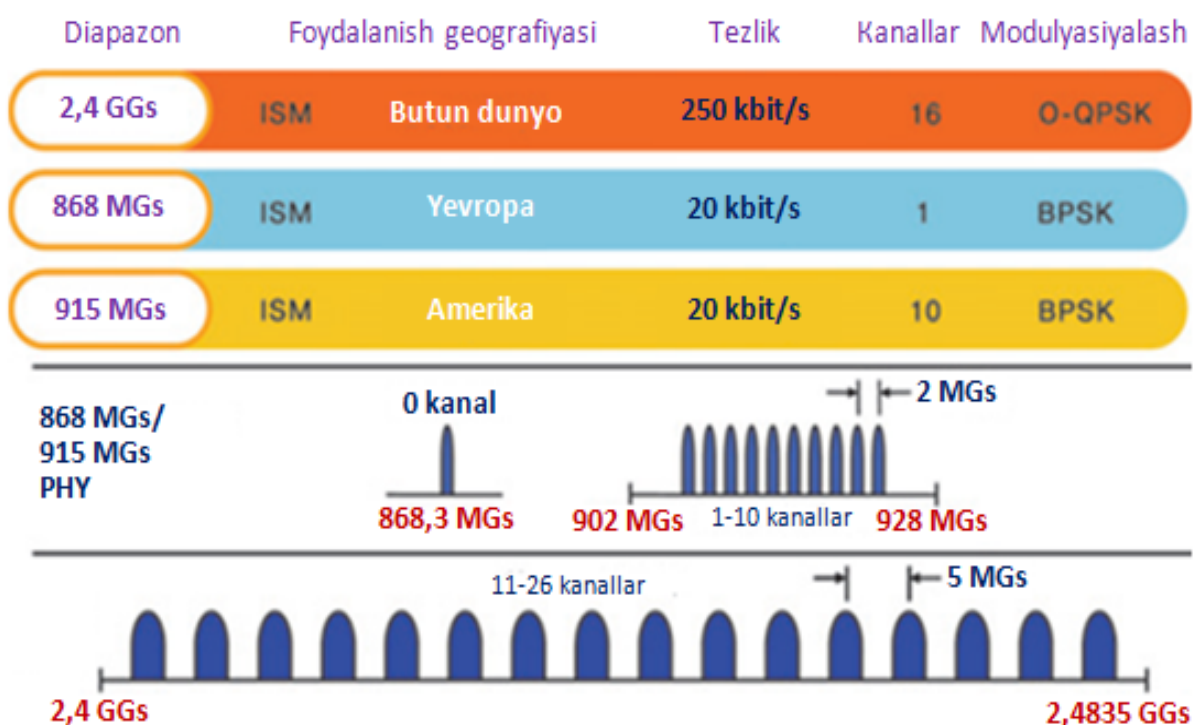
Ko'plab ZigBee qurilmalari quyidagi algoritm bo'yicha ishlaydi: qurilma butun vaqt davomida kutish rejimida bo'ladi, bu bilan optimal energiya tejamkorligini ta'minlaydi. Yangi ma'lumotlar kelganida yoki navbatdagi aloqa seansida qurilma aktivlashadi, ma'lumotlarni

tez uzatadi va yana pasaytirilgan energiya iste'moli rejimiga o'tadi. Bunda odatdagi vaqt kechikishlari yangi qurilmani tarmoqqa ulanishida 30 ms, "kutish" rejimidan aktiv holatga o'tish uchun 15 ms, kanal ulanish uchun 15 msni tashkil etadi. Shunday tarzda batareyalarning xizmat ko'rsatish muddatini ilovaning turiga va ish siklining davomiyligiga bog'liq ravishda uzaytirishga erishiladi, binobarin, uzatishda tok 15...30 mA, kutish rejimida 2 mA dan kamni tashkil etadi. Natijada javob ta'siri bo'yicha kechikish shunchalik kichikki, inson xonaga kirishi bilan va ZigBee simsiz aloqa qayta ulagichni bosishi bilan, hatto yoritish deyarli oniy paydo bo'lganligini sezmaydi, shu bilan bir vaqtda bunda qurilmalarni tarmog'iga ulanishida kechikish 3 sekundni tashkil etadi.

Past tezlikli ma'lumotlarni simsiz uzatish tarmoqlari (WPAN) uchun IEEE 802.15.4 standarti PHY fizik daraja va MAS muhitga ulanish darajasini aniqlaydi. PHY fizik daraja radiosignalni tarqalishi fizik muhitga ulanishni ta'minlaydi, modulyatsiya turi, tezlik va signalning boshqa parametrlarini beradi, to'g'ridan-to'g'ri qabullash va uzatishni amalga oshiradi.

MAS darajasi tarmoqqa qurilmalarni qo'shish va ularni chiqarishni amalga oshiradi, ma'lumotlar paketlarini yetkazilishini nazorat qiladi, ma'lumotlarni olinishini avtomatik tasdiqlanishini ta'minlaydi, uzatish kanaliga ulanish mexanizmlarini amalga oshiradi, 128-bitli AES- shifrlash va boshqa funksiyalarni qo'llaydi. ZigBee steki spetsifikatsiyasi tarmoq darajasi, xavfsizlik va ulanish darajalarini aniqlaydi va qurilmalarning moslashuvchanligini ta'minlash uchun 802.15.4 standart asosidagi yechimlar bilan birga ishlatilishi mumkin. PHY-darajaning asosiy funksiyalari energiya va aloqa sifatini nazorat qilish va kanallarni tahlil qilishni o'z ichiga oladi. Muhitga ulanish ISM (Industrial, Scientific and Medical) chastotalar diapazonida amalga oshiriladi, fizik daraja 868/915 MHzs chastotalarda ikkilik fazaviy modulyatsiyalashni (BPSK) va 2,4 GHzs chastotada surilishli fazaviy manipulyatsiyalashni (O-PSK) ishlatadi. Kanalga ulanish uchun muhitga tashuvchini nazorat qilishli va kolliziyalarni oldini olishli ko'p tomonlama ulanish mexanizmi (CSMA-CA) ishlatiladi. Aloqa kanalining holatini aniqlashga asoslangan bu mexanizm uzatishni boshlashdan oldin bir necha qurilmalar orqali bir vaqtda ma'lumotlarni uzatilishi keltirib chiqaradigan to'qnashuvlarni sezilarli qisqartirishga imkon beradi.

802.15.4 standarti ma'lumotlarni yarim dupleks uzatilishiga (qurilma ma'lumotlarni uzatishi yoki qabul qilishi mumkin) asoslangan, bu CSMA-CA usulini faqat kolliziyalarni aniqlash uchun emas, balki ularni oldini olish uchun ishlatishga imkon beradi. Signalning tarqalishi masofasi odatda 30 ... 50 metrlarni tashkil etadi, lekin tashqi quvvat kuchaytirgichlari, kam shovqinli kuchaytirgichlar va moslashtirilgan antennalar ishlatilganida masofa tezlikdagi sezilarsiz yo'qotishlarsiz 100 metrlargacha yetishi mumkin. O'tkazish qobiliyati to'g'ridan-to'g'ri tanlangan chastotaga bog'liq bo'ladi. 250 Kbit/sga teng maksimal uzatish tezligiga 2,4 GGs (5 MGsdan qadamli 16 ta kanallar) diapazonda erishiladi. 868 MGs (1 kanal) va 902 — 928 MGs (2 MGsdan qadamli 10 ta kanallar) chastotalar uchun ma'lumotlarni uzatish tezligi mos ravishda 20 Kbit/s va 40 Kbit/s larga teng. 6.1-rasmda 802.15.4 standartning qisqacha xarakteristikasi keltirilgan.



6.1- rasm. 802.15.4 standartning qisqacha xarakteristikasi

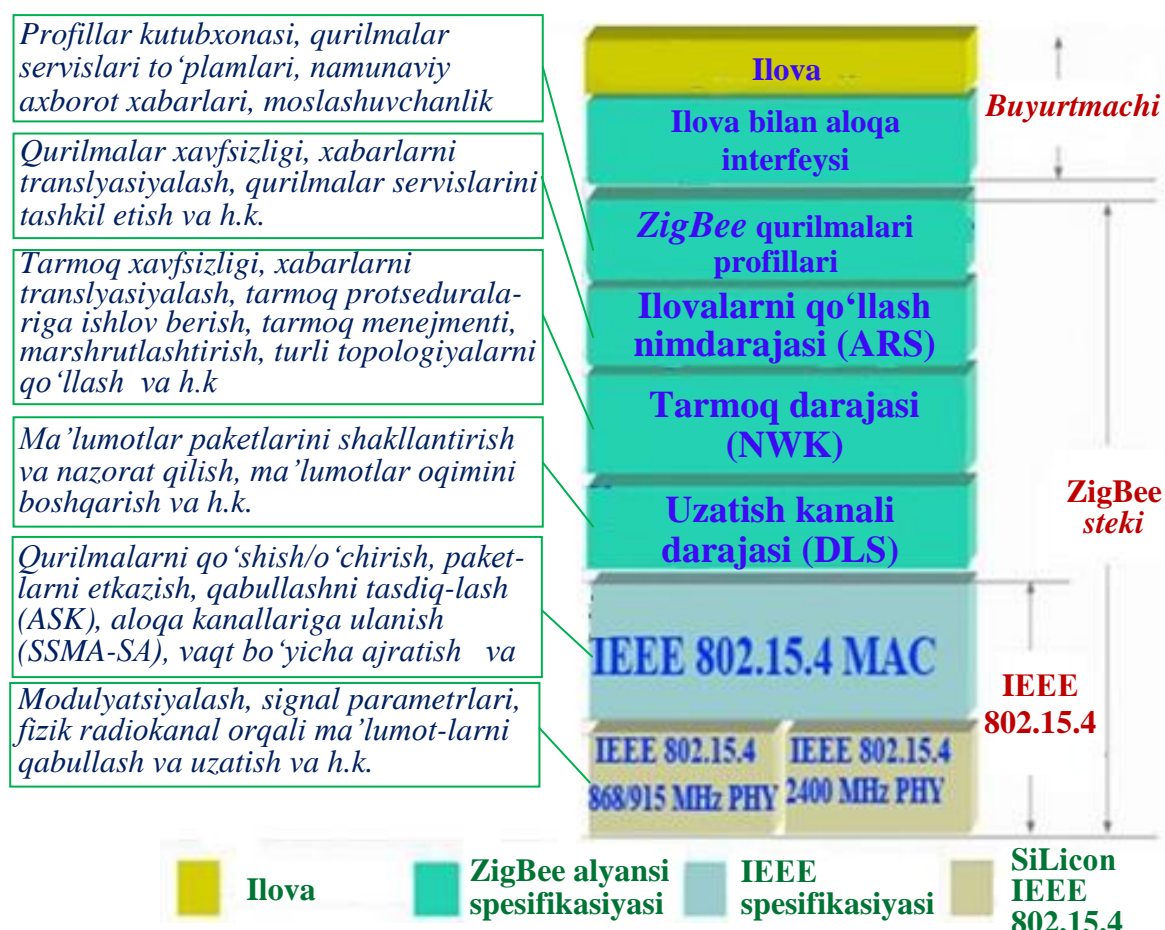
Tarmoq protokoli arxitekturasi

IEEE 802.15.4 hujjati chastotalar, apparatli o'ziga xosliklar va tarmoqning boshqa parametrlarini tavsiflaydi, shu bilan bir vaqtda ZigBee hujjati tarmoq boshqarish jarayoni, xavfsizlik parametrlari,

shuning muhim qurilmalarning moslashuvchanligi va profillari tushunchalariga ega [4].

IEEE 802.15.4-2006 tarmoqlarining o'ziga xos xususiyati deyarli istalgan topologiyani, shu jumladan, sotali topologiyani ishlatish imkoniyati hisoblanadi.

ZigBee protokllar steki OSI (Open System Interconnection) ochiq tizimlardagi ierarxik yetti darajali ma'lumotlarni uzatish protokollari modeli prinsipi bo'yicha qurilgan. Stek ZigBee alyansi spetsifikatsiyasidan aniqlangan aloqa kanalini ishlatilishiga javob beradigan IEEE 802.15.4 standarti darajalari va dasturiy tarmoq darajalari va ilovalarni qo'llash darajalarini o'z ichiga oladi (6.2-rasm).



6.2- rasm. ZigBee/802.15.4 steki arxitekturasi

IEEE 802.15.4 arxitekturasi o'z navbatida, standartni soddalashtiradigan qator darajalarni o'z ichiga oladi. Har bir daraja standartning bir qismiga javobgar va yuqorida joylashgan darajaga xizmat ko'rsatadi.

Darajalar orasidagi interfeyslar bu standartda tavsiflangan mantiqiy aloqalarni aniqlaydi.

IEEE Std 802.15.4 hujjati portativ ko'chma qurilmalarli va 10 metrga teng maksimal POS (Personal Operating Space) yetish masofasili simsiz muhit uchun fizik daraja (PHY) va MAC (Medium Access Control) tarmoq muhitiga ulanib nimdarajasi spetsifikatsiyalarini aniqlaydi. Bunda pastroq uzatish tezliklarida katta masofalarda (< 100 m) ishlash ham mumkin bo'ladi.

Stekning fizik darajasi

PHY fizik daraja ikkita turdagi xizmatlarni taqdim etadi:

- PHY axborot servisi;
- Boshqarish servisi, u SAP ulanish nuqtasi (PLME-SAP nomi orqali ma'lum bo'lgan) PLME servis (Physical Layer Management Entity) bilan o'zaro ta'sirlashishni ta'minlaydi.

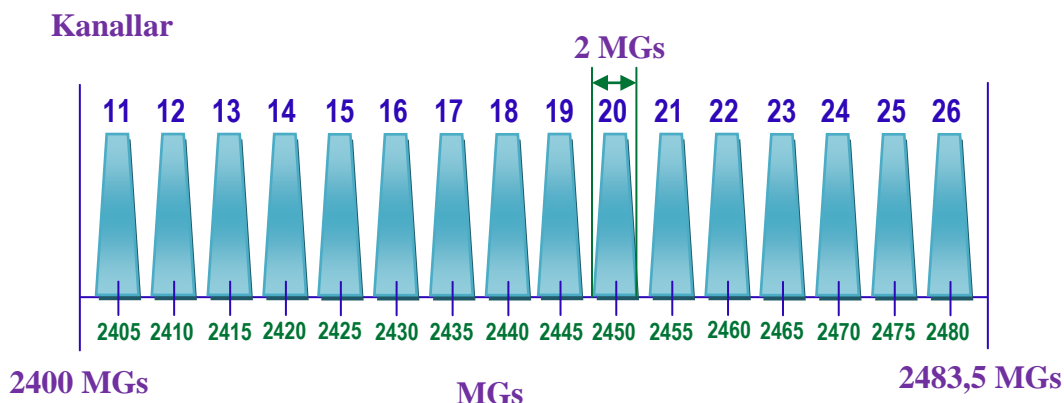
PHY axborot servisi PPDU (Protocol Data Unit) ma'lumotlar protokollari bloklari radiokanali orqali uzatish va qabullashni mumkin qiladi.

Standart 250 kbit/c, 100kbit/c, 40 kbit/c va 20 kbit/c ma'lumotlarni uzatish tezliklarini aniqlaydi. Radiokanal bo'yicha ma'lumotlarni qabul qilish va uzatish ishchi chastotalar diapazoni, modulyatsiyalash turi, maksimal tezlik, kanallar sonini aniqlaydigan PHY fizik darajada amalga oshiriladi: O-QPSK — 2,4 GGs (16 kanallar, 250 Kbit/s) diapazon uchun surilishli kvadratik fazaviy manipulyatsiyalash, BPSK — 915 MGs (10 kanallar, 40 Kbit/s) va 868 MGs (1 kanal, 20 Kbit/s) chastotalar uchun ikkilik fazaviy manipulyatsiyalash. PHY darajasi qabullagich-uzatkichni aktivlashtirish/noaktivlashtirish, ishchi kanalda qabul qilingan signal energiyasini detektorlash, fizik chastota kanalini tanlash, ma'lumotlar paketini olishda signal sifatini indikatsiyalash va CSMA-CA protokolini (tashuvchi nazorat qilinadigan va kolliziyalarni oldi olinadigan muhitga ko'p tomonlama ulanish protokoli) ishlatilishi uchun bo'sh kanalni baholashni amalga oshiradi. Tushunish muhimki, 802.15.4 standarti bu fizik radio (radioqobullagich-uzatkich mikrosxemasi), ZigBee esa bu xavfsizlik va marshrutlashtirish funksiyalarini ta'minlaydigan mantiqiy tarmoq va dasturiy stek hisoblanadi [2].

Radioqurilmalar quyidagi litsenziyalanmaydigan chastotalar diapazonlaridan birida ishlaydi (6.3-rasm):

- 868–868.6 MGs (masalan, Yevropa uchun)

- 902–928 MGs (SHimoliy Amerika uchun)
- 2400–2483.5 MGs (qolgan dunyo uchun)



6.3- rasm. IEEE 803.15.4 standartda radiokanallarni tanlash (PHY 2400 MGs).

Stekning MAC darajasi

MAC subdarajasi ikkita servislarni taqdim etadi:

- axborot MAC-servisi;
- MAC-daraja boshqarish servisi, ulanish nuqtalari uchun (MLME-SAP sifatida ma'lum bo'lgan) MLME (MAC Level Management Entity) boshqarish subdarajasi uchun interfeysni ta'minlash.

MAC axborot servisi fizik daraja axborot servisi yordamida MAC-daraja ma'lumotlar protokollari (MPDU) qabul qilinishi va uzatilishini ta'minlaydi.

MAC subdarajasining xarakterli o'ziga xos xususiyatlari mayoqlarni (beacon) boshqarishdan foydalanish, ulanishni amalga oshirish, GTS (Guaranteed Time Slot) boshqarish, kadrlarning to'g'riligini tekshirish, kadrlarning yetkazilishini tasdiqlash va boshqalar ishlatiladi. Bundan tashqari, MAC subdarajasi amaliy darajada xavfsizlik mexanizmlarini qo'llashni ta'minlaydi.

Bu standart superkadr tuzilmasining ishlatilishiga opsional ruxsat etadi. Superkadrning formati koordinator orqali aniqlanadi. Superkadr koordinator jo'natadigan tarmoq mayoqlari (beacon) orqali cheklangan (5.22-rasmga qarang) va davomiyligi bo'yicha teng 16 ta domenlardan tashkil topgan. Superkadr opsional ravishda aktiv va passiv seksiyalarga ega bo'lishi mumkin. Noaktiv davrda koordinator ta'minotni tejimli sarflash rejimiga o'tishi mumkin. Kadr-mayoq har

bir superkadrning birinchi domenida uzatiladi. Agar koordinator superkadrni tuzilmasidan foydalanishni istamasa, u mayoqlarni uzatilishini uzadi. Mayoqlar PANni identifikatsiyalash va superkadr tuzilmasini tavsiflash uchun ulangan qurilmalarni sinxronlashtirish uchun kerak bo‘ladi. Ikkita mayoqlar orasida CAP (Contention Access Period) davrda ma’lumotlarni almashlashni amalga oshirishni istaydigan istalgan qurilma bu huquq uchun CSMA-CA domen mexanizmini ishlatadigan boshqa qurilmalar bilan raqobatlashadi. Barcha almashlar navbatdagi tarmoq mayog‘i momentigacha yakunlanadi [21].

MAC daraja xarakteristikalar:

- 64-bitli IEEE manzillashtirish, lokal tarmoqlar ichida 16-bitli manzillashtirish (nazariy jihatdan tarmoqdagi maksimal qurilmalar soni 264 ta).

Manzillashtirish usullari:

- identifikatorlar: tarmoq ID + ID qurilmalar (“Yulduz” topologiyasi);

- Jo‘natuvchi/Oluvchi identifikatori (teng huquqli tugunlar orasida uzatish);

- Tarmoqni avtomatik/yarim avtomatik tashkil etilishiga kirish/undan chiqish

- ZigBee tarmog‘i xabarlar paketlari formati, ma’lumotlar bitta paketning maksimal foydali yuklanishi 104 ma’lumotlar baytini tashkil etadi, kadrning maksimal uzunligi 127 baytga teng;

- xavfsizlik darajasi:

- tarmoqqa erkin ulanish;

- ulanishni nazorat qilish ro‘yxati;

- uzatishda kechikishni aniqlash taymerlari va ma’lumotlar paketlarining dolzarbligi;

- 128-bitli simmetrik AES kalitdan foydalanish bilan shifrlash;

- tarmoqqa ulanish mexanizmlari, vaqt bo‘yicha bo‘lish va kafolatlangan vaqt intervallari funksiyalari, CSMA-CA protokoli orqali kanalga ulanish;

- tarmoq topologiyalarini, shu jumladan “nuqta-nuqta”, “yulduz”, ko‘p yacheykali va klasterli ulanishdagi topologiyalarni qo‘llash;

- ma’lumotlar paketlarini kelganligi haqida ogohlantirish, qabullashni tasdiqlash (ACK), 16-bitli xatoliklarni nazorat qilish (CRC);

- paketli/oqimli uzatish rejimlari [21].

6.4. Zigbee tarmog‘ini qurish va ishlash prinsipi

Zigbee texnologiyasiga muvofiq simsiz uzatish tarmoqlari bir necha sinflardagi qurilmalar - to‘liq funksional marshrutizatorlar (Full function device - FFD), koordinator-qurilmalar (Coordinators — FFD, tarmoqning murakkabligiga bog‘liq ravishda qo‘shimcha tizim resurslarili) va cheklangan funkionallikli qurilmalarni (Reduced function device - RDD) o‘z tarkibiga oladi [21].

Qurilma topologiyani qurish bo‘yicha keng imkoniyatlarni ta‘minlaydi, tarmoq ishi koordinatori (radiotarmoq bosh stansiyasi) rolini bajarishi mumkin va tarmoqning istalgan boshqa stansiyasi bilan xabarlarini almashlashi mumkin. Ikkinchi turdagi qurilmalar faqat yulduzsimon shakldagi tarmoqda ishlashi mumkin, ma‘lumotlarni almashlash tarmog‘ining ishlashini koordinatsiyalash funksiyasini bajara olmaydi va soddalashtirilgan konstruksiyaga ega. Dastlab qurilmalar yagona tarmoqda ishlaganida ularning imkoniyatlari tengsizligi texnologiyasi g‘oyasiga qo‘yilgan oxirgi xususiyat, aynan ularning o‘ta past energiya iste‘molini ta‘minlashga imkon beradi.

Har bir ZigBee lokal tarmoqda faqat bitta koordinator-qurilma bo‘ladi. Koordinatorning asosiy vazifasi tarmoq parametrlarini o‘rnatish va yaratish, asosiy radiochastota kanalini tanlash, noyob tarmoq identifikatorini berishdan iborat. Bunda koordinator uchta turlardagi qurilmalardan eng murakkabi hisoblanadi, eng katta xotira hajmiga va oshirilgan energiya iste‘moliga (tarmoqdan ta‘minlanadi) ega bo‘ladi. Marshrutizatorlar tarmoqning ishlash radiusini kengaytirish uchun ishlatiladi, chunki bir-birlaridan uzoqda joylashgan qurilmalar orasida retranslyatorlar funksiyalarini bajara oladi. Qurilma istalgan ZigBee tarmoq topologiyasini qo‘llaydi, koordinator funksiyasini bajarishi va tarmoqni barcha tugunlariga (FFD va RFD) murojaat qilishi mumkin.

Cheklangan funksiyalar to‘plamli qurilmalar marshrutlashtirishda qatnashmaydi, koordinator funksiyasini bajara olmaydi, faqat lokal tarmoq koordinatoriga (FFD qurilmaga) murojaat qiladi, “nuqta-nuqta” va “yulduz” turdagi bog‘lanishni qo‘llaydi, oxirgi tarmoq qurilmalari rolini o‘ynaydi. Amalda tarmoqdagi ko‘pchilik tugunlar RFD-qurilmalar hisoblanadi, FFD-qurilmalar va koordinatorlarning

qoʻllanilishi esa aloqa koʻpriklari va mos tarmoq topologiyasini hosil qilish uchun zarur boʻladi.

Marshrutizatorlar va boshqa qurilmalar tarmoqqa ulanishi bilanoq, ular koordinatordan yoki tarmoqda ishlayotgan istalgan marshrutizatoridan tarmoq haqidagi maʼlumotlarni oladi va bu maʼlumotlar asosida oʻz operatsion parametrlarini tarmoq xarakteristikalariga muvofiq oʻrnatadi. ZigBee marshrutizatorlari ular tarmoqqa ulangan oxirgi qurilmalar orasida taqsimlaydigan tarmoq manzillari jadvalini oladi.

FFD qurilmasi marshrutlashtirish haqidagi qarorlarni qabul qilishda daraxtsimon manzillashtirishni ishlatadi. Marshrutlashtirishning samaradorligini oshirish uchun ZigBee algoritmi FFD-qurilmalarga qisqartirilgan manzillashtirishdan foydalanishga imkon beradi. Qisqartirishdan foydalanish koʻzda tutiladigan har bir marshrutizator DN turdagi juftliklarga ega boʻlgan jadvalni qoʻllashi kerak, bu yerda D – joʻnatish manzili, N – bu joʻnatish manziliga yoʻlda keyingi qurilmaning manzili. Daraxtsimon prinsip va jadval asosidagi marshrutlashtirish birligi ishlashning tez moslashuvchanligini bildiradi va ishlab chiquvchilarga optimal narx/unumdorlik nisbatini tanlashga imkon beradi [21].

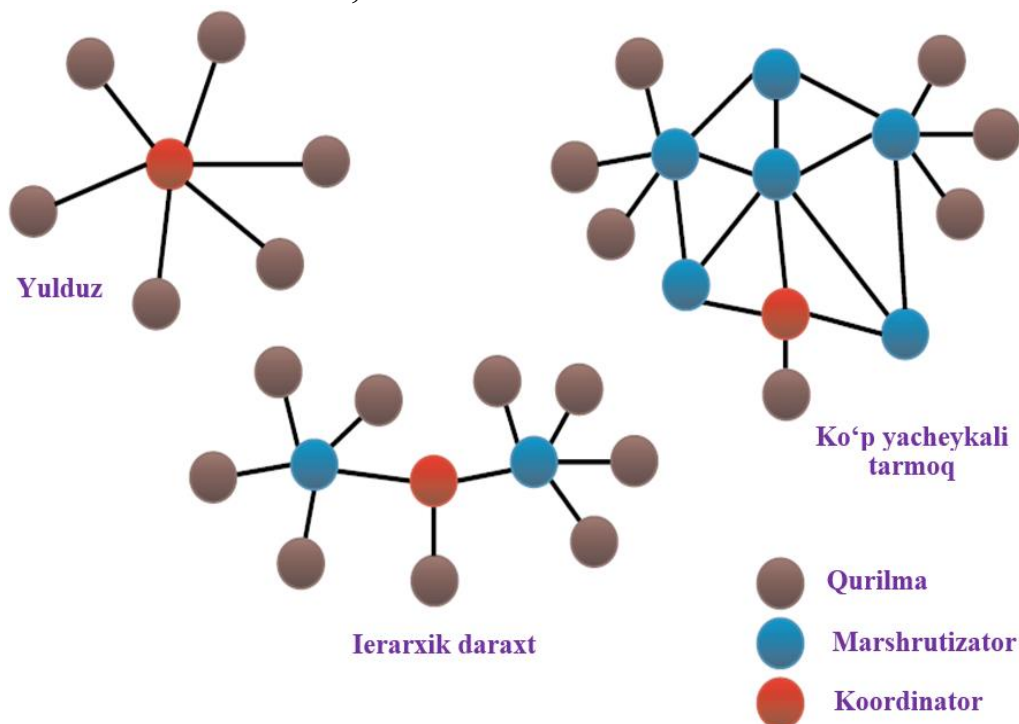
ZigBee steki tarmoqning turli topologiyalarini, shu jumladan “nuqta-nuqta”, “klasterli (ierarxik) daraxt” va “koʻp yacheykali tarmoq” topologiyalarini qoʻllaydi (6.4-rasm). Stekning tarmoq funksiyalari aktiv kanallarni aniqlash uchun tarmoqni skanerlash, aktiv kanallarda qurilmalarni identifikatsiyalash, ishlatilmayotgan kanallarda tarmoqni yaratish va personal simsiz tarmoq zonasida mavjud tarmoq bilan birlashtirish, qurilmalarning aniqlangan profillariga muvofiq qoʻllanadigan servislarni aniqlash, marshrutlashtirishni oʻz ichiga oladi. Bu qurilmalarga tarmoqqa avtomatik kirishga va undan chiqishga, har bir tugunga bir necha marshrutlarni borligi hisobiga “bitta nuqtadagi uzilishning” keraksiz oqibatlarini yoʻqotishga imkon beradi.

Turiga bogʻliq ravishda har bir qurilma maʼlum tarmoq funksiyalariga ega:

– koordinator tarmoqni skanerlaydi va tarmoqni tashkil etish uchun boʻsh kanallarni aniqlaydi;

marshrutizator (FFD) tarmoqni skanerlaydi va aktiv kanallarni topadi va mavjud tarmoq tarkibiga kirishga harakat qiladi yoki agar aktiv kanallar boʻlmasa yoki aktiv tarmoq bilan birlashish amalga

o'shmasa, koordinator huquqlarida o'z personal tarmog'ini yaratadi. Agar birlashish bo'lib o'tsa, mavjud tarmoq qoidalariga muvofiq lokal tarmoqqa tutashgan koordinator marshrutizator darajasiga o'tkaziladi va lokal tarmoq haqidagi barcha ma'lumotlarni mavjud tarmoq koordinatoriga uzatadi. Koordinatoridan sinxronlashtirish signal paketidan yangi hosil bo'lgan marshrutizator keyingi signallar paketlarini aniqlash uchun tarmoqning vaqt parametrlari haqidagi zarur ma'lumotlarni oladi;



6.4- rasm. Tarmoqlar topologiyalari variantlari

– oxirgi RFD qurilma doimo mavjud tarmoqqa kirishga urinadi; “Klasterli daraxt” topologiyasi infratuzilmaga qo‘shimcha xarajatlarni talab qilmasligi bilan tarmoqning masshtablanuvchanligi va qamrab olish zonasini kengaytirilishini ta’minlaydi. “Klasterli daraxt” turdagi tarmoq “yulduz” topologiyali va cheklangan funksiyalarli qurilmalarli (RFD) bir necha nimtarmoqlarni o‘z ichiga olishi mumkin. “Klasterli daraxt” va “yulduz” turlardagi topologiyalar bilan birga ZigBee texnologiyasi tarmoqlarning ko‘p yacheykali qurilishi prinsipini qo‘llaydi. Bunday topologiyada istalgan tarmoq tuguni tarmoqdagi boshqa qurilmalar uchun marshrutizator funksiyasini ham bajarishi mumkin.

Agar bitta tugundan boshqa tugunga signal yo‘lida to‘siq (beton yoki metall to‘siq va h.k.) vujudga kelsa, ma’lumotlarni manzilga

uzatish uchun muqobil marshrut tanlanadi. Tarmoq tugunlarining zich konsentratsiyasi yanada himoyalangan, ishonchli tizimga olib keladi. Agar tugunlardan biri ishdan chiqsa, marshrut avtomatik ravishda tarmoqning boshqa tugunlari orqali aniqlanadi va natijada tarmoq o'z-o'zidan tiklanadigan bo'lib qoladi.

Lekin ko'p yacheykali tarmoqda avtonom ta'minot manbalarining xizmat muddatlari sinxronlashtirilgan ulanish usulining qo'llanilishi hisobiga kamayadi, uzatish kanallarini aniqlanishi murakkabligi ortadi va tarmoq tugunlariga xabarlarini har bir qayta uzatishda kechikish (o'nlab millisekund) bo'lib o'tadi.

Ko'p yacheykali tarmoqning barcha tugunlari boshqa tugunlarni aniqlay oladi va bir-birlarini tanish bilan paketlarni optimal uzatish yo'lini, maksimal almashlash tezligini, xatoliklarni vujudga kelishi chastotasi va kutish vaqtini hisoblay oladi. Hisoblangan qiymatlar qo'shni tugunlarga uzatiladi, trafikni uzatilishi optimal yo'li esa qabul qilinadigan signallarning quvvatidan kelib chiqish bilan tanlanadi.

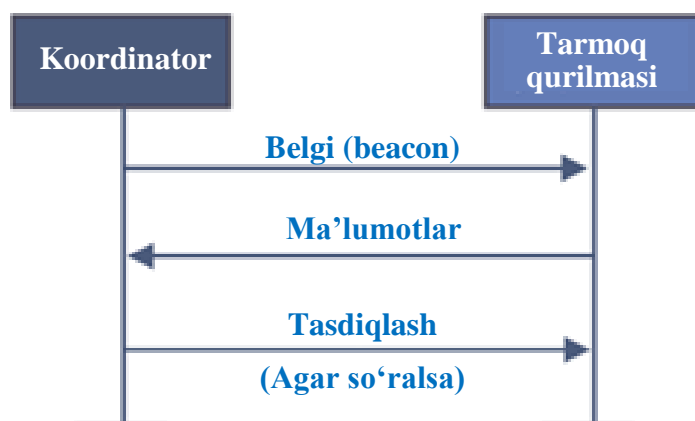
Tugunlarni aniqlash va yo'lni tanlash jarayonlar doimo boradi, shuning uchun har bir tugun qo'shnilarning joriy ro'yxatini qo'llaydi va ularning joylashishi o'zgarganida eng yaxshi marshrutni tezkor aniqlashi mumkin. Agar qandaydir tugun tarmoqdan olinsa (texnik xizmat ko'rsatish uchun yoki buzilishi tufayli), qo'shni tugunlar o'z jadvallari konfiguratsiyalarini tezda o'zgartiradi va yangidan trafik oqimlari marshrutlarini aniqlaydi. Bu o'z-o'zidan qayta tiklanish va buzilishlarni chetlab o'tish xossasi yacheykali topologiyani qat'iy arxitekturali tarmoqlardan sezilarli ajratib turadi [21].

Uchta turlardagi ma'lumotlarni uzatish tranzaksiyalari mavjud. Ulardan biri tarmoq qurilmasi ma'lumotlarni uzatadigan koordinatorga ma'lumotlarni uzatish bilan uyg'unlashtirilgan. Ikkinchi tranzaksiya koordinatoridan tarmoqqa ma'lumotlarni qayta uzatishga bog'langan. Uchinchi turdagi tranzaksiyalarga to'g'ridan-to'g'ri tarmoqlar orasida ma'lumotlarni almashlash kiradi. Yulduz topologiyasida faqat ikkita tranzaksiyalar ishlatiladi, chunki faqat koordinator va tarmoq qurilmasi orasidagi axborot almashinuvi bo'lishi mumkin. P2P topologiyasida uchta turdagi tranzaksiyalar turlari bo'lishi mumkin.

Almashlashlar har bir turi mexanizmi tarmoq mayoqlarni uzatilishini qo'llashiga bog'liq bo'ladi. Mayoqlar qo'llanadigan PAN tarmoqlari sinxronlashtirish talab qilinadigan yoki RS periferiyasi kabi kichik javob ta'siri kechikishini talab qiladigan tarmoq qurilmalari

qoʻllanadigan tarmoqlarda ishlatiladi. Agar tarmoqning sinxronlashtirish yoki kichik kechikishlarga ehtiyoji boʻlsa, u standart almashlashlar uchun mayoqlar-kadrlardan foydalanmasligi mumkin. Lekin mayoqlar istalgan holda tarmoqning qayta tiklanishi uchun zarur boʻladi.

Tarmoq qurilmasi mayoqlar-kadrlar qoʻllanadigan PAN tarmogʻida koordinatorga maʼlumotlarni uzatishni istaganida u dastlab mayoq-kadrni (beacon) detektorlashga urinadi. Mayoq aniqlanganida, qurilma superkadrning tuzilmasi bilan sinxronlashadi. Mos vaqt momentida qurilma CSMA-CA domen algoritmidan foydalanish bilan oʻz axborot kadrini koordinatorga uzatadi. Koordinator tasdiqlash kadrini joʻnatish yoʻli bilan muvaffaqiyatli yetkazishni opsional tasdiqlashi mumkin. Bu amallar ketma-ketligi 6.5-rasmda tasvirlangan.

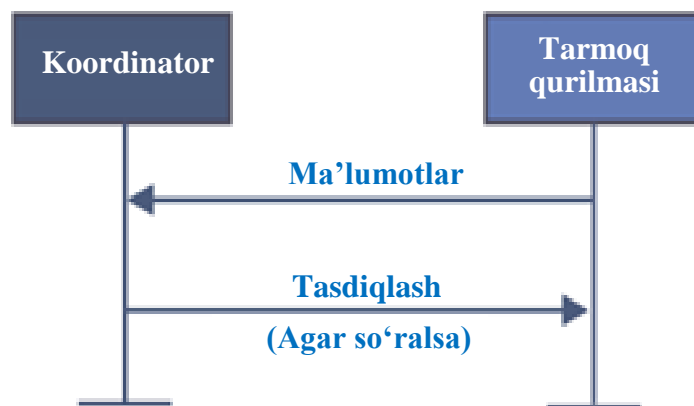


6.5- rasm. Mayoqlardan (beacon) foydalaniladigan PAN tarmoqda koordinatorga maʼlumotlarni uzatish

Tarmoq qurilmasi mayoqlardan (beacon) foydalanilmaydigan PAN tarmoqda maʼlumotlarni uzatishni istasa, u domensiz CSMA-CA sxemasidan foydalanish bilan oddiy axborot kadrini koordinatorga uzatadi. Koordinator tasdiqlash kadrini joʻnatish bilan muvaffaqiyatli yetkazishni opsional tasdiqlaydi. Bu amallar ketma-ketligi 6.6-rasmda tasvirlangan.

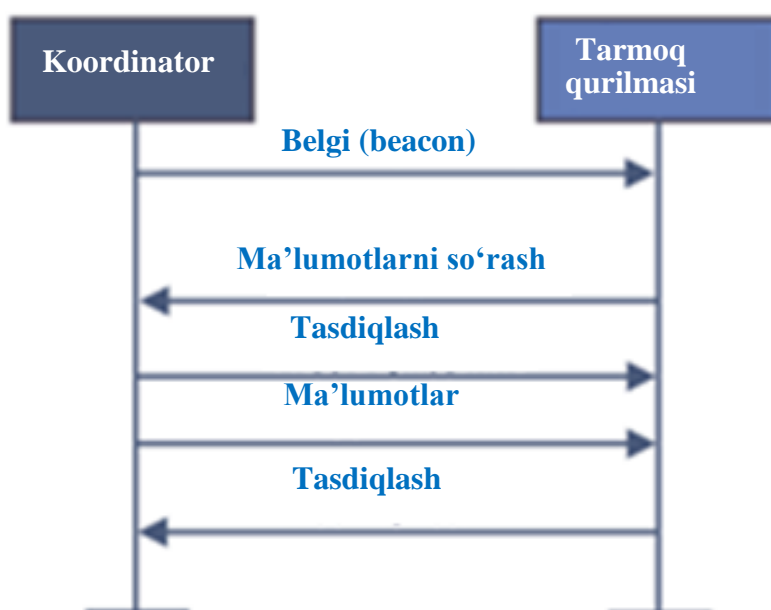
Koordinator mayoqlardan (beacon) foydalanilmaydigan PAN tarmoqda tarmoq qurilmasiga maʼlumotlarni uzatishni istaganida, u tarmoq mayogʻi boʻyicha qaysi maʼlumotlar joʻnatishni kutayotganligini aniqlaydi. Qurilma davriy ravishda tarmoq mayoqlarini (beacon) eshitadi va agar joʻnatishni kutayotgan xabar

bo'lsa, CSMA-CA domen mexanizmidan foydalaniladigan ma'lumotlarni so'rash MAS-komandasi uzatiladi. Koordinator mos kadr (ASK) yordamida ma'lumotlar so'rovini olinishini tasdiqlaydi. CSMA-CA domen mexanizmidan foydalanish bilan jo'natishni kutayotgan kadr, agar mumkin bo'lsa, u holda tasdiqlashdan keyin qayta uzatiladi.



6.6- rasm. Mayoqlardan (beacon) foydalanilmaydigan PAN tarmoqda koordinator bilan kommunikatsiyalar

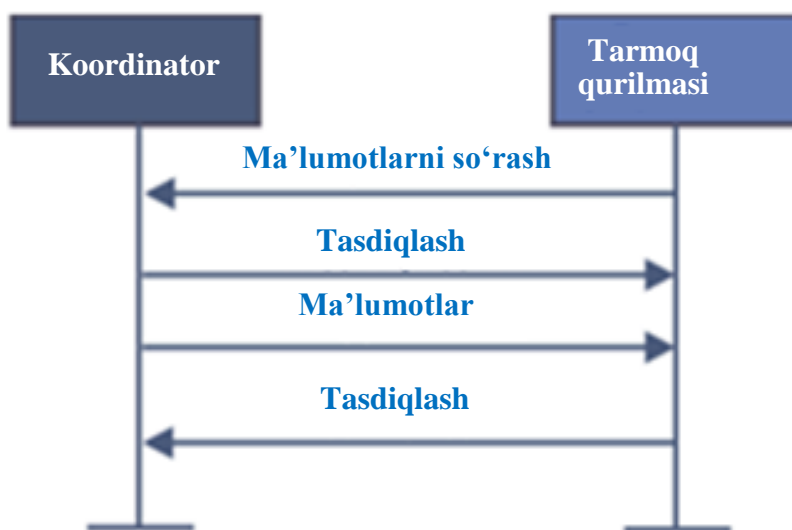
Qurilma tasdiqlash kadrini jo'natish yo'li bilan ma'lumotlarni muvaffaqiyatli olinishini tasdiqlashi mumkin. Bu bilan tranzaksiya yakunlanadi. Tranzaksiya muvaffaqiyatli yakunlanganida xabar mayoqda yozilgan jo'natishni kutayotganlar ro'yxatidan o'chiriladi. Tavsiflangan amallar ketma-ketligi 6.7- rasmda tasvirlangan.



6.7- rasm. Mayoqdan foydalaniladigan PAN tarmoqda kommunikatoridan ma'lumotlarni uzatish

Koordinator mayoqlardan (beacon) qo‘llanmaydigan PAN tarmoqda tarmoq qurilmasiga ma’lumotlarni uzatishni istaganida, u mos qurilmalar uchun ma’lumotlarni xotirada saqlaydi va ma’lumotlarni so‘rashni bajaradi. Tarmoq qurilmasi ilovada berilgan almashlash tezligida domensiz CSMA-CA mexanizmidan foydalanish bilan ma’lumotlarni so‘rash MAC-komandasini jo‘natish yo‘li orqali koordinator bilan aloqani o‘rnatishi mumkin.

Koordinator tasdiqlash kadri yordamida axborot so‘rovini muvaffaqiyatli tasdiqlaydi. Agar axborot kadri jo‘natishni kutayotgan bo‘lsa, koordinator domensiz CSMA-CA mexanizmidan foydalanish bilan qurilmaga ma’lumotlar kadrini uzatadi. Agar jo‘natishni kutayotgan ma’lumotlar kadri bo‘lmasa, koordinator buni ma’lumotlar so‘rovidan keyin keladigan tasdiqlash paketida yoki nol uzunlikli ma’lumotlar maydoni bilan axborot kadrida qayd etadi. Agar kerak bo‘lsa, qurilma ma’lumotlar kadrini muvaffaqiyatli olinganligini tasdiqlaydi. Bu sxema uchun amallar ketma-ketligi 6.8-rasmda tasvirlangan [21].



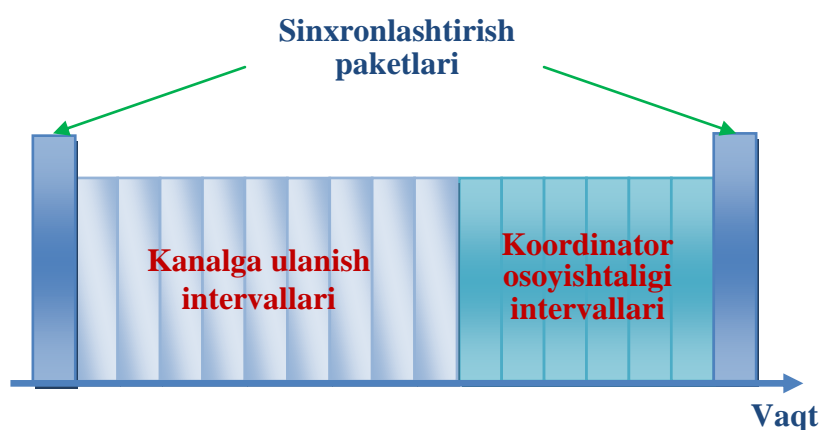
6.8- rasm. Mayoqlarsiz PAN tarmoqda koordinatoridan telekommunikatsiyalar

Energiya iste'molini optimallashtirish ZigBee tarmoqlarni qurishda ustuvor masala hisoblanadi. Bu masalaning yechimlaridan biri faqat ma’lumotlar kelganida ularni uzatish va manzil tomonidan paketni muvaffaqiyatli qabul qilinganligida tasdiqlashni keyingi kutishga asoslangan aloqa strategiyasi hisoblanadi. Bunda har bir qurilma istalgan momentda uzatishni uyushtirishi mumkin.

Bu usulning ma'lum kamchiligi bir necha qurilmalar ma'lumotlarni bir vaqtda uzatishida interferensiya ehtimolligi hisoblanadi. Lekin ustma-ust tushish imkoniyati qurilmaning o'ta kichik aktivligi sikli davomiyligi, uzatish momentining tasodifiyligi va uzatiladigan ma'lumotlarning uncha katta bo'lmagan hajmi tufayli minimumga keltiriladi.

Bog'lanishning ishonchligi CSMA-CA protokolidan foydalanish hisobiga ortadi. Oddiy ko'p tomonlama ulanish strategiyasi faqat "nuqta-nuqta" yoki "yulduz" turdagi bog'lanishlarga qo'llanilsa bo'ladi. U barcha ilovalarga ham to'g'ri kelavermaydi. Keraksiz o'zaro ta'sirlashishning oldini olish uchun vaqt bo'yicha ajratishli ko'p tomonlama ulanish (TDMA) protokolini qo'llash mumkin.

ZigBee/802.15.4 texnologiyasi TDMA texnologiyasiga o'xshash prinsip bo'yicha vaqt intervallarini kafolatlaydi, lekin bu ajratishning ishlatilishi faqat sinxronlashtirish va vaqt bo'yicha ajratish birga bo'lganda mumkin bo'ladi, bu yanada murakkab va oddiy TDMA-ulanishga qaraganda kam energiya samaradorligi algoritmi hisoblanadi. ZigBee vaqt bo'yicha ajratish sinxronlashtirish rejimidan foydalanishga asoslanadi, bunda bo'ysunvchi tarmoq qurilmalari vaqtni katta qismida "kutish" holatida bo'ladi, tarmoq koordinatoridan sinxronlashtirish signalini qabul qilish uchun davriy ravishda aktivlashadi, bu lokal tarmoq yacheykasi ichidagi qurilmalarga vaqtning qaysi momentida ma'lumotlarni uzatishni amalga oshirish kerakligini bilishga imkon beradi.



6.9- rasm. ZigBee tarmoqqa sinxronlashtirilgan ulanish

Koordinator almashlashni boshqaradi, kanallarni ajratadi va 15 ms ... 252 sgacha intervalli chaqiruvlarni amalga oshiradi. Signallar paketlarini uzatish o'tkazish qobiliyatini aniqlaydi, ulanish navbatini

kutish kichik vaqtini va har birida kolliziyalar yo‘qotilgan bir xil uzunlikdagi 16 ta vaqt intervallarini ajratilishini ta‘minlaydi.

Tarmoq tugunlaridan har biri uchun ulanish vaqt intervali koordinator yoki CSMA-CA mexanizmi orqali aniqlanadi. Osoyishtalik intervallari avtonom ta‘minot manbaidan ishlashda tarmoq koordinatorining energiyani tejash rejimlarini ishlatilishi uchun zarur bo‘ladi.

Kamchiligi bu sinxronlashtirish signalini kutish holati uncha katta bo‘lmagan vaqt bo‘yicha mos kelmasliklar tufayli energiya iste‘molini sezilarsiz ortishiga olib kelishi hisoblanadi, bu signalni o‘tkazib yubormaslik uchun qurilmani ancha oldin aktivlashishga majburlaydi. Sinxronlashtirilgan ulanish funksiyasi “klasterli daraxt” va “ko‘p yacheykali tarmoq” kabi kengaytirilgan topologiyali tarmoqlarda qo‘llaniladi [21].

6.3- jadvalda oddiy ko‘p tomonlama ulanish va sinxronlashtirish funksiyasili ulanish hollari uchun koordinator va tarmoq tuguni orasidagi ma‘lumotlarni qayta uzatishdagi farqlar keltirilgan. Standart ko‘p tomonlama ulanish xavfsizlik va binolarni qo‘riqlash tizimlarida turli xil xabarlagichlarni (suqulib kirish, harakat, tutun va h.k.) tashkil etishda o‘z o‘rniga ega bo‘lishi mumkin.

6.3- jadval

Tarmoqqa ulanish ikkita strategiyalari uchun qayta uzatishlar protokollari

Ma‘lumotlarni uzatish yo‘nalishi	Sinxronlashtirilgan ulanish	Oddiy ko‘p tomonlama ulanish
Koordinatorga	-signal paketini kutadi -tarmoq bilan sinxronlash -ma‘lumotlarni CSMA/CA protokoli bo‘yicha ma‘lum momentda uzatish - qabullashni tasdiqlash	- CSMA/CA protokoli bo‘yicha ma‘lumotlarni paydo bo‘lishida ularni uzatilishi -qabullashni tasdiqlash
Koordinatoridan	-yangi ma‘lumotlarni borligini xabar qiladi -agar yangilari bo‘lsa, ma‘lumotlar paketini kutish, qurilma	-so‘rov bo‘lmaganida ma‘lumotlarni saqlash -CSMA/CA protokoli bo‘yicha

	CSMA/CA protokoli bo'yicha ma'lum vaqt intervalida ma'lumotlarni so'raydi -so'rovni olinishini tasdiqlash	so'rov jo'natadi -qurilmadan so'rovni olinishiga tasdiqlashni uzatadi -ma'lumotlarni qayta uzatish
--	--	---

Qo'llanilishi sharti deb tizimlarning 99,9% tartibdagi osoyishtalik holatining umumiy vaqtini, o'zining tarmoqdagi borligi haqida koordinatorga xabar qilish uchun vaqtning psevdotasodifiy momentlarida aktiv holatga o'tishni hisoblash mumkin. Xabariga oniy aktiv holatga o'tadi va trevoga signalini uzatadi. Bunda ta'minot tarmog'idan ishlaydigan koordinator doimo aktiv holatda bo'ladi va barcha oxirgi tarmoq qurilmalaridan signallarni qabul qiladi.

Sinxronlashtirilgan ulanish koordinatorga oxirgi qurilmalardan tasodifiy qayta uzatishlarning yo'qligi tufayli avtonom ta'minotga ega bo'lishga imkon beradi.

Bu holda tarmoqda qayd etish quyidagi tarzda bo'lib o'tadi:

- oxirgi qurilma ta'minot berilishi bilan mavjud ZigBee tarmog'i koordinatoridan sinxronlashtirish signalini kutadi (signalni kutish vaqt intervali - 0,015...252 s);

- koordinator bilan birlamchi ma'lumotlarni almashlash va javobni kutish;

- osoyishtalik holatiga o'tish, ZigBee tarmog'i koordinatori aniqlaydigan momentlarda aktivlashish;

- oxirgi qurilma bilan aloqa seansi tugashi bilan koordinator ham osoyishtalik holatiga o'tadi.

Bu ulanish usuli tarmoqning har bir tugunlarida vaqtni beruvchi zanjirlarning narxini sezilarsiz ortishini ko'zda tutadi. Uzoqroq osoyishtalik holati intervallari aniq vaqtni beruvchi zanjirlarning bo'lishini ko'zda tutadi, signal paketini ishonchli qabul qilish uchun aktiv holatga erta o'tish qabullash tomonining elektr energiyasi iste'molini oshiradi [21].

Nazorat savollari

1. Zigbee tarmog'ini qurish va ishlash prinsipini tushuntiring.
2. Tizimning asosiy komponentlarini tushuntiring.
3. ZigBeening o'ziga xos xususiyatini tushuntiring.

4. ZigBee aloqaning asosiy texnik parametrlarini tushuntiring.
5. Zigbee texnologiyasining tavsifini tushuntiring.
6. Zigbee tarmog‘ining qurish afzalligi bor?
7. WPAN tarmoqlarini tushuntiring
8. IEEE 802.15.4 standartlarini tushuntiring

7- BOB. BLUETOOTH TEXNOLOGIYASI

7.1. Bluetooth texnologiyasining tavsifi

Bluetooth texnologiyasi (IEEE 802.15 standarti) ma'lumotlarni uzatishning personal tarmog'ini (WPAN — Wireless Personal Network) tashkil etishga imkon beradigan birinchi texnologiya bo'ldi. Radiokanal bo'yicha litsenziyalanmagan 2,4 GGs chastotalar diapazonida uncha katta bo'lmagan masofalarga (10–100 m) ma'lumotlarni va tovushlarni uzatishni amalga oshirishga va to'g'ri ko'rinish bo'lmaganida PK, mobil telefonlar va boshqa qurilmalarni ulashga imkon beradi [23].

1994 yilda Ericsson firmasi yangi aloqa texnologiyasi - Bluetooth texnologiyasi ishlab chiqishni boshladi. Dastlab maqsadning asosi mobil telefon va simsiz garnitura orasida aloqani o'rnatishga imkon beradigan past energiya iste'mol qiladigan va uncha yuqori qimmat bo'lmagan radiointerfeysni ishlab chiqish hisoblandi. Lekin radiointerfeysni ishlab chiqish natijasida u asta-sekin yangi texnologiyani yaratishga o'zgardi.

Telekommunikatsion bozorda, shuningdek kompyuterlar bozorida yangi texnologiyaning yutuqlarini yangi texnologiyalarni o'z ishlanmalariga intergatsiyalanishini maqsadga muvofiqligi va iqtisodiy foydaligi haqida qarorni yetakchi ishlab chiqaruvchi firmalar ta'minlaydi. Shuning uchun o'z texnologiyasiga munosib kelajakni va keyingi rivojlanishni ta'minlash uchun Ericsson firmasi 1998 yilda oldiga quyidagi vazifalar qo'yilgan Bluetooth SIG (Spesial Interest Group) konsorsiumini tashkil qildi:

- Bluetooth texnologiyasini keyingi rivojlantirish;
- telekommunikatsion vositalar bozorida yanga texnologiyani ilgari surish.

Bluetooth SIG konsorsiumiga Ericsson kabi Nokia, 3COM, Intel, National Semiconductor firmalari ham kiradi.

Bu to'g'ri ko'rinish bo'lmaganida simsiz telefonlar, kompyuterlar va turli periferiyalarning aloqasini ta'minlashga imkon beradigan radio qisqa masofalarga ma'lumotlarni uzatish texnologiyasi hisoblanadi. Kompyuterda yoki mobil telefonda mavjud bo'lgan shtatdagi interfeysning ishlatilishi ko'p hollarda juda qulay bo'ladi (7.1- rasm).

Mavjud qurilmalar uchun standart Bluetooth-bogʻlanish profillarini ishlatadigan uncha qimmat boʻlmagan oʻrnatiladigan radiomodullar taklif etilmoqda. Masalan, simsiz garnituralarda HeadSet profili ishlatiladi, qurilmalar orasida fayllarni almashlash uchun FTP profili ishlab chiqilgan mobil telefonlarda Dial-up Networking Profile profili qoʻllaniladi. Maʼlumotlarni toʻplash va boshqarish tizimlarida koʻpincha SPP ketma-ket porti profili ishlatiladi.



7.1- rasm. Bluetooth tizimi

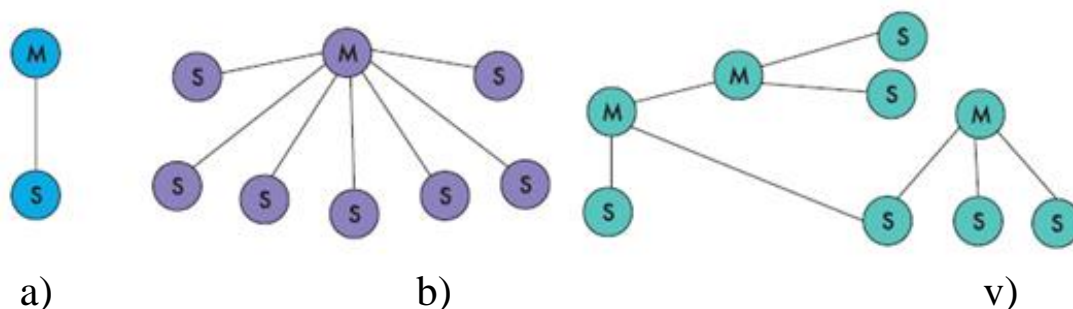
Bluetooth protokoli nuqta-nuqta va nuqta-koʻp nuqta topologiyalarini qoʻllaydi. Ikki yoki undan ortiq oʻsha bir kanalni ishlatadigan qurilmalar pikotarmoqni (piconet) tashkil etadi. Bunda qurilmalardan biri asosi (Master) sifatida, qoganlari esa boʻysunuvchi (Slave) qurilmalar sifatida ishlaydi.

Bluetooth qabullagich-uzatkichlari 2.45 GGs chastotada ishlaydi va FHSS (Frequency Hopping Spread Spectrum – chastotani sakrashsimon qayta sozlanishi) spektrni kengaytirish usulini ishlatadi.

Ikki yoki undan ortiq oʻsha bitta kanalni ishlatadigan qurilmalar pikotarmoqni (piconet) tashkil etadi. Qurilmalardan biri asosiy qurilma (master), qolganlari esa boʻysunuvchi qurilmalar (slave) sifatida ishlaydi. Bitta pikotarmoqda yettitagacha aktiv boʻysunuvchi qurilmalar boʻlishi mumkin, bunda qolgan boʻysunuvchi qurilmalar asosiy qurilma bilan sinxronlashtirilgan qolishi bilan “kutish” rejimida boʻladi. Oʻzaro taʼsirlashuvchi pikotarmoqlar “taqsimlangan tarmoqni” (scatternet) tashkil etadi.

Har bir pikotarmoqda faqat bitta asosiy qurilma ishlaydi, lekin boʻysunuvchi qurilmalar turli pikotarmoqlarga kirishi mumkin.

Bundan tashqari, bitta pikotarmoqning asosiy qurilmasi boshqa tarmoqning qurilmasiga bo'ysunuvchi bo'ladi (7.2-rasm).



7.2- rasm. Bo'ysunuvchi qurilmalarli pikotarmoq: a) bitta bo'ysunuvchi qurilmali; b) bir necha bo'ysunuvchi qurilmalarli; v) taqsimlangan tarmoq

Uzatkichning quvvatiga bog'liq ravishda Bluetooth® qurilmalar uchta sinflarga bo'linadi:

- 1-sinf – 100 mVtgacha (ochiq fazoda masofa 100 metrgacha);
- 2-sinf – 2,5 mVtgacha (ochiq fazoda masofa 15 metrgacha);
- 3-sinf – 1 mVtgacha (ochiq fazoda masofa 5 metrgacha).

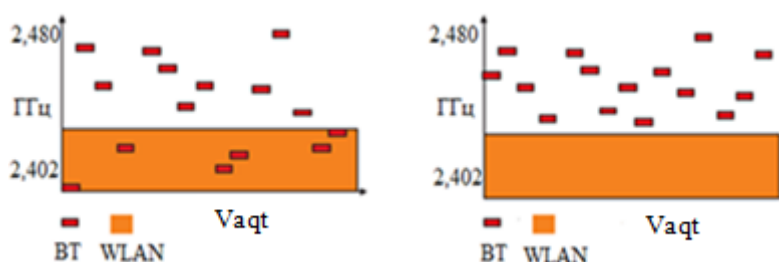
Birinchi Bluetooth modullarining paydo bo'lishidan boshlab ularning yangi ilovalarda qo'llanilishiga Bluetooth protokoli stekining murakkab dasturiy ishlatilishiga to'sqinlik qildi. Ishlab chiquvchiga Bluetooth-modulini bilan mustaqil boshqarish va modulning boshqa Bluetooth-qurilmalari bilan xost-kontroller interfeysi komandalari (HCI — Host Controller Interface) yordamida o'zaro ta'sirlashishini aniqlaydigan profillarni ishlab chiqish zarur bo'ldi.

2004 yilning o'rtalarida 2001 yilda e'lon qilingan Bluetooth 1.1-versiyasi spetsifikatsiyasi o'rniga Bluetooth 1.1-versiyasi spetsifikatsiyasi qabul qilindi. Bluetooth 1.2-versiyasi spetsifikatsiyasining Bluetooth 1.1-versiyasi spetsifikatsiyasidan asosiy farqlariga quyidagilar kiradi:

1. Kanal chastotasini adaptiv qayta sozlash texnologiyasining ishlatilishi (Adaptive Frequency hopping, AFH).
2. Tovushli bog'lanishlarni takomillashtirish.
3. Ikkita Bluetooth modullari orasida bog'lanishni o'rnatishga sarflanadigan vaqtni qisqartirish.

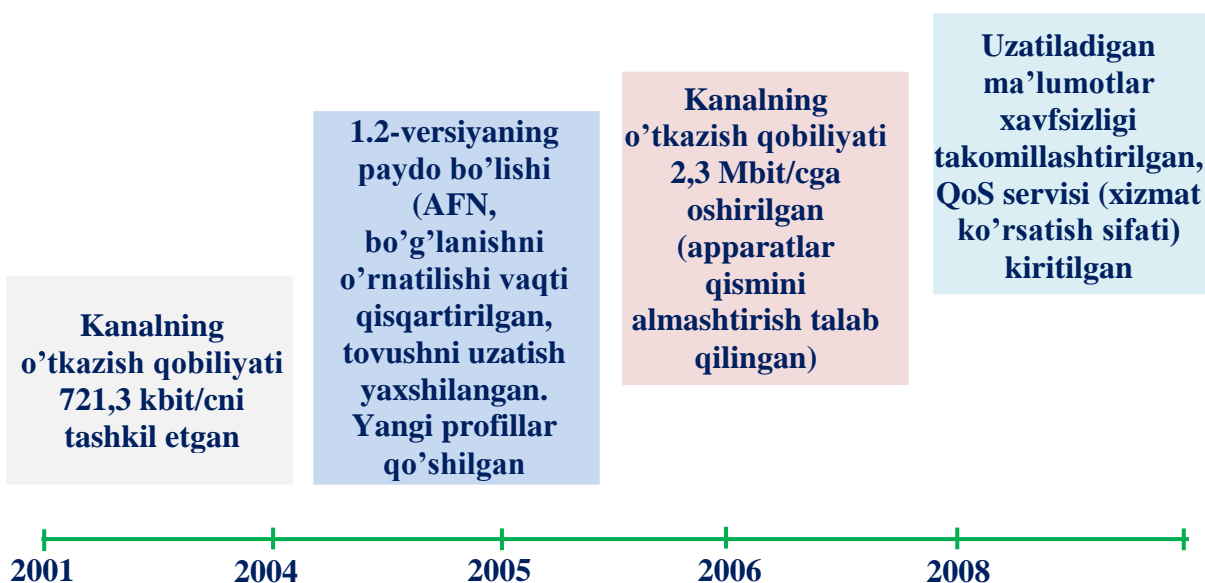
Ma'lumki, Bluetooth va Wi-Fi o'sha bir litsenziyalanmagan 2,4 GGs diapazonni ishlatadi. Demak, Bluetooth-qurilmalar Wi-Fi

qurilmasining ishlash diapazonida bo‘ladigan va o‘zaro ma’lumotlar almashadigan hollarda bu kolliziyalarga olib kelishi va qurilmalarning ishlash qobiliyatiga ta’sir qilishi mumkin [22]. AFH texnologiyasi kolliziyalarning paydo bo‘lishini oldini olishga imkon beradi: Bluetooth texnologiyasi interferensiyaga qarshi kurashishi uchun ma’lumotlarni almashtirish vaqtida tanlanishida Wi-Fi qurilmalari ma’lumotlar almashtiradigan chastotalar kanallari hisobga olinmaydigan kanal chastotasining sakrashesimon qayta sozlanishidan foydalanadi. 7.3-rasmda AFH texnologiyasining ishlash prinsipi ko‘rsatilgan.



7.3- rasm. AFH texnologiyasining ishlash prinsipi: a) kolliziyalar; b) kanal chastotasining adaptiv qayta sozlanishi yordamida kolliziyalardan ketish

Bluetooth texnologiyasining rivojlanishi bir joyda to‘xtab qolgani yo‘q. SIG konsorsiumi tomonidan texnologiyani rivojlantirish konsepsiyasi ishlab chiqilgan (7.4-rasm).



7.4- rasm. Bluetooth texnologiyasini rivojlanishi bosqichlari

7.2. Bluetooth texnologiyasining spetsifikatsiyalari

Hozirgi vaqtda bozorda Bluetooth modullarini, shuningdek Bluetooth-qurilmalari apparatli qismlarini mustaqil ishlatish uchun komponentlar taklif etadigan ko'p sonli firmalar ishlamoqda.

Deyarli barcha ishlab chiqaruvchilar Bluetooth 1.1- va 1.2-versiyalari spetsifikatsiyalarida ishlaydigan va 2-sinf (10 metr ishlash zonasili) va 1-sinfga (10 metr ishlash zonasili) mos modullarni taklif qilmoqda. Lekin, 1.1-versiya to'liq 1.2 versiyaga moslashishiga qaramasdan, yuqorida ko'rib chiqilgan 1.2 versiyada ishlatilgan takomillashtirishlar, faqat har ikkala qurilma 1.2-versiyaga mos bo'lsa olinishi mumkin.

2004 yilning noyabrida ma'lumotlarning kengaytirilgan uzatish texnologiyasida ishlaydigan Bluetooth 2.0-versiyasining spetsifikatsiyasi (Enhanced Data Rate, EDR) qabul qilindi. EDR da ishlaydigan 2.0 spetsifikatsiya 3 Mbit/s gacha tezliklarda ma'lumotlarni almashtirishni amalga oshirishga imkon beradi. Bluetooth 2.0-versiyasiga mos va EDR ma'lumotlarning kengaytirilgan uzatish texnologiyasida ishlaydigan birinchi turkum ishlab chiqarilgan modullarning namunalari 2005 yilning oxirlarida ishlab chiqaruvchilarga taqdim etildi. Bunday modullarning ishlashi radiusi to'g'ri ko'rinish bo'lmaganida 10 metrni tashkil qiladi, to'g'ri ko'rinish bo'lganida esa 30 metrni tashkil etadi, bu 2-sinfga mos keladi.

2008 yilning avgustida Bluetooth SIG 2.1+EDR ni taqdim etdi. Bluetooth ning yangi versiyasi energiya iste'molini 5 martaga kamaytiradi, ma'lumotlarni himoyalash darajasini oshiradi va u bajariladigan qadamlar sonining kamaytirilishi tufayli Bluetooth-qurilmasining tanilishi va bog'lanishini yengillashtiradi [22].

Bluetooth SIG tomonidan Bluetooth 3.0 + HS 2009 yilning 21 aprelida qabul qilingan. U nazariy jihatdan 24 Mbit/s gacha uzatish tezligida ishlaydi. Uning asosiy o'ziga xos xususiyati 802.11 ga yuqori tezlikli xabarni qo'shishi kabi AMR ni qo'shish (asimmetrik multiprotsessorli ishlov berish) (MAC/PHY ga muqobil) hisoblanadi. Yangi spetsifikatsiyada ishlaydigan modullar o'zida ikkita radiotizimlarni birlashtiradi: birinchisi 3 Mbit/s gacha (Bluetooth 2.0 uchun standart) ma'lumotlarni uzatish tezligini ta'minlaydi va past energiya iste'moliga ega; ikkinchisi 802.11 standart bilan mos tushadi va 24 Mbit/s gacha ma'lumotlarni uzatish tezligi imkoniyatini (Wi-Fi

tarmoqlarining tezliklari bilan taqqoslasa bo‘ladigan) ta’minlaydi. Ma’lumotlarni uzatish uchun radiotizimni tanlash uzatiladigan faylning o‘lchamlariga bog‘liq. Uncha katta bo‘lmagan fayllar sekinroq kanal bo‘yicha, katta fayllar yuqori tezlikli kanal bo‘yicha uzatiladi. Bluetooth 3.0 yanadi umumiy 802.11 standartini (so‘z yasovchi qo‘shimchasiz) ishlatadi, ya’ni ning Wi-Fi 802.11b/g yoki 802.11n kabi standartlari bilan moslashmaydi.

Bluetooth SIG Bluetooth 4.0 spetsifikatsiyani 2010 yilning 30 iyunida tasdiqladi. Bluetooth 4.0 spetsifikatsiya Klassik Bluetooth, YUqori tezlikli Bluetooth va Past energiya iste’mol qiladigan Bluetooth larni o‘z ichiga oladi.

Bluetooth spetsifikatsiyasining texnik parametrlari 7.1- jadvalda keltirilgan.

7.1- jadval

Bluetooth spetsifikatsiyasining texnik parametrlari

Parametrning nomi	Klassik Blyutus	Past energiya iste’molili Blyutus
Radiochastota	2,4 GGs	2,4 GGs
Masofa	100 m	50 m
Havo bo‘yicha ma’lumotlarni uzatish tezligi	1-3 Mbit/s	1 Mbit/s
O‘tkazish qobiliyati	0,7-2,1 Mbit/s	0,26 Mbit/s
Yetakchi qurilmalar	7	aniqlanmagan
Xavfsizlik	64/128-bitli shifrlash va foydalanuvchi aniqlaydigan amaliy daraja	128-bitli AES Counter Mode CBC-MAC shifrlash va foydalanuvchi aniqlaydigan amaliy daraja
Ulanishni kechikishi	Odatda 100 ms	6 ms
Umumiy ma’lumotlarni uzatish vaqti	100 ms	6 ms
Sertifikatsiya	Bluetooth SIG	Bluetooth SIG

Ovozni uzatish	Ha	Yo'q
Tarmoq topologiyasi	Scatternet	Star-bus
Iste'mol quvvati	1 Vt	Ot 0,01 Vt do 0,5 Vt (ishlatish variantiga bog'liq)
Maksimal iste'mol toki	< 30 mA	< 20 mA (batareyadan ishlash uchun maks. 15 mA)

Yuqori tezlikli Bluetooth Wi-Fi ga asoslangan, Klassik Bluetooth oldingi Bluetooth spetsifikatsiyalari protokollaridan iborat.

Uzatiladigan ma'lumotlar tezligi ishlatiladigan spetsifikatsiya versiyasi va Bluetooth profiliga bog'liq bo'ladi. Ketma-ket port profili ishlatilganida ma'lumotlarni uzatish tezligi 704 kbit/c nazariy chegaraga ega bo'ladi.

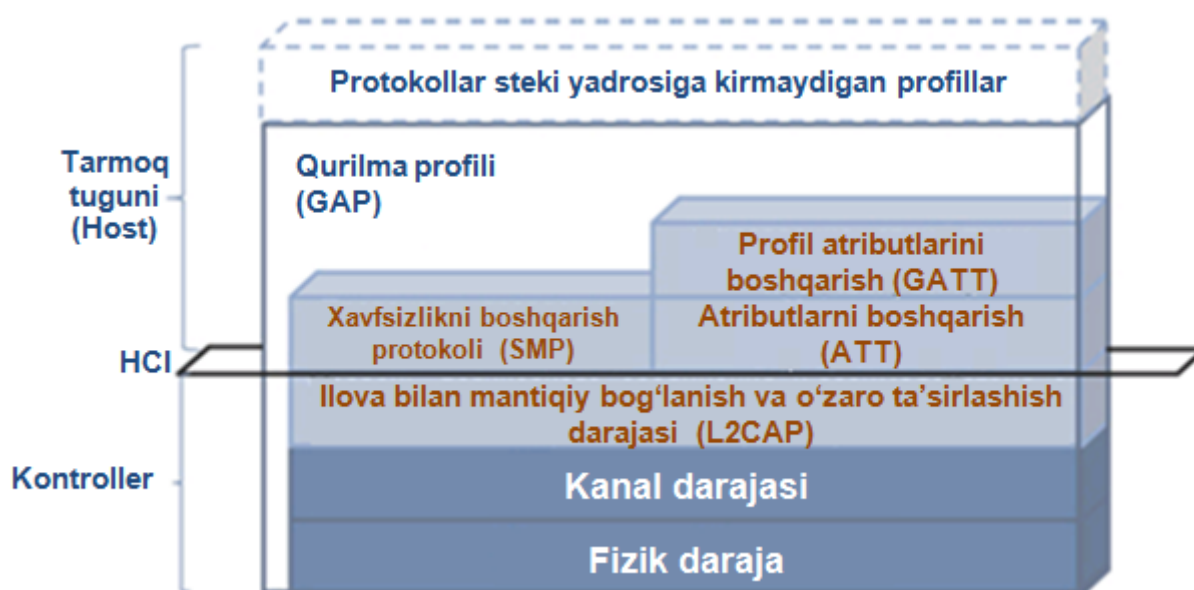
Bluetooth protokollar klassik stekidagi kabi Bluetooth steki ikkita asosiy qismlar - kontroller (Controller) va tarmoq tugunidan (Host) iborat. Kontroller fizik va kanal darajasini o'z ichiga oladi va integratsiyalangan simsiz transiverli kristalldagi-tizimlar (KT) ko'rinishida bajarilishi mumkin. Tarmoq tuguni deyiladigan stekning qismi ilovalar mikrokontrollerida dasturiy yig'iladi va quyidagi yuqori darajalar funktsionalliklarini o'z ichiga oladi:

- mantiqiy aloqa darajasi (Logical Link Control – LLC);
- moslashtirish protokoli (Adaptation Protocol – L2CAP);
- atributlar protokoli (Attribute Protocol – ATT);
- qurilmalar profillari atributlari protokoli (Generic Attribute Profile – GATT);
- xavfsizlikni ta'minlash protokoli (Security Manager Protocol – SMP);
- qurilmalar profillari funktsiyalariga ulanishni ta'minlash protokoli (Generic Access Profile – GAP).

7.3. Bluetooth texnologiyasining protorollari steki va profillari

Stekning yuqori va pastki qismlari orasidagi o'zaro ta'sirlashish Host Controller Interface (HCI) interfeys orali amalga oshiriladi. Amaliy darajaning qo'shimcha funktsionalligi tarmoq tuguni darajasi ustidan yig'ilishi mumkin. Bluetooth protokollari stekining tuzilmasi 7.5- va 7.6-rasmlarda keltirilgan.

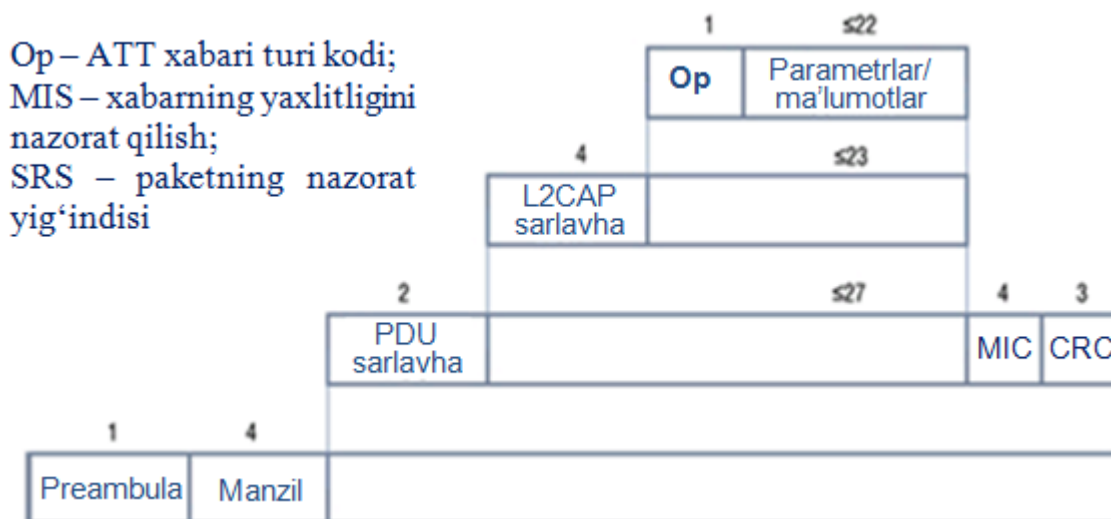
Bluetooth qurilmalari 2,4 GGs diapazonda ishlaydi. Standartda kanallar orasidagi 2 MGs masofali 40 ta chastotalar kanallari aniqlangan. Fizik darajada 0,45 dan 0,55 gacha chegaralardagi modulyatsiyalash indeksili GFSK-modulyatsiyalash (gauss filtrlashli chastotaviy modulyatsiyalash) qo‘llanilgan, bu energiyaning maksimal iste‘molini kamaytiradi. Fizik darajadagi ma‘lumotlarni uzatish tezligi 1 Mbit/s. BLE standartida qabullagichning sezgirligi bitli xatoliklari chastotasi (Bit Error Rate – BER) 10^{-3} sathga yetadigan qabullagichdagi signal sathi sifatida aniqlanadi. U 70 dBm yoki undan yaxshini ta‘minlashi kerak.



7.5- rasm. Bluetooth Low Energy (BLE) protokollari stekining tuzilmasi

Shuningdek, ta‘kidlash kerakki, Bluetooth 4.0 spetsifikatsiyasi qurilmaning bir yoki ikki rejimli ishlashini ko‘zda tutadi. Bunda Klassik Bluetooth va BLE bir rejimli kontrollerlari moslashuvchan emas. Moslashuvchanlikni ta‘minlash uchun kontroller ikki rejimli bo‘lishi kerak. Tarmoqning tugunlari esa bir rejimli hisoblanadi.

Kanal darajasida ikkita bildirish kanallari va ma‘lumotlar kanallariga ajratiladi. Bildirish kanallari qurilmalarni qidirish, bog‘lanishlarni o‘rnatish, keng tarqatishli uzatish ishlatiladi, ma‘lumotlar kanallari esa qurilmalar orasida ikki tomonlama almashlash uchun ishlatiladi.



7.6- rasm. Bluetooth ma'lumotlar paketi formati

Bildirish kanallari uchun polosa markazida uchta chastotalar kanallari ajratilgan, bu IEEE 802.11 standartining 1, 6 va 11 kanallari bilan qoplanishni minimallashtiradi. Qolgan 37 ta kanallar ma'lumotlarni almashlash uchun ishlatiladi. Halaqitlar ta'siri, ko'p nurli tarqalishni kamaytirish, shuningdek ma'lumotlarni almashlash qo'shni qurilmalarning ta'sirini kamaytirish uchun chastotani sakrashesimon qayta o'zgartirish ko'zda tutilgan.

Bluetoothda paketlarni keng tarqatishli uzatish uchun bildirish kanallari qo'llaniladi. Bu kanallar bo'yicha paketlarni uzatadigan istalgan qurilma bildirgich deyiladi. Bildirish kanallari bo'yicha paketlarni uzatilishi faqat maxsus ajratilgan vaqt intervallarida bo'lib o'tadi, ular bildirishlar hodisalari deyiladi. Bu hodisalar vaqtida qurilma-bildirgich uchta chastotalar kanallarining har bir biri bo'yicha bildirishlar paketlarini ketma-ket uzatadi. Yagona funksiyasi bildirishlar paketlarini qabul qilish hisoblangan qurilmalar skanerlar deyiladi.

SPP profili (Serial Port Profile) oldin simli ketma-ket interfeys bilan bog'langan ikkita qurilmalar orasida "ochiq" simsiz kanalni juda oddiy tashkil etishga imkon beradi. O'rnatiladigan Bluetooth-modul simli sinxron ketma-ket kanal bo'yicha keladigan ma'lumotlar oqimini SPP (Serial Port Profile) profiliga muvofiq simsiz oqimga o'zgartiradi. Olisdagi tomonda Bluetooth qabullagich-uzatkichi sifatida personal kompyuterning shtatdagi Bluetooth-adapterini yoki ikkinchi o'rnatiladigan modulni ishlatish mumkin.

Bunday Bluetooth bogʻlanishda qurilmalardan biri yetakchi (master). Boshqasi esa yetaklanuvchi (slave) hisoblanadi. Kompyuter tomonida master joylashadi. Shuning uchun oʻrnatiladigan tizimlar uchun koʻpincha yetaklanadigan sifatda konfiguratsiyalangan Bluetooth-modullar ishlatiladi.

Ketma-ket port profili Bluetooth qurilmalari bilan quyidagi operatsiyalarning bajarilishini koʻzda tutadi.

- Bluetooth-qurilmalarni topish;
- ikkita Bluetooth-qurilmalarning bogʻlanishini oʻrnatish;
- “ochiq” kanal rejimida maʼlumotlarni uzatish.

Yetaklanadigan Bluetooth modul taʼminot yoqilganida topish uchun mumkin holatda boʻladi. Yetakchi Bluetooth modul taʼminot yoqilganida yetaklanadigan qurilmalarni qidirishni boshlaydi va boʻsh yetaklanadigan qurilma topilganida unga ulanishga urinadi. Yetaklanadigan qurilma PIN-kodni soʻraydi, yetakchi qurilma javob beradi. Agar PIN-kodlar mos tushsa, u holda qurilmalar oʻz manzillari bilan almashadi, juftlikni tashkil etadi va maʼlumotlarni almashlashni bajarishi mumkin. Shunday qilib, bogʻlanishni oʻrnatilishi avtomatik boʻlib oʻtadi.

Yetaklanadigan va yetakchi qurilmalar olisdagi modul soʻrovlarga javob bermaganida vaziyatni turlicha qayta ishlaydi. Yetaklanadigan qurilma bu holda bogʻlanish yoʻqotilgan hisoblaydi va yana topish uchun mumkin boʻladi. Yetakchi Bluetooth modul oldin oʻrnatilgan bogʻlanishga qoladigan boʻlib qoladi. U oldingi hamkorini unutishi uchun unga tashqi chiqishga bekor qilishi impulsini berish kerak.

Bluetooth texnologiyasi Bluetooth Special Interest Group (SIG) tijorat uyushmasi tomonidan qoʻllab-quvvatlanadi va rivojlantiriladi. U Bluetooth spetsifikatsiyalarini eʼlon qiladi, qurilmalarning sertifikatlashtirilishini tashkil etadi, Bluetooth savdo belgisini himoya qiladi va texnologiyani targʻib qiladi.

Bluetooth texnologiyasi rivojlanishda davom etmoqda. Batareyalardan bir necha yillar ishlay oladigan ultra past energiya isteʼmolili Bluetooth qurilmalarini ishlab chiqishga imkon beradigan "Bluetooth Low Energy" spetsifikatsiyaning tasdiqlanishi kutilmoqda.

Sanab oʻtilganlardan tashqari, Bluetooth SIG ishchi guruhi koʻplab boshqa standart profillarni aniqladi:

- Generic Access Profile (umumiy foydalanishdagi profil) – qurilmalar orasidagi aloqani taʼminlash, boshqa mumkin profillarni

aniqlash, shuning xavfsizlikka javob beradigan asosiy Bluetooth® profili hisoblanadi;

- Service Discover Application Profile (xizmatlarni topish ilovalari profili) – qanday Bluetooth® xizmatlari bu qurilma bilan ishlashda mumkin bo‘lishini aniqlash imkoniyatini beradi;

- Serial Port Profile (ketma-ket port profili) – Bluetooth® qurilmalarga PK ketma-ket portini emulyatsiyalashga imkon beradi va yuqoriroq darajadagi ko‘plab profillar orqali ishlatiladi;

- Dial-up Networking Profile (sisiz telefoniya profili) – Bluetooth®li sotali telefonlarga mo‘ljallangan va telefonni simsiz "go‘shak" sifatida ishlatilishiga imkon beradi. Bluetooth® ulanish nuqtasi orqali uyda, ofisda, jamoat joylarida va boshqalarda telefon tarmog‘i bilan bog‘lanishini ta’minlaydi;

- Fax Profile (faks profili) – ko‘p tomondan oldingi profilga o‘xshaydi, faksni qo‘llaydigan dasturiy ta’minotga ega bo‘lgan qurilma bilan Bluetooth® orqali bog‘lanishda faks-modemni emulyatsiyalashga imkon beradi;

- Generic Object Exchange Profile (ob’ektlar bilan umumiy almashlash profili) – ilovalarga IRdan foydalanmasdan ma’lumotlar bilan to‘g‘ridan-to‘g‘ri almashlashga imkon beradi;

- File Transfer Profile (faylni uzatish profili) – qurilmaga ftpda amalga oshirilishidagiga o‘xshash boshqa qurilmada saqlanadigan ma’lumotlarga ulanishni olishga imkon beradi;

- Headset Profile (garnitura profili) – dinamik va mikrofon bilan jihozlangan garnitura bilan qurilmalarning simsiz bog‘lanishini ta’minlaydi.

- LAN Access Profile (lokal tarmoqqa ulanish profili) – IP-tarmoqlarni qurish uchun mo‘ljallangan va uncha katta bo‘lmagan Intranet tarmoqlarini qurishga imkon beradi, shuningdek lokal tarmoq yoki Internet tarmog‘i bo‘lsin, kabelli tarmoqlar bilan aloqa uchun ulanish nuqtalari sifatida ishlatiladi;

- Advanced Audio Distribution Profile (A2DP) – radiokanal bo‘yicha audio stereo oqim qanday uzatilishini tavsiflaydi;

- Audio / Video Control Transport Protocol (AVRCP) – hi-fi sinfdagi televizion va ovoz apparaturalarini simsiz o‘zaro ta’sirlashish standart interfeysini, shuningdek bu apparaturalarni simsiz boshqarilishini aniqlaydi.

Past energiya iste’mol qiladigan Bluetooth, avvalo miniatyurali elektron datchiklar (sport payabzallari, trenajyorlar, patsientlar

tanalariga joylashtiriladigan miniatyurali sensorlarda va boshqalarda ishlatiladigan) uchun mo'ljallangan. Past energiya iste'moliga maxsus ishlash algoritmidan foydalanish hisobiga erishiladi. Uzatkich faqat ma'lumotlarni uzatilishi vaqtiga yoqiladi, bu bitta CR2032 turdagi batareyadan bir necha yil davomida ishlash imkoniyatini beradi. Standart ma'lumotlar paketlari o'lchamlari 8—27 bayt bo'lganida 1 Mbit/s ma'lumotlarni uzatish tezligini beradi. Yangi versiyada ikkita Bluetooth-qurilmalari 5 millisekunddan kam vaqtda bog'lanishni o'rnatadi va 100 metrgacha masofada uni ishlatishi mumkin. Buning uchun takomillashtirilgan xatoliklarni tuzatish ishlatiladi, zarur xavfsizlik darajasini esa 128-bitli AES-shifrlash ta'minlaydi.

Xulosada ta'kidlash kerakki, Bluetooth texnologiyasiga juda katta qiziqish namoyon bo'lmoqda. Sanoat va xalq ho'jaligining ko'p sonli bir vaqtda o'lchanadigan parametrlarini to'plash va qayta ishlash talab qilinadigan sohalari, masalan, neft mahsulotlarini qayta ishlash, metallurgiya zavodlari, turar-joy kommunal xo'jaliklari va boshqa sohalar eng istiqbolli hisoblanadi.

Nazorat savollari

1. Bluetooth nima?
2. Bluetooth texnologiyasi afzalliklarini tushuntiring.
3. Bluetooth texnologiyasining xususiyatlarini tushuntiring.
4. Bluetooth texnologiyasining spetsifikatsiyalarini izohlang
5. Bluetooth texnologiyasining protokollari steki nima?
6. Bluetooth texnologiyasining protokollari profillari nima?

8- BOB. BOSHQA SIMSIZ KENG POLOSALI ULANISH TEKNOLOGIYALARI

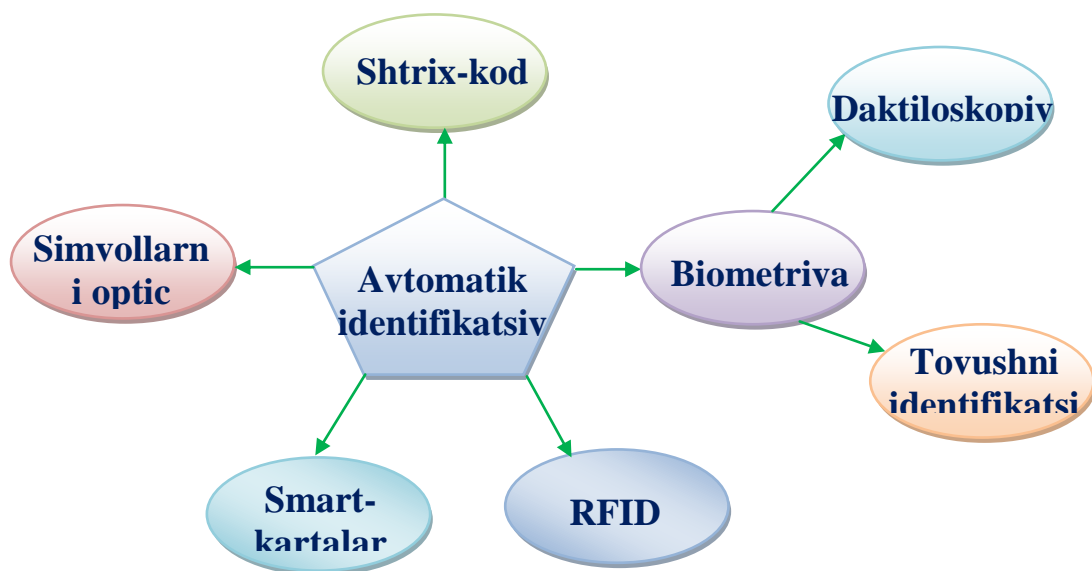
8.1. RFID radiochastotali identifikatsiyalash texnologiyasi

Radiochastotali identifikatsiyalash, bu aloqa radiochastota kanali yordamida ob'ektlarni avtomatik identifikatsiyalash va ro'yxatga olish guruhiga kiradigan mustaqil yo'nalish hisoblanadi (8.1- rasm).

RFID – bu an'anaviy belgilash tizimlariga qaraganda ko'p imkoniyatlarni beradigan zamonaviy identifikatsiyalash texnologiyasi hisoblanadi.

RFID tizimlari ko'plab turli variantlarda mavjud va bu tizimlarga qisqacha tahlilni berish uchun bir RFID tizimni boshqasiga differensiallashtirishga imkon beradigan o'ziga xos xususiyatlarini aniqlash zarur.

RFID tizimlari ikkita asosiy aloqa turlaridan biriga muvofiq dupleks (FDX)/yarim dupleks (HDX) yoki impulsli rejim desa ham bo'ladigan ketma-ket tizimlar (SEQ) prinsipi bo'yicha ishlaydi [24].



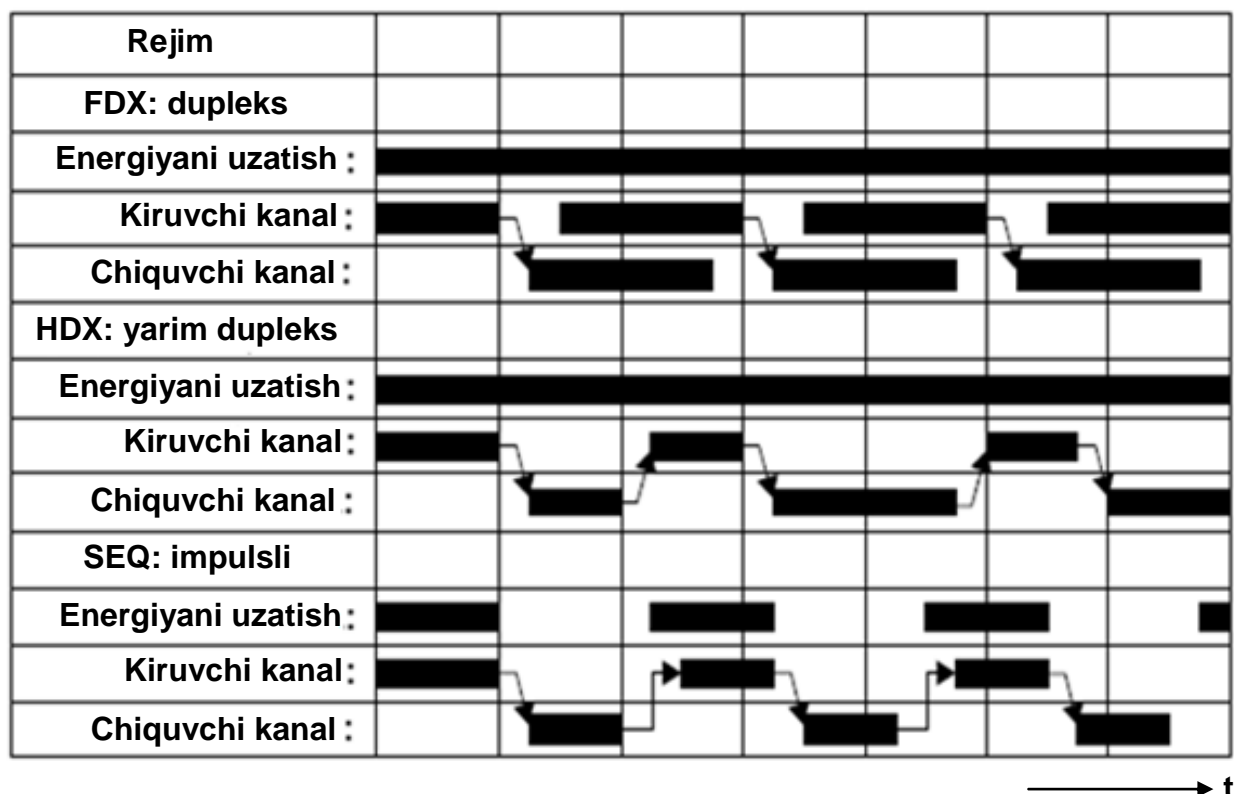
8.1- rasm. Avtomatik identifikatsiyalash texnologiyalarining bo'linishi

Yarim dupleks va dupleks rejimlarda transponderning javobi o'qigich qurilmaning radiochastotasi (elektr maydoni) aniqlanganida uziladi. Binobarin, bu javob signali yetarlicha kuchsiz bo'lishi

mumkin, boshqa quvvatliroq manbalardan halaqitlar fonida qabullagich-uzatkich signalini ajratishga imkon beradigan usullarga tayanish zarur. Transponderdan ma'lumotlarni o'qish qurilmasiga uzatishda yuklama modulyatsiyasi degan modulyatsiya amaliy ishlatiladi, unda nimitashuvchidan tashqari o'qish qurilmasi ishchi chastotalarining ikkinchi darajali garmonikalari ishlatiladi.

Ketma-ket tizimlarda o'qish qurilmasi maydoni har bir so'rovdan keyin qisqa vaqt oralig'iga o'chiriladi. Bu oraliq qabullagich-uzatkichdan o'qish qurilmasiga so'raladigan ma'lumotlarni uzatish uchun ishlatiladi. Impulsi rejimning kamchiligi uzatishdagi tanaffus vaqtida ta'minot elektromagnit maydonini yo'qotilishi hisoblanadi. Bu kamchilik yordamchi kondensatorlar yoki batareyalardan foydalanish bilan o'g'rilanadi.

Keltirilgan ish rejimlarida o'qish qurilmasidan impulsi qabullagich-uzatkichgacha ma'lumotlarni uzatish kiruvchi kanali, shu bilan bir vaqtda qabullagich-uzatkichdan o'qish qurilmasiga ma'lumotlarni uzatish chiquvchi kanal deyiladi (8.2- rasm)



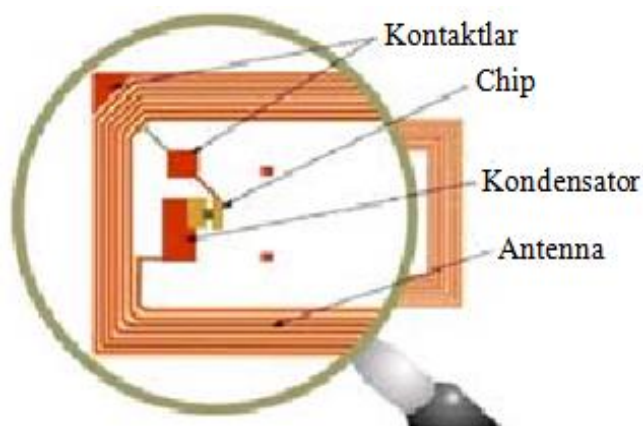
8.2- rasm. Turli aloqa rejimlarida t vaqtda ma'lumotlarni va elektromagnit maydon energiyasini uzatish prinsipi

Ob'ektlarni (sub'ektlarni identifikatsiyalash ob'ektga biriktiriladigan maxsus mikrosxema-trasponder – elektron belgi xotirasidan o'qiladigan unikal raqamli kod bo'yicha amalga oshiriladi. Raqamli kodni uzatish transponderning kormusiga montaj qilingan (maxsuslashtirilgan mikrosxema ham) va u bilan bir butun bo'lgan antenna yordamida amalga oshiriladi.

Transponder xotirasidan ulkan kodni o'qish radiochastotali signal-jo'natmasini shakllantiradigan boshqa qurilma bo'lgan o'qish qurilmasi yoki qabullagich-uzatkichning so'rovi bo'yicha amalga oshiriladi, bunda signal-jo'natma ta'sir etish maydoniga tushganida transponder javob raqamli kodini uzatadi.

Ko'plab shtrix-kodlar kabi eng keng tarqalgan belgilar o'zi yopishadigan yorliqlar hisoblanadi. Lekin, agar shtrix-kodda ma'lumotlar grafik ko'rinishda saqlansa, u holda belgiga ma'lumotlar radioto'lqinlar yordamida kiritiladi va o'qiladi.

Radiochastotali yorliq (8.3-rasm) qabullagich, uzatkich va ma'lumotlarni saqlash uchun xotiradan iborat [24]. Radiochastotali o'qish qurilmasi on–line rejimidan ishlaydigan qabullagich va uzatkichdan iborat. Uzatkich ma'lum chastotali elektromagnit maydonni generatsiyalaydi. Bu maydon RFID yorliqlarga tushganida, u RFID dan siganalni “aniqlaydi” va undagi tovar haqida yozilgan ma'lumotlarni uzatadi. Signal skanerning RFID antennasida qabul qilinadi, ishlov berish uchun kompyuterga retranslyatsiya qilinadi. Tovarni radiochastotaviy identifikatsiyalash uchun to'g'ri ko'rinish shart emas, shuning uchun RFID yorliqlar tez va oson o'qiladi, bu vaqtni tejashga imkon beradi.



8.3- rasm. Radiochastotali yorliqning tashqi ko'rinishi

Radiochastotali belgi bir yoki bir necha santimetr kvadratlarli maydonda yuzlab bayt ma'lumotlardan iborat bo'lishi mumkin. RFID belgilar ham faqat ma'lumotlarni o'qish uchun, ham ma'lumotlarni yozish va o'qish uchun ishlatiladi. RFID belgilarda saqlanadigan ma'lumotlar o'zgartirilishi, to'ldirilishi va hatto boshqasi bilan almashtirilishi mumkin. RFID belgilar tovar haqida eng batafsil ma'lumotlarga ega bo'lishi mumkin: davlat, ishlab chiqaruvchi, artikul, tur, rang, o'lcham, chiqarilishi sanasi, seriya raqami va h.k.. Yana shuni ta'kidlash kerakki, radiochastotali belgilar o'g'irliklardan himoyalash funksiyasini bajaradi va ularni buzish qiyin, deyarli mumkin emas, bu ularning uzoq vaqt xizmat muddatini ta'minlaydi.

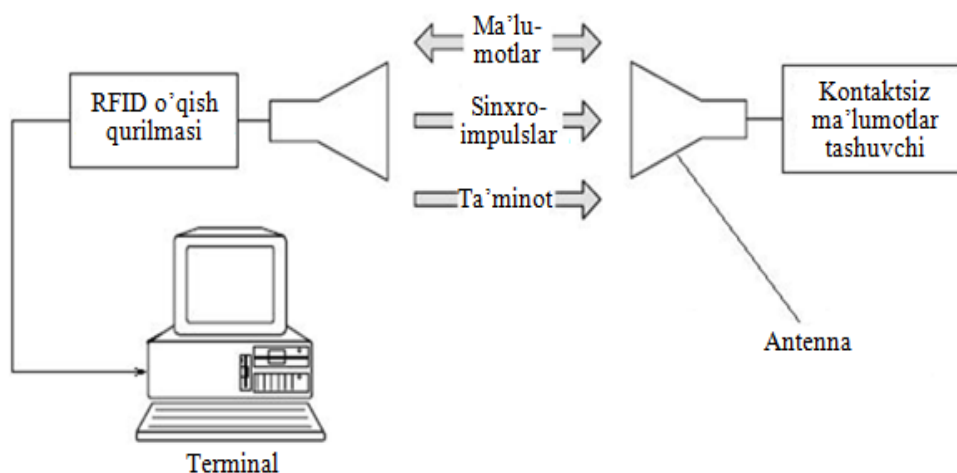
Radiochastotali identifikatsiyalash usulining o'ziga xos xususiyatlari quyidagilar:

- bu usul kontaktli hisoblanadi va to'g'ri ko'rinishni talab qilmaydi;
- elektron belgini yashirin o'rnatish imkoniyati;
- qiyin iqlimiy sharoitlarda va zararli muhitlarda ishlash;
- ma'lumotlarni o'qishning yuqori tezligi;
- ishlatishning cheklanmagan muddati (passiv identifikatsiyalash uchun);
- kodli ma'lumotlarning katta miqdori;
- o'qish/yoziqsh imkoniyati.

RFID tizimlar smart-kartalar bilan yaqin bog'langan. Ulardagi ma'lumotlar smart-kartalardagi kabi elektron tashuvchida saqlangan. Lekin, smart-kartalardan farqli ravishda RFID-belgi va o'qish qurilmasi orasidagi ma'lumotlarni almashtirish elektromagnit maydonlar yordamida va galvanik elementlar ishlatilmasdan bo'lib o'tadi.

Antenna RFID-belgi belgini aktivlashtiradigan va bu belgiga ma'lumotlarni yozish va o'qishga imkon beradigan elektromagnit to'lqinlarni nurlantiradi. Antenna belgi va qabullagich-uzatkich orasidagi o'ziga xos kanal hisoblanadi, u butun ma'lumotlarni uzatish va olish jarayonlarini nazorat qiladi. Antennalar o'lchamlari va shakllari bo'yicha farq qiladi. Ular antenaning ta'sir etish zonasidan o'tadigan predmetlar yoki odamlardan ma'lumotlarni o'qish uchun maxsus skanerlarga, shuningdek darvozalarga, turniketlarga, eshiklarga va boshqalarga o'rnatilishi mumkin. Ko'p sonli belgilarni uzluksiz o'qish kerak bo'ladigan hollarda antenna elektromagnit nurlanishlarni uzluksiz nurlantiradi. Agar doimiy so'rov talab

qilinmasa, u holda maydon operatorning komandasi bo'yicha aktivlashtirilishi mumkin. Antenna va qabullagich-uzatkich konstruktiv jihatdan bitta kopusda joylashtirilishi mumkin. Dekoder va qabullagich-uzatkichning funksiyalari radioqabullagich va skanerdagi o'xshash bloklardagi funksiyalarga o'xshash. Antennadan kelgan signal demodulyatsiyalanadi, rasshifrovka qilinadi va keyingi ishlov berish uchun kompyuterga uzatiladi (8.4- rasm).



8.4- rasm. RFID tizimning asosiy komponentlari

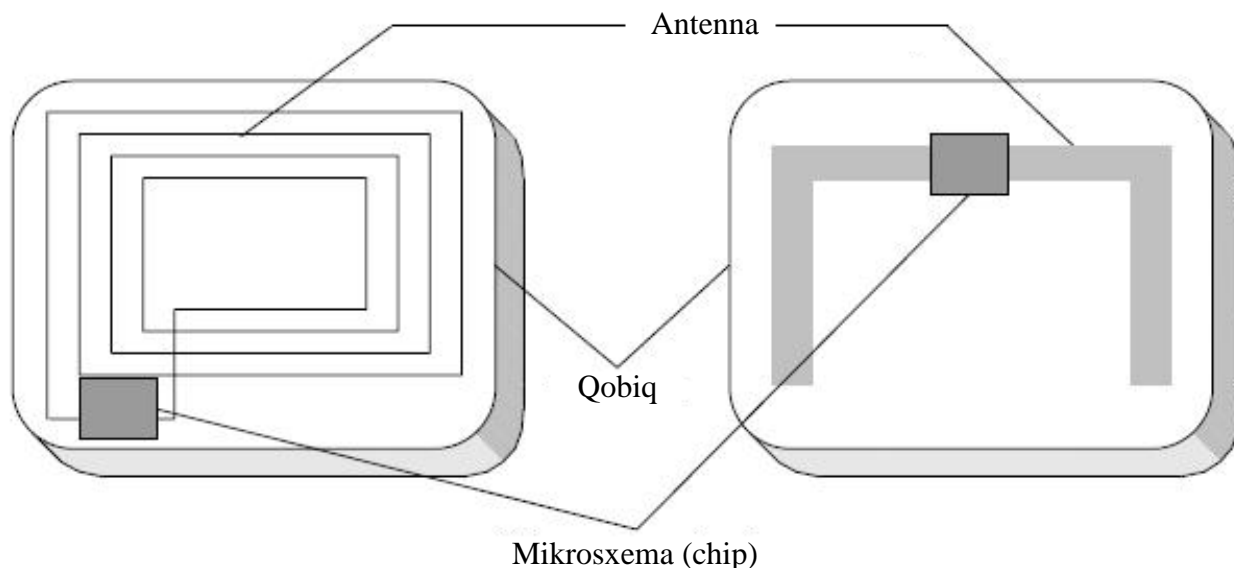
Radiochastotali belgi yoki transponder

Transponder, ya'ni qisqacha TRANSmitter/resPONDER (uzatkich-qabullagich) nomining o'zi bu qurilmaning funksiyani tushuntiradi. RFID-belgi odatda qabullagich, uzatkich, ma'lumotlarni saqlash uchun xotira bloki va antennani o'z ichiga oladi [22]. Bunda birinchi uchta komponent bitta mikrosxema ko'rinishida konstruktiv yig'iladi (8.5-rasm). Statsionar mahkamlangan o'qish qurilmasi yoki qo'lda boshqariladigan skaner nurlantiradigan radiosignaldan energiyani qabul qilish bilan transpondender foydali ma'lumotlarga ega bo'lgan o'z signali bilan javob beradi (8.4- rasm). RFID-belgilar haqiqatan "aqli yorliqlar" (smart labels) deyiladi.

RFID transponderlarli belgilarni turli sharoitlarda va muhitlarda joylashtirish uchun taniladigan ob'ektlarning xarakteristikalariga bog'liq ravishda korpuslarning maxsus modifikatsiyalari yaratilgan.

Masalan, shishali impulsi qabullagich-uzatkichlar (8.6- rasm) kapsula terining ostiga kiritiladigan hayvonlarni identifikatsiyalash uchun ishlatiladi. Shishali kapsulalar faqat 12 – 32 mm o'lchamlarga, bosma plataga joylashtiriladigan mikrosxema va olinadigan ta'minot

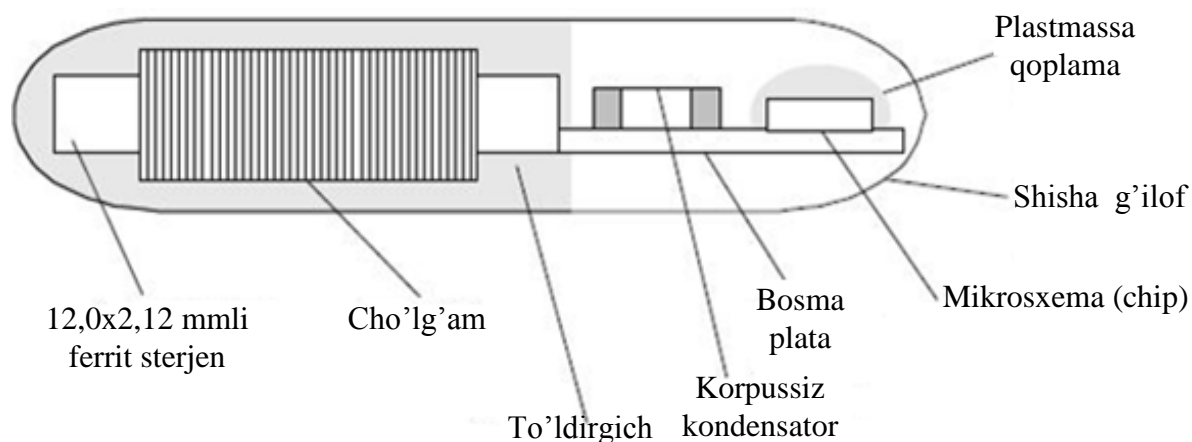
tokini silliqdash uchun zarur bo'ladigan kondensatorga ega. Induktivlik g'altagi 0,03 mm qalinlikdagi simdan mis cho'lg'amga ega. Ichki komponentlar mexanik barqarorlikka erishish uchun yumshoq to'ldirgichga joylashtiriladi [23].



8.5- rasm. Mikroshemaning joylashtirilishi: antenna g'altagi bilan induktiv bog'langan qabullagich uzatkich (chapda), dipol antennali mikroto'lqinli impulsli qabullagich-uzatkich

Plastik korpus mexanik ta'sirlardan barqarorlikka oshirilgan talablar qo'yiladigan qo'llanilish sohalari uchun maxsus ishlab chiqilgan.

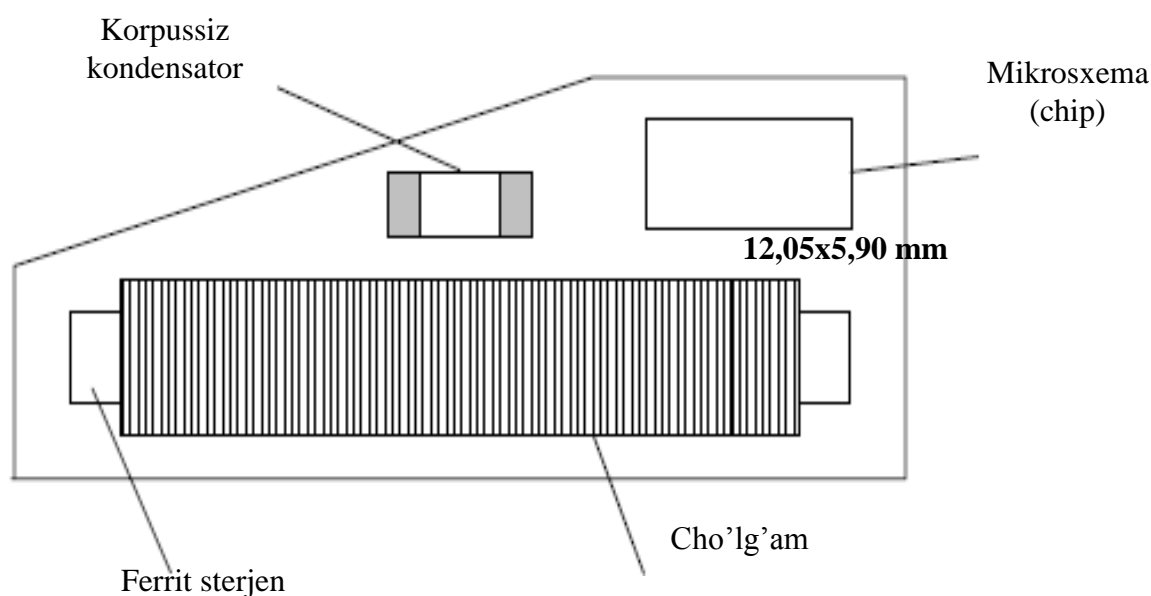
Bunday korpus boshqa predmetlarga masalan, elektron yopuvchi tizimlar uchun mashina kalitiga oson o'rnatilishi mumkin.



8.6- rasm. Transponderning shisha kapsulada joylashtirilishi

Plastik korpus deyarli shishali transpondedagi kabi komponentlarga ega bo‘ladi, lekin uning yanada uzun induktivlik g‘altagi katta funksional diapazonni beradi (8.7- rasm). Asosiy afzalliklariga yanada katta mikrosxemalarni joylashtirish imkoniyati va mexanik tebranishlarga katta ruxsat etishni kiritish mumkin.

Induktiv bog‘langan impulsli qabullagich-uzatkichlarni metall sirtlarga o‘rnatish uchun induktivlik g‘altagi III-simon shakldagi ferrit bronlangan o‘zakka joylashtiriladigan maxsus konstruksiyadagi shakl ishlab chiqilgan (8.8- rasm). Transponderning mikrosxemasida bunda o‘zakning orqa tomoniga joylashtiriladi va g‘altak cho‘lg‘ami bilan ulanadi.



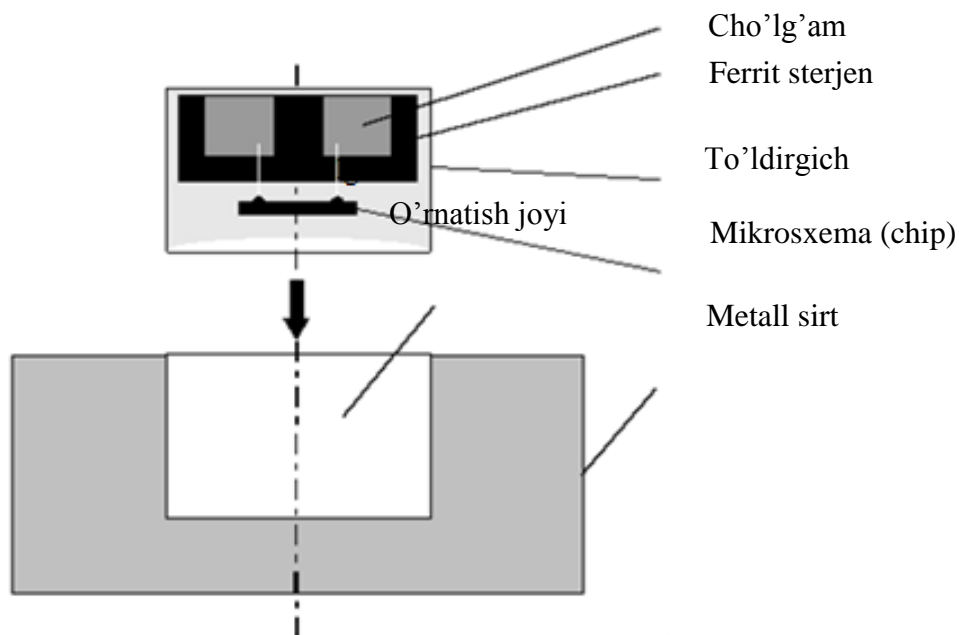
8.7- rasm. Transponderning plastik korpusda joylashtirilishi

Belgilar aktiv yoki passiv bo‘lishi mumkin. Aktiv belgi ulangan yoki o‘rnatilgan batareyadan ishlaydi, ular o‘qish qurilmasining kam quvvatini talab qiladi va o‘qishning katta uzoq masofaliligiga ega. Passiv belgi o‘qish qurilmasidan signalni olish bilan ta‘minot manbaisiz ishlaydi. Passiv belgilar aktiv belgilardan kichik va yengil, kamroq qimmat, deyarli cheklanmagan xizmat qilish muddatiga ega [23], [24].

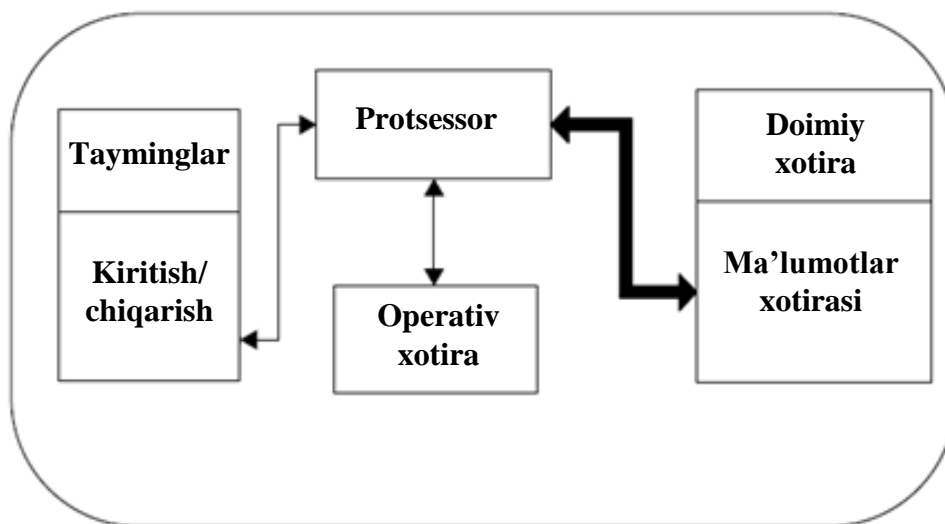
Aktiv va passiv teglar faqat o‘qish uchun, foydalanuvchi ma‘lumotlarni o‘qish-yozishli va ma‘lumotlar bir marta yozilishli bo‘lishi mumkin.

Radiochastotali belgi odatda qabullagich, uzatkich, antenna va ma‘lumotlarni saqlash uchun xotira blokini o‘z ichiga oladi. Qabullagich, uzatkich va xotira alohida mikrosxema (chip)

ko‘rinishida konstruktiv bajariladi (8.9- rasm), shuning uchun tashqaridan tuyuladiki, radiochastotali belgi faqat ikkita qismlardan ko‘p o‘ramli antenna va chipdan iborat.



8.8- rasm. Transponderning metall sirtida joylashtirilishi



8.9- rasm. Belgiga o‘rnatilgan elektron chipning umumlashtirilgan sxemasi

Aktiv belgi uchun konstruksiya tarkibiga ta‘minot manbai (masalan, litiyli batareya) qo‘yiladi.

Aktiv belgilarning passiv belgilarga nisbatan afzalliklari ma‘lumotlarni o‘qishning sezilarli katta uzoq masofaliligi (2-3

martadan ortiq) va o‘qish qurilmasiga nisbatan aktiv belgining yuqori ruxsat etiladigan harakatlanishi tezligi hisoblanadi.

Passiv belgilarning afzalliklari ularning deyarli cheklanmagan xizmat muddati (batareyalarning almashtirilishini talab qilmaydi) hisoblanadi. Passiv belgilarning kamchiliklari quvvatli ta’minot manbalariga ega bo‘lgan mos quvvatli o‘qish qurilmalaridan foydalanish zarurati hisoblanadi.

RFID-belgilarning afzalliklarini hozirgi vaqtda keng foydalaniladigan shtrix-kodlar bilan taqqoslashda kuzatish mumkin [24]. 8.1- jadvalda RFID tizimlarning boshqa avtomatik identifikatsiyalash tizimlari bilan taqqoslash xarakteristikallari keltirilgan.

8.1- jadval

RFID tizimlarning boshqa avtomatik identifikatsiyalash tizimlari bilan taqqoslash xarakteristikallari

Tizimning parametrlari	Shtrix-kod	Signal-larni optik tanish	Tovu shli identifikatsiya	Biometriya	Smart-kartalar	RFID
Xotiraning hajmi (bayt)	1-100	1-100	—	—	16-64K	16-64K
Ma’lumotlarning zichligi	Past	Past	O‘rta-cha	O‘rta-cha	Yuqori	Yuqori
Mashinali ishlov berish	Arzon	Arzon	Qimmat	Qimmat	Arzon	Arzon
Qo‘lda ishlov berish	Cheklangan	Oddiy	Oddiy	Murakkab	Mumkin emas	Mumkin emas
Kir/na mlkning ta’siri	Yuqori	Yuqori	—	—	Mumkin	Yo‘q
Qoplama sifatining ta’siri	To‘liq rad etish	To‘liq rad etish	—	Mumkin	—	Yo‘q
Joylashishining ta’siri	Past	Past	—	—	Bir tomon	Yo‘q

					ga yoʻnal- gan	
Eskirishi	Chek- langan	Chek- langan	—	—	Elekt- rodlar	Yoʻq
Appara- turaning narxi	Juda past	Oʻrta- cha	Juda yuqori	Juda yuqori	Past	Mum kin
Ekspluatat- sion sarflar	Past	Past	Yoʻq	Yoʻq	Oʻrta- cha	Yoʻq
Sanksiyal anmagan nusxa koʻchirish, oʻzgartirish	Mum kin	Mum- kin	Mum- kin	Mum- kin emas	Mum- kin	Mum kin
Oʻqish tezligi (s)	~ 4s	~ 3s	> 5s	> 5-10s	~ 4s	~ 0,5s
Maʼlumotlar tashuvchi va oʻqish qurilmasi orasidagi maksimal masofa	0-50 sm	< 1 sm	0-50 sm	Toʻgʻri kontakt	Toʻgʻri kontakt	0-5 m

8.2. Z-Wave texnologiyasi

Z-Wave uy avtomatizatsiyasi, xususan, turar-joy va tijorat obʻektlarini nazorat qilish uchun ishlab chiqilgan patentlashtirilgan simsiz aloqa protokoli hisoblanadi [5].

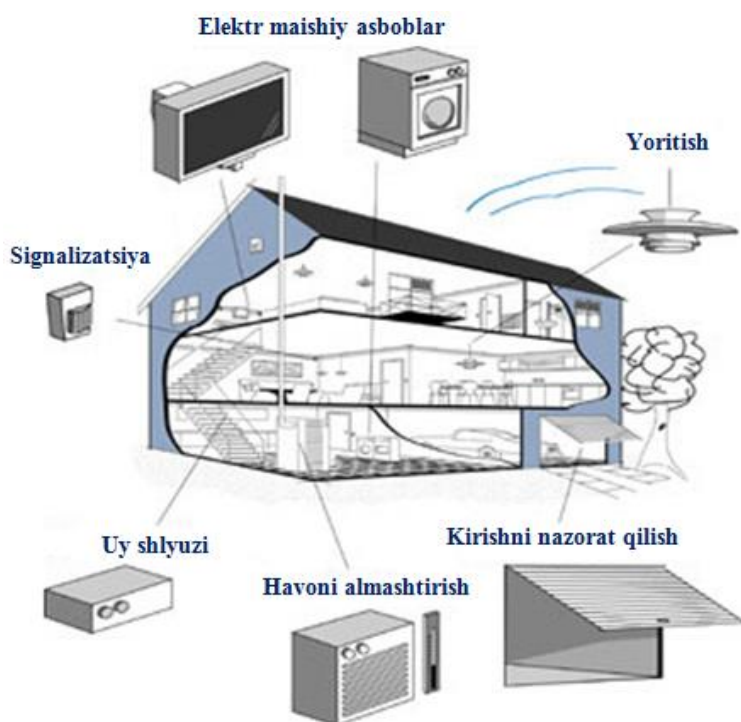
Uy avtomatizatsiyasi elektr tokdan ishlaydigan yoritish, isitish, ovqat tayyorlash, havoni almashtirish, xavfsizlik va boshqa barcha muhandislik tizimlarini oʻzaro birlashtirishgan va bu funksiyalarni avtomatlashtirilishini amalga oshirishga imkon beradi. Bu uylar va ofislarda xavfsizlik va qulaylikni oshirilishiga, elektr energiyasi va boshqa kommunal resurslarni tejashga olib keladi.

Z-Wave texnologiyasi yoritish, isitish, kirishni nazorat qilish, koʻngil ochish tizimlari va maishiy texnika kabi maishiy elektronika

va turli qurilmalarga o'rnatiladigan past quvvatli va kichkina radiochastotaviy modullarni ishlatadi (8.10- rasm).

Z-Wave turli industrial va ilmiy maqsadlar uchun ochiq bo'lgan ISM (Industrial-Scientific-Medical) polosasini ishlatadi. Chastota 868,42 MGsni tashkil etadi va taxminan 34 sm to'liq uzunligiga mos keladi.

Tizim qisqa vaqt davomida 10 mVtdan ortiq bo'lmagan maksimal quvvatni uzatish bilan ishlaydi. Bu atiga 1 mVt o'rtacha nurlantirish quvvatiga mos keladi. 1 metrga masofada Z-Wave radiosignalining inson organizmiga ta'siri darajasi mobil telefon nurlanishidan taxminan 4000 martaga kam.



8.10- rasm. Z-Wave texnologiyasining uy avtomatizatsiyasida ishlatilishi

Ma'lumotlarni uzatish tezliklari 9,6 kbit/s yoki 40 kbit/s, to'liq moslashuvchan ishlab to'ldirilgan protokolning versiyasi mavjud. Modulyatsiyalash turi Gauss filtrlashli chastotaviy modulyatsiyalash (GFSK – Gaussian Frequency Shift Keying) hisoblanadi. Ishlash radiusi to'g'ri ko'rinish sharoitlarida 30 metrlar atrofida, binoda devorlarning shakl va materialiga bog'liq ravishda kamayadi.

Simsiz tarmoqning har bir tuguni uni tarmoqdagi boshqa tugunlardan ajratish uchun noyob identifikatorga ega bo'lishi kerak.

Z-Wave protokoli tarmoqni tashkil etish uchun ikkita identifikatorni aniqlaydi :

- asosiy identifikator (Home ID) – bitta Z-Wave tarmoqqa kiradigan barcha tugunlar uchun 32 bit uzunlikdagi umumiy identifikator;

- tugun identifikatori (Node ID), u tarmoqdagi bitta tugunning manzili hisoblanadi. Tugun identifikatori 1 bayt = 8 bit uzunlikka ega bo‘ladi.

Turli asosiy identifikatorlarli tugunlar bir-birlari bilan aloqa qila olmaydi. Bitta Home ID orqali aniqlanadigan bitta tarmoq doirasida bir xil ID identifikatorlarli ikkita tugun bo‘lishi mumkin emas.

Z-Wave tarmog‘ida quyidagi ikkita asosiy qurilmalar turlari mavjud bo‘ladi:

- kontrollerlar – boshqa Z-Wave qurilmalarni boshqara oladigan qurilmalar;

- slave-tugunlar (ijrochi tugunlar) – boshqa Z-Wave qurilmalar nazorati ostida bo‘ladigan qurilmalar.

Slave-tugunlar standart va marshrutlashtiriladigan Slave-tugunlarga bo‘linadi. Marshrutlashtiriladigan Slave-tugunlar marshrutlashtirish jadvalini qisman bilish bilan asoslanadigan kengaytirilgan marshrutlashtirish funksiyalarili tugunlar hisoblanadi. Standart Slave-tugunlarda bunday ma’lumotlar bo‘lmaydi.

Kontrollerlar zavodda yaratilgan noyob individual asosiy identifikatorga (Home ID) ega bo‘ladi. Ijrochi tugunlar ma’lum Home ID identifikatorga ega bo‘lmaydi. Shuning uchun kontrollerlar o‘z Home ID identifikatorini boshqa Z-Wave qurilmalarga uzatishi va ularni o‘z Z-Wave tarmog‘iga qo‘shib olishi mumkin.

Kontrollerlar tarmoqdagi barcha talab qilinadigan tugunlarga xabarlarni jo‘natishi va zarur bo‘lganida kim bilan kerak bo‘lsa bog‘lanishi mumkin. Standart slave-tugunlar so‘ralmagan xabarlarni jo‘natishi mumkin emas, balki faqat so‘rovlarga javob beradi (slave-tugun faqat nima so‘ralganini berishi kerak). Marshrutlashtiriladigan Slave-tugunlar so‘rovlarga javob berishi mumkin va ular kontroller oldindan aniqlagan tugunlarga xabarlarni tarqatish huquqiga ega bo‘ladi.

Har bir tugun o‘zining to‘g‘ri simsiz ko‘rinishida qaysi tugunlar borligini aniqlash imkoniyatiga ega. Bu tugunlar qo‘shnilar deyiladi. Yoqilganida, keyin esa so‘rov bo‘yicha tugun kontrollerga o‘z qo‘shnilari ro‘yxatini xabar qilishi mumkin. Bu ma’lumotlardan

foydalanish bilan kontroller marshrutlashtirish jadvalini tuzadi, unda Z-Wave tarmog'idagi barcha bo'lishi mumkin marshrutlar haqidagi ma'lumotlar bo'ladi.

Asosiy kontrollerning marshrutlashtirish jadvali qurilma yoqilganidan keyin doimo tarmoqning haqiqiy holatini ko'rsatadi. Kontroller tarmoqning butun topologiyasini biladi va shuning uchun doimo talab qilinadigan tugun bilan haqiqiy bog'lanish yo'lini topishi mumkin (marshrutlashtirish jadvali to'g'ri va yangilanishi ko'zda tutiladi).

Dastlab kontroller xabarni yuborish tuguniga to'g'ridan-to'g'ri uzatishga urinadi. Agar bu mumkin bo'lmasa, u boshqa eng optimal yo'lni topish uchun marshrutlashtirish jadvalini ishlatadi. Kontroller uchtagacha muqobil marshrutlarni tanlanishi va ular yordamida xabarni uzatishga urinishi mumkin.

Shunday qilib, Z-Wave topologiyasi asosida yacheykali mesh-tarmoq texnologiyasi yotadi, unda har bir tugun aralash tugunlar zanjiridan foydalanish bilan boshqarish signallarini tarmoqning boshqa tugunlariga uzatishi va ulardan qabul qilishi mumkin. Masalan, tarmoqning ikkita qo'shni tugunlari orasida to'siq yoki jonsiz radiozona vujudga kelganida signal aloqani yo'qotgan tugunning ishlash radiusida bo'lgan aralash tugunlar orqali uzatiladi.

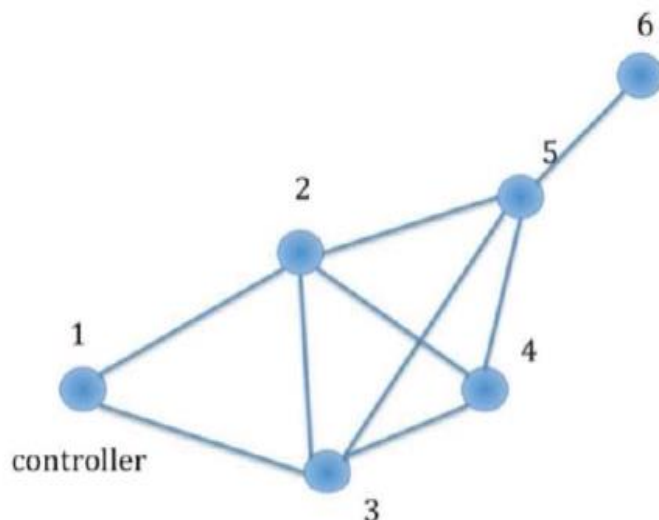
Qurilmalar oraliq tugunlar yordamida bir-birlari bilan aloqa qilishi va to'siqlar yoki jonsiz radiozonalarni chetlab o'tishi mumkin. A tugundan xabar S tugunga, hatto agar bu ikkala tugunlar aloqaning ishlashi radiusida bo'lmasa ham muvaffaqiyatli yetkaziladi. Bu A va S tugunlar bilan o'zaro ta'sirlasha oladigan uchinchi V tugun yordamida amalga oshiriladi. Agar afzal marshrut mumkin bo'lmasa, kontroller talab qilinadigan tugun bilan boshqa marshrutlar orqali bog'lanishga urinadi. Shunday qilib, Z-Wave tarmog'ining ishlash radiusi bitta tugunning uzatish masofasidan ancha katta bo'ladi.

Z-Wave to'rtta takrorlanadigan tugunlar orqali xabarlarni qayta uzatishi mumkin. Bu tarmoqning o'lchami va stabilligi, shuningdek tarmoqda xabarni yetkazishning maksimal ruxsat etiladigan vaqti orasidagi kelishtirish hisoblanadi.

Bir necha retranslyatorlardan foydalaniladigan mesh-marshrutlashtirishga misol 8.11- rasmda keltirilgan.

Slave-tugunlar ular so'ramagan ma'lumotlarni retranslyasiyalash imkoniyatiga ega bo'lishi uchun ular doimo aktiv bo'lishi kerak. Shuning uchun ko'proq kutish rejimida bo'ladigan batareyalardan

ta'minlanadigan tugunlar retranslyasiyalash qurilmalari sifatida ishlash uchun mo'ljallanmagan.



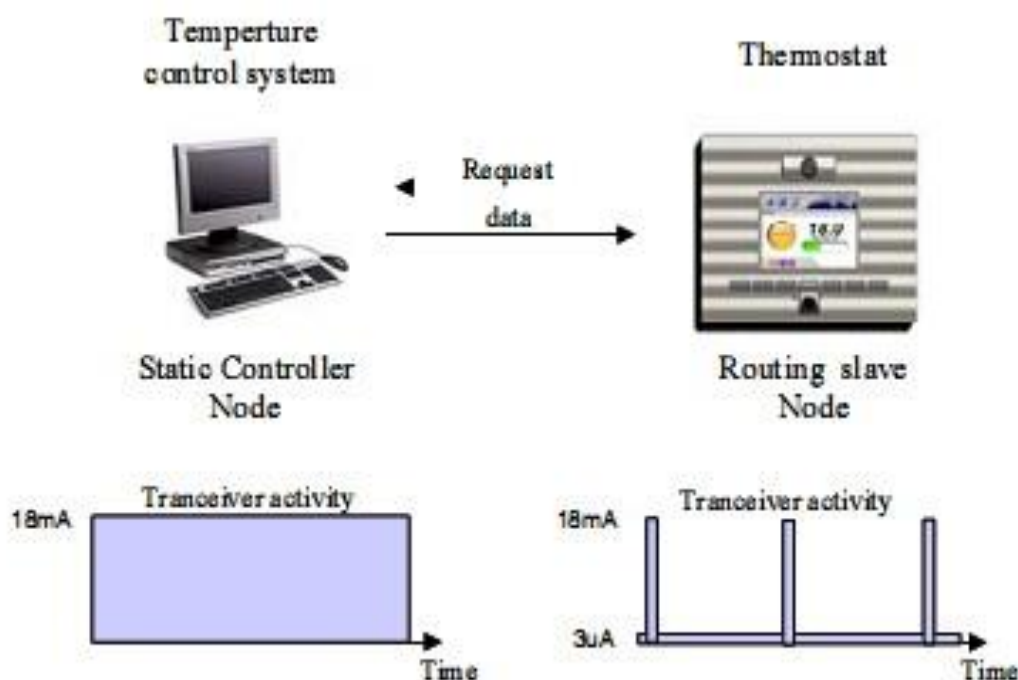
8.11- rasm. Bir necha retranslyatorlardan foydalaniladigan marshrutlashtirish

Bitta Z-Wave tarmog'i 232 tagacha tugunlarga ega bo'lishi mumkin va bunda agar yana bir necha qo'shimcha tugunlarni kiritish talab qilinsa, ko'priklar yordamida tarmoqni kengaytirish imkoniyatiga ega bo'lishi mumkin.

Batareyalardan ta'minlanadigan qurilmalar uchun AAA turdagi ikkita batareyalar bitta jamlanmasidan 10 va undan ortiq yillar qurilmalarning ishlashini ta'minlash uchun ta'minotni samarali boshqarish muhim. Shuningdek qurilmalarni taymer bo'yicha yoqish va keyingi kutish rejimiga o'tkazish samarali vositalari taqdim etiladi. 1.6- rasmda termostat (batareyalardan ta'minlanadigan) va haroratni boshqarish tizimlari tasvirlangan. Tizim kompyuterda doimo yoqilgan rejimda ishlaydi. Termostat davriy ravishda yoqiladi, joriy haroratni xabar qiladi va haroratni o'zgarishiga aktiv komandalar borligini so'raydi.

Z-Wave texnologiyasining oxirgi versiyalarida tarmoq topologiyasini yangi o'rganish mexanizmi joriy etilgan. Qurilmalarning surilishi yoki o'chirilishi keltirib chiqaradigan buzilgan marshrutlarni qayta tiklash uchun "Kadrlar o'tkazuvchisi" (explorer frames) ishlatilishi mumkin. Tarmoqni o'rganish kadrlarini uzatilishi uchun tarmoqlarni kesishli (pruning) qarorlarni qabul qilish daraxti prinsipi ishlatiladi. Shuning uchun ma'lumotlar hatto kontroller tarmoq topologiyasini haqiqiy bilmasada, jo'natish tuguniga

yetib borishi kerak. “Kadrlar o‘tkazuvchisi” barcha boshqa jo‘natish tuguni bilan bog‘lanishga urinishlar amalga oshmasa, oxirgi marshrutlashtirish varianti sifatida ishlatiladi.



8.12- rasm. Termostat (batareyalardan ta‘minlanadigan) va haroratni boshqarish tizimlari

Z-Wave alyansi bu hozirgi vaqtda uy avtomatizatsiyasi va boshqarish bozorida ishlaydigan taxminan 200 ishlab chiqaruvchilarni birlashtirgan ochiq konsorsium hisoblanadi. Ularga yana dasturiy ta‘minot ishlab chiquvchilari va yirik Z-Wave qurilmalari distribyuterlari kiradi. Z-Wave texnologiyasini ishlab chiquvchi Zensys (AQSh) kaliforniya kompaniyasi bo‘lib, u hozirgi vaqtda Sigma Designs kompaniyasiga tegishli.

Z-Wave texnologiyasining afzalliklari tez moslashuvchanlik, kam energiya iste‘moli, Z-Wave modullarini turli maishiy qurilmalarga past o‘rnatish narxi hisoblanadi.

Bu texnologiyaning kamchiliklariga ma‘lumotlarni past uzatish tezligi va alohida komandalarni uzatilishiga mo‘ljallangan uzatiladigan xabarlar uzunligiga (ish vaqtining 1% tartibida) cheklashlar kiradi. Cheklangan masshtablanuvchanlik va avtonom elektr ta‘minotining yo‘qligi bilan bir qatorda bu Z-Wave asosida ma‘lumotlarni to‘plash tarmog‘ini qurishga imkon bermaydi.

Nazorat savollari

1. RFID radiochastotali identifikatsiyalash qanday texnologiya?
2. RFID tizimida nechta asosiy aloqa turlari mavjud?
3. RFID tizimning asosiy komponentlarini bilasizmi?
4. Z-Wave tarmog'ida nechta asosiy qurilma turlari mavjud?
5. Z-Wave texnologiyasini tushuntiring.
6. Z-Wave texnologiyasi qayerlarda qo'llaniladi?

ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidenti SH.Mirziyoevning 2018 yil 3 fevraldagi “O‘zbekiston Respublikasi turizm salohiyatini rivojlantirish uchun qulay sharoitlar yaratish bo‘yicha qo‘shimcha tashkiliy chora-tadbirlar to‘g‘risida “ 5326-sonli Farmoni
2. Семенов Ю.А. Алгоритми телекоммуникационных сетей. Част 1. Алгоритмы и протоколы каналов и сетей передачи данных. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.РУ, 2007..
3. Новиков Ю.В., Кондратенко С.В. Основы локальных сетей. Интернет-университет информационных технологий - ИНТУИТ.РУ, 2005.
4. А.Х. Абдукадыров, Д.А. Давронбеков. Мобильные системы связи поколения 4G. - Ташкент. 2011. – 317 с.
5. Вишнеvский В., Ляхов А., Портной С, Шахнович И. Широкополосные беспроводные сети передачи информации М.: ЭКО-Трендз, 2005, 592 с.
6. Григорьев В.А, Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа М.: ЭКО-Трендз, 2005, 384 с.
7. ХТИ prezentatsiyasi. www.itu.int/ITU-D/tech/events/2007/.../Presentation_Moscow_TMuluk.pdf
8. Sayt WiMAX Forum. WiMAX 2 and WiMAX 2 Collaboration Initiative. <http://www.WiMAXforum.org/>
9. Стефен Ринг. Перспективы развития мобильной радиосвязи.
10. <http://www.projectmesa.org>
11. *Wireless Mobile Telephony*. Arian Durresi. CIS Department. The Ohio State University. <http://www.cis.ohio-state.edu/~durresi/>
12. Вишнеvский, С. Портной, И. Шахнович. Энциклопедия WiMAX. Пут к 4G. М: Техносфера, 2009. – 472с.
13. Пролетарский А.В., Баскаков И.В., Чирков Д.Н., Федотов Р.А., Бобков А.В., Платонов В.А. Беспроводные сети Wi-Fi. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.РУ, 2007.
14. Мерит Максим, Девид Полино. Безопасность беспроводных сетей. М.: Компания "АйТи"; ДМК Пресс, 2004, 288 с.
15. WiMAX forumi materiallari: <http://www.WiMAXforum.org/>

16. Vikipediya materiallari.
http://en.wikipedia.org/wiki/IEEE_802.16
17. WiMAX 802.16E: Подходы к качественному улучшению рабочих характеристик систем мобильного широкополосного доступа стандарта 802.16E. Klaus Daniel (Klaus Daniel), директор центра компетенции беспроводных систем связи компании в странах СНГ, 2007г. <http://www.mforum.ru/news/article/058869.htm>
18. Glore, N. & Mishra, A., Chapter 11 "Privacy and Security in WiMAX Networks" in "WiMAX Standards and Security" (Edited by M. Piyas & S. Ahson), CRC Press, June 2007.
19. Wireless.ru materiallari. <http://www.wireless.ru/clearwire-corporation-xotel-by-obedinit-WiMAX-i-lte/>
20. Mobil aloqa tizimlariga oid atamalarning ruscha-o'zbekcha izohli lug'ati. Fan-texnika va marketing tadqiqotlari markazi. Toshkent, 2008 y.
21. Simsiz foydalanish tizimlariga oid atamalarning ruscha-o'zbekcha izohli lug'ati. «UNICON.UZ» – Fan-texnika va marketing tadqiqotlari markazi Davlat unitar korxonasi. Toshkent, 2010 y.
22. www.lex.uz – Ўзбекистон Республикаси қонун ҳужжатлари Қонун ҳужжатлари маълумотлари миллий базаси.
23. Балонин Н.А., Сергеев М.Б. Беспроводные персональные сети на основе ZigBee. Учебное пособие. Санкт-Петербург. 2012 г.
24. Bluetooth, NFC, RFID. <http://knowledge.allbest.ru/programming/>.
25. Технология RFID. <http://hundure.ru/rfid.htm>.

MUNDARIJA

KIRISH.....	3
1-BOB. SIMSIZ KENG POLOSALI ALOQA TIZIMLARINING RIVOJLANISHI.....	6
1.1. Simsiz keng polosali ulanish texnologiyalarning rivojlanish tarixi va tavsifi	6
1.2. Simsiz keng polosali simsiz texnologiyalarni tasniflashga yondashishlar.....	8
1.3. Wi-Fi (IEEE 802.11) texnologiyasi	12
1.4. WiMAX (IEEE 802.16) texnologiyasi.....	14
2-BOB. Wi-Fi (IEEE 802.11 STANDARTI) SIMSIZ KENG POLOSALI ULANISH TEXNOLOGIYASI.....	16
2.1. IEEE 802.11 standartning arxitekturasi. IEEE 802.11 protokollar steki.....	18
2.2. IEEE 802.11 standarti muhitiga ulanish darajasi.....	19
2.3. IEEE 802.11 standartlari: IEEE 802.11; IEEE 802.11b standartlari	23
2.4. IEEE 802.11a, IEEE 802.11g va IEEE 802.11n standartlari.....	29
2.5. Simsiz tarmoqlarni tashkil etish va rejalashtirilish. Ad Hoc rejimi Infratuzilmali rejim, WDS, WDS with AP rejimlar...41	
2.6. Tarmoqlarning ishlash rejimlari va ularning tashkillashtirish xususiyatlari.....	47
3. WIMAX (IEEE 802.16 STANDARTI) SIMSIZ KENG POLOSALI ULANISH TEXNOLOGIYASI.....	56
3.1. WIMAX texnologiyasi haqida umumiy tushunchalar.....	56
3.1.1. WiMAX tizimining tavsifi.....	56
3.1.2. WiMAX tizimi va IMT-2000 dasturi.....	57
3.1.3. WiMAX tizimi va “raqamli tengsizlik” muammosi.....	60
3.1.4. WiMAX tizimining asosiy xarakteristikalar.....	62
3.1.5. WiMAX tizimlarining tarqalishi va qo‘llanish sohalari....	66
3.1.6. WiMAX tizimining afzalliklari va kamchiliklari.....	67
3.1.7. WiMAX va Wi-Fi tizimlarini taqqoslash.....	69
3.2. WiMAX (IEEE 802.16) standartlari.....	70
3.2.1. WiMAX standartlarining qisqacha rivojlanish tarixi.....	70
3.2.2. IEEE 802.16 standartlari oilasining tavsifi.....	73
3.2.3. IEEE 802.16 stanlartning qayd etilgan va mobil versiyalari.....	74
3.3. WIMAX tizimining arxitekturasi.....	82

3.3.1. WiMAX tizimi arxitekturasining asosiy prinsiplari.....	82
3.3.2. WiMAX tarmog‘i tugunlarining funkcionalligi.....	85
3.3.3. IEEE 802.16 standartidagi ish rejimlari.....	93
3.3.4. IEEE 802.16 standarti tarmog‘i fizik darajasining tavsifi.....	95
3.3.5. MAC darajasining ishlatilishi.....	108
3.3.6. QoS - xizmat ko‘rsatish sifati.....	111
3.3.7. Mobillikni boshqarish.....	113
3.4. WiMAX tarmog‘ini tashkil qilishning o‘ziga xos xususiyatlari, ishlash rejimlari va profillari.....	123
3.4.1. WiMAX profillari.....	123
3.4.2. WiMAX tarmog‘ining ishlash rejimlari.....	125
3.4.3. WiMAX tarmog‘ini tashkil etishning o‘ziga xos xususiyatlari.....	129
3.4.4. WiMAX tarmoqlarini loyihalashtirish va tashkil qilish...	134
3.5. WiMAX tarmoqlarida radiochastota diapazonidan foydalanish.....	143
3.5.1. WiMAX tizimlari uchun radiochastotalarni taqsimlashda butun dunyo an‘analari.....	143
3.5.2. WiMAX tizimlari uchun spektrni ajratishga bog‘liq muammolar.....	144
3.5.3. Turli chastotalar diapazonlarida va dunyoning turli davlatlarida spektrning taqsimlanishining o‘ziga xos xususiyatlari..	146
3.5.4. WiMAX texnologiyasining yaqin yillardagi rivojlanish istiqbollari.....	152
4-BOB. SIMSIZ TARMOQLARDA XAVFSIZLIK MASALALARI.....	154
4.1. Wi-Fi simsiz tarmoqlar xavfsizligiga tahdidlar va xavflar.....	154
4.2. Boshqarish kadrlaridan foydalaniladigan DOS – hujumlar.....	166
4.3. Zararli ulanish nuqtalari.....	169
4.4. Qo‘lga kiritish bilan hujum qilish.....	170
4.5. Simsiz tarmoqlarda qo‘llaniladigan kriptografiya usullari.....	173
4.6. Simsiz tarmoqlardagi autentifikatsiyalash usullari.....	179
4.7. WPA, WPA2 va 802.1x shifrlash protokollari	182
4.8. IEEE802.11 standartida abonentni autentifikatsiyalash prinsipi	190

4.9. Virtual xususiy tarmoqlarni qurish	195
4.10. Simsiz tarmoqlarda qo‘llaniladigan RADIUS va TACACS+ protokollarini taqqoslash.....	203
4.11. Uzatiladigan ma’lumotlarning yaxlitligi va konfidentsialligi	206
4.12. WiMAX tarmoqlarida axborot xavfsizligi masalalari.....	212
4.12.1. IEEE 802.16. standartidagi zaifliklar va hujumlar turlari.....	214
4.12.2. IEEE 802.16 standartida xavfsizlik tizimini tashkil etish	214
5-BOB. NFC TEXNOLOGIYALARINING QO‘LLANILISHI ISTIQBOLLARI	230
5.1. NFC texnologiyasi spetsifikatsiyasi.....	230
5.2. NFC texnologiyasini standartlashtirish va sanoat loyihalari.....	231
5.3. NFC aloqa rejimlari.....	234
5.4. NFC texnologiyasining qo‘llanilishi sohalari	237
5.5. NFC texnologiyalarining jahon mamlakatlarida joriy etilishi.....	240
5.6. O‘zbekistonda NFC-texnologiyalardan foydalanish istiqbollari.....	242
6-BOB. ZIGBEE TEXNOLOGIYASINING QO‘LLANILISHI.....	245
6.1. Zigbee texnologiyasining tavsifi.....	245
6.2. Zigbee tarmog‘ini qurish afzalligi.....	246
6.3. WPAN tarmoqlar va IEEE 802.15.4 standartlari.....	249
6.4. Zigbee tarmog‘ini qurish va ishlash prinsipi.....	258
7-BOB. BLUETOOTH TEXNOLOGIYASI.....	269
7.1. Bluetooth texnologiyasining tavsifi.....	269
7.2. Bluetooth texnologiyasining spetsifikatsiyalari.....	273
7.3. Bluetooth texnologiyasining protokollari steki va profillari.....	275
8-BOB. BOSHQA SIMSIZ KENG POLOSALI ULANISH TEXNOLOGIYALARI.....	281
8.1. RFID radiochastotali identifikatsiyalash texnologiyasi	281
8.2. Z-Wave texnologiyasi.....	290
ADABIYOTLAR.....	297

“Simsiz keng polosali texnologiyalar” fanidan darslik
(Telekommunikatsiya texnologiyalari – 5350100 ta’lim
yoʻnalishi uchun)

Mobil aloqa texnologiyalari kafedrasida majlisida muhokama etildi (26-majlis bayonnoma, 27.02.2018 y.) va koʻrib chiqish uchun tavsiya qilindi

Telekommunikatsiya texnologiyalari fakulteti ilmiy-uslubiy kengashida muhokama etildi, nashr etishga va universitet ilmiy-uslubiy kengashi tavsiya qilindi (7-sonli yigʻilish bayonnoma, 06.03.2018 y.)

Muhammad al-Xorazmiy nomidagi
TATU
ilmiy-uslubiy kengashi tomonidan chop etishga tavsiya qilindi
(9(110) sonli bayonnoma, 2018 yil
«20» 04).

Tuzuvchilar :

D.A. Davronbekov,

Sh.U.Pulatov,

M.O.Sultonova,

U.T. Aliyev,

E.B.Tashmanov.

Korrektor

S.Abdullayeva

Mas’ul muharrir:

T.D. Radjabov

Bosishga ruxsat etildi _____
Bichimi 60x84 1/16. bosma tabog‘i
Adadi Buyurtma №
Toshkent axborot texnologiyalari universiteti
“Nashr-matbaa” bo‘limida chop etildi.
Toshkent shahar, A.Temur ko‘chasi, 108-uy.