O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUXAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Mobil aloqa texnologiyalari kafedrasi

“Simsiz keng polosali texnologiyalar” fanidan ma’ruza ma’tinlari

(5350100–Telekommunikatsiya texnologiyalari ta’lim yo‘nalishi uchun)

Toshkent – 2017

Avtor: M.O.Sultonova. «Simsiz keng polosali texnologiyalar». / Muxammad al-Xorazimiy nomidagi TATU. 141 b. Toshkent, 2017

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. Бунда ma’ruzalarning ma’no jihatdan ketma-ketligi o’quv jarayonining modul tamoillariga va qo’shimcha o’quv axborotini olishga hamda talabalar bilimlarini mustahkamlashga undaydi.

Маъруза матнлари 5350100–Telekommunikatsiya texnologiyalari ta’lim yo’nalishi bo’yicha mutaxassislarni tayyorlashda ўқув жараёнида фойдаланиш учун мўлжалланган.

Taqrizchi: Mobil aloqa texnologiyalari
kafedra katta o’qituvchisi, t.f.n., Sh.U.Pulatov

Muxammad al-Xorazimiy nomidagi
Toshkent axborot texnologiyalari universiteti, 2017

Kirish

Ushbu ma’ruza ma’tinlari “Simsiz keng polosali texnologiyalar” fanidan o’qilayotgan ish rejasiga mos keladi va 5350100–Telekommunikatsiya texnologiyalari ta’lim yo’nalishi bo’yicha mutaxassislarni tayyorlashda asosiy fanlardan biri hisoblanadi. Bu fanni o’rganishda o’quv dasturida amaliy mashg’ulotlarni bajarilishi ko’zda tutilgan.

Talaba ushbu ma’ruza ma’tinlaridan IEEE 802.11 standartning arxitekturasini, protokollar stekini, IEEE 802.11a: IEEE 802.11b;IEEE 802.11g; IEEE 802.11n standartlarini, simsiz tarmoqlarning tashkil etish va rejalashtirilishni, infratuzilmali rejimni, WDS, WDS with AP rejimlarni, Ad Hoc rejimini, tarmoqlarning ishlash rejimlari va ularning tashkillashtirish xususiyatlarini, Wimax texnologiyasini, uning asosiy xarakteristikalarini, ishlash printsplari va rejimlarini, simsiz tarmoqlar xavfsizligiga tahdidlar va xavflarni, simsiz tarmoqlar xavfsizlik protokollarini, WEP shifrlash mexanizmini, simsiz tarmoqlarda audentifikatsiyalash WPA spetsifikatsiyasini, simsiz tarmoqlarda audentifikatsiyalashni 802.11i (WPA2), uzatiladigan ma’lumotlarning butunlik va konfedentsialli texnologiyasini, RFID, ZigBee, NFC, Bluetooth keng polosali ulanish texnologiyalarini, raqamli aloqa tizimlaridagi “signal-shovqin” nisbatini o‘rganishi nazarda tutilgan.

.

1-ma’ruza

Simsiz keng polosali ulanish texnologiyalari

Reja:

1. Simsiz keng polosali ulanish texnologiyalarining o’ziga xosligi.
2. IEEE 802.11 standartlari.

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 dipazonida 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.

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 uzaro 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 suzilarli 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‘lavermaydigan optik tolali yoki mis kabelni yotqizish va ijaraga olishni radi etish.

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 dipazonida 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 psevdo-tasodifiy 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 etadigan yirik shaharlar uchun xarakterli bo'lib qoldi. Natijada 2,4-2,5 GGs chastotalar diapazoni kuchli o'ta yuklangan va shovqinlashgan bo'lib qoldi.

Shovqinlashganlik muammosi ko'rsatilgan diapazon yaqinida GSM-1800 sotali aloqa, radioreleli aloqa tizimlari, idoraviy vatijorat 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 echilishining bo'lishi mumkin yo'llarini, ma'lumotlarni simsiz uzatish

tarmoqlarida radioaloqa sifatini yaxshilashga asosiy yondashishlarni tahlil qilish dolzarb hisoblanadi.

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 a 2 Mbit/sekund ulanish tezliklarida ishlaydigan radioqurilmalar a tarmoqlar uchun umumiy standartni ishlab chiqish bilan shug‘ullandi. Standart ustida ishlar 7 yildan keyin yakunlandi va 1997 yilning iyunida birinchi 802.11 spesifikatsiya 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.

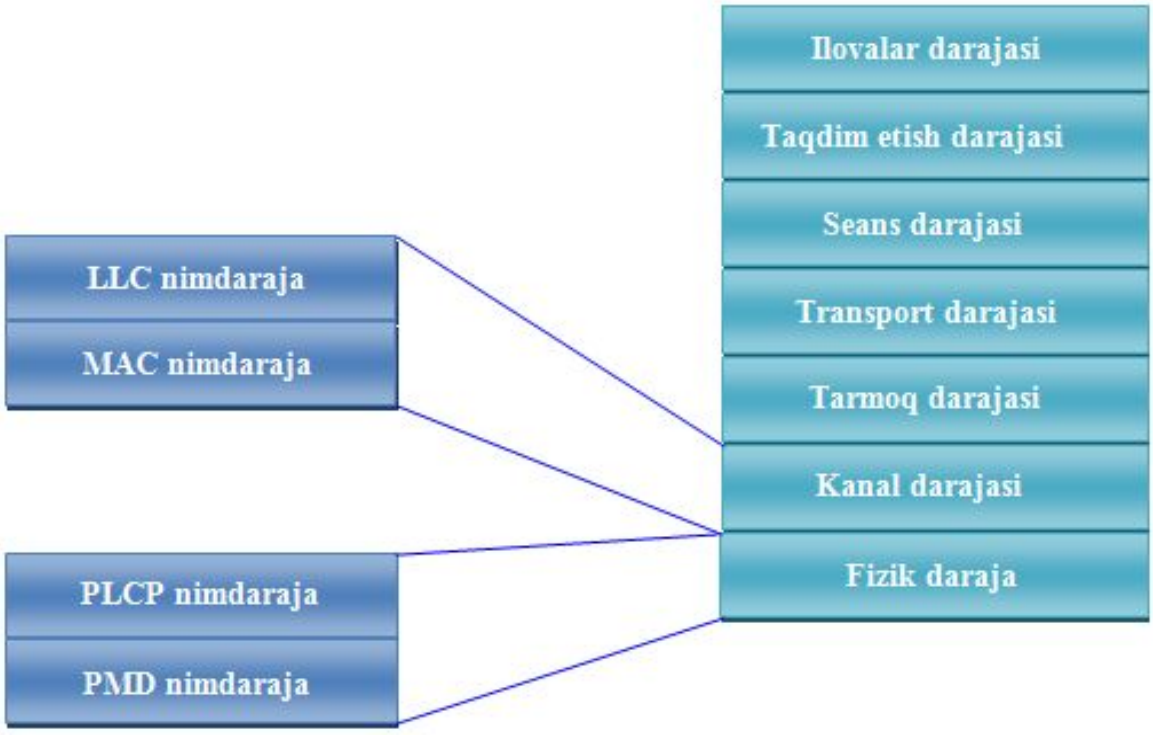
802.11 standartlari to‘plami 802.11 MAS nimdarajasi bilan ishlatilishi mumkin bo‘lgan fizik darajaning (Physisal Layer Protocol-PHY) qator ishlatilishi texnologiyalarini aniqlaydi. PHY darajalari quyidagilar (1.1-rasm):

- 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 Phisical 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 ishlailishiga 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.



1.1-rasm. PHY darajaning nimdarajalari

PLCP nimdaraja borligicha simsiz muhit orqali ma’lumotlarni u yoki bu uzatish va qabul qilish usuli ishlatiladigan PMD nimdarajasidan foydalaniladigan

MAS-stansiyalar orasida MAS protokoli ma’lumotlari elementlarining (MAS 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 tashkl etuvchilarining qo‘llanilishi hisobiga olinadigan ko‘plab avzalliklarini 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 tuziomalashtirilganidan 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 de-skrembleri keyin dastlabki tuzilmalashtirilgan ketma-ketlikni olish uchun tasodifiy ketma-ketlikni teskari o‘zgartirishni bajaradi. Ko‘plab skremblirlash usullari o‘zi sinxronlashadigan usullarga kiradi. Bu de-skrembler skrembler orqali mustaqil sinxrolashtirilishi mumkinligini bildiradi.

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. Skremblirlash nima?

2-ma’ruza

IEEE 802.11 standartning arxitekturasi. IEEE 802.11 protokollar steki

Reja:

1 IEEE 802.11 standarti muhitiga ulanish darajasi

2. IEEE 802.11 protokollari steki

Tabiiyki, IEEE 802.11 standarti protokollari steki 802 qo‘mita standartlarining umumiy tuzilmasiga mos keladi, ya’ni MAS (Media Access Control) darajasiga ulanishni va LLS (Logical Link Control) ma’lumotlarni mantiqiy uzatishni boshqarish nimdarajalarili fizik va kanalli darajalardan tashkil topgan. 802 oilaning barcha texnologiyalaridagi kabi 802.11 texnologiya ikkita pastki, ya’ni fizik daraja va MAS daraja orqali aniqlanadi, LLS darja esa barcha LAN texnologiyalari uchun umumiy standart bo‘lgan o‘z funksiyalarini bajaradi (1-rasm).

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

IEEE 802.11 standarti muhitiga ulanish darajasi

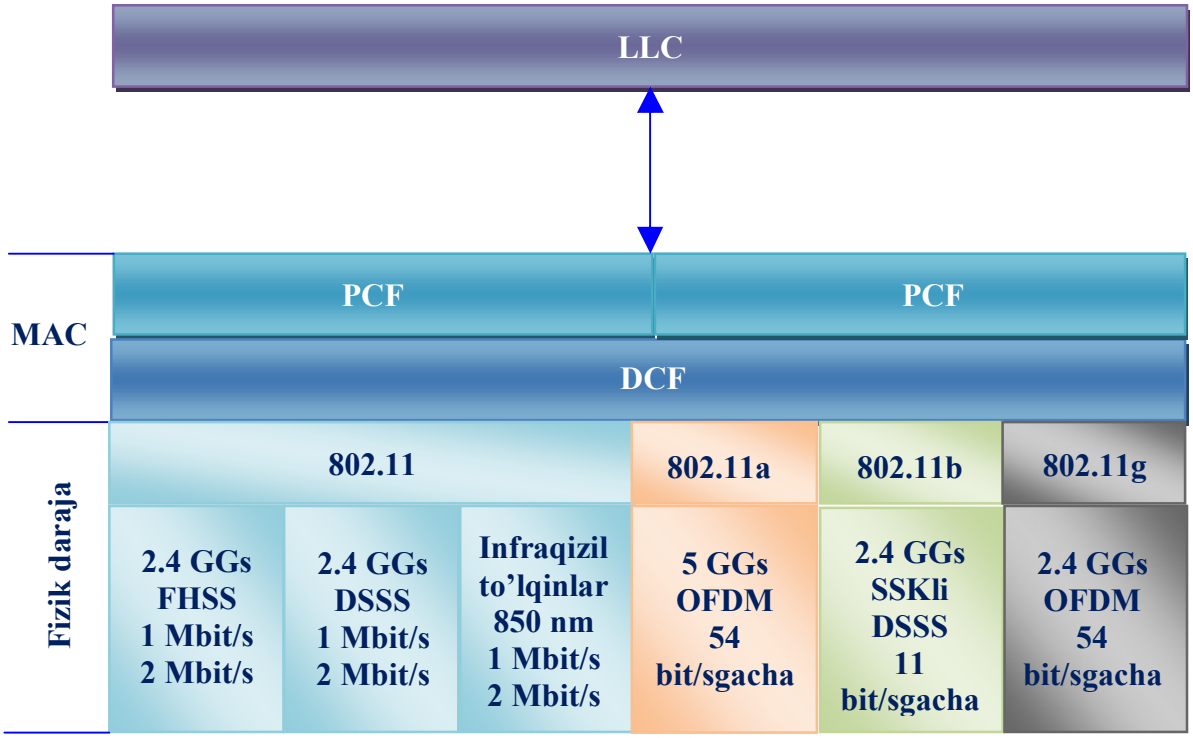
IEEE 802.11 tarmoqlarda MAS daraja ajratiladigan muhitga ikki ulanish rejimini ta’minlaydi (2.1-rasm):

- 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. Simsz 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.



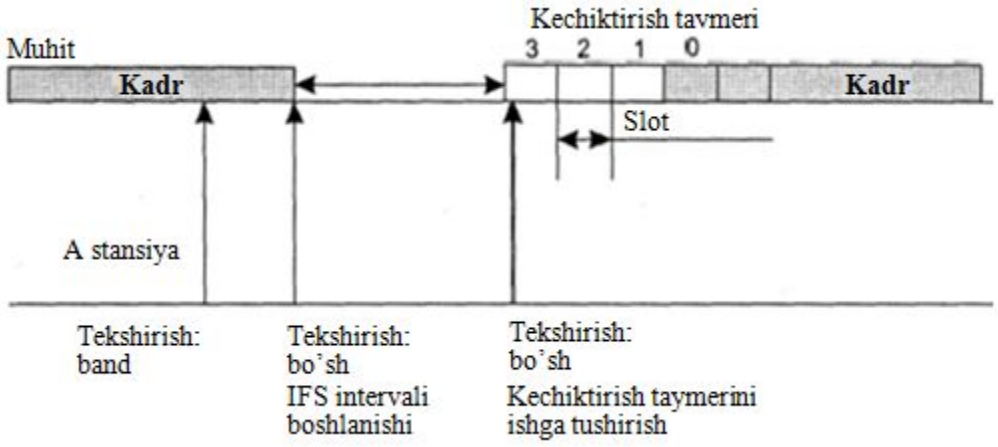
2.1-rasm. IEEE 802.11 protokollari steki

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 (2.2-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‘sag‘aviy qiymat 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.

Bu yetarlicha oson bo‘lmagan ulanish usulini 2.2-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 ayriladi, va agar natija nolga teng bo‘lsa kadrni uzatish boshlanadi.



2.2-rasm. DSF ulanish rejimi

Shunday qilib, barchaslotlarning, shu jumladan tanlangan slotning band bo‘lmasligi 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 siklдagidek, 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.

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.

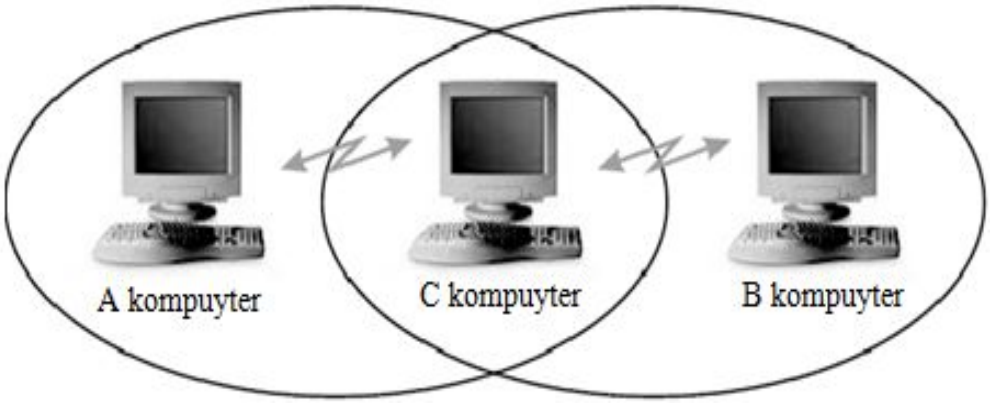
Kolliziya faqat bir necha stansiyalar uzatish uchun o‘sha bir slotni tanlagan hollarda o‘z o‘rniga ega bo‘lishi mumkin.

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 (3-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.



2.3-rasm. Yashirin terminal muammosi

Nazorat savollari

1. IEEE 802.11 tarmoqlarda MAS daraja ajratiladigan muhitga nechta ulanish rejimini ta’minlaydi?
2. DSF ulanish rejimini tushuntiring
3. Kolliziya nima?
4. Yashirin terminal muammosi nima?

3-ma’ruza

IEEE 802.11 standartlari: IEEE 802.11; IEEE 802.11b standartlari

Reja:

1 IEEE 802.11 standartlari.

2. 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.

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 standart

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, shipdan 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/sekunduzatishtezliklarida 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.

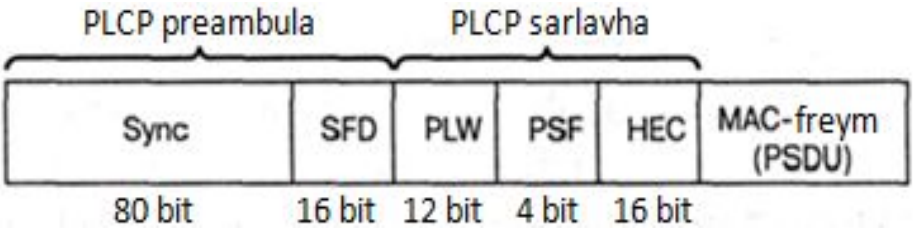
Chastotani qayta sozlanishi ketma-ketligi quyidagi parametrlarga ega bo‘lishi kerak: sakrab o‘tishlar chastotasi minimum 6 ta kanallar orasida (6 MGs) sekundiga 2,5 marttadan kam bo‘lmasligi kerak. Berkitiladigan qoplash zonalari kolliziyalar sonini minimallashtirish uchun bo‘lishi mumkin sakrab o‘tishlar ketma-ketligi uchta ketma-ketliklar to‘plamiga bo‘linishi kerak, ularni uzunligi Shimoliy Amerika va Yevropaning katta qismi uchun 26 ni tashkil etadi. 1-jadvalda minimalberkitilishni ta’minlaydigan chastotani sakrashsimon qayta sozlash sxemasi keltirilgan.

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.

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. 1-rasmda PLCP nimdaraja FHSS freymining formati keltirilgan.



3.1-rasm. PLCP nimdaraja FHSS freymining formati

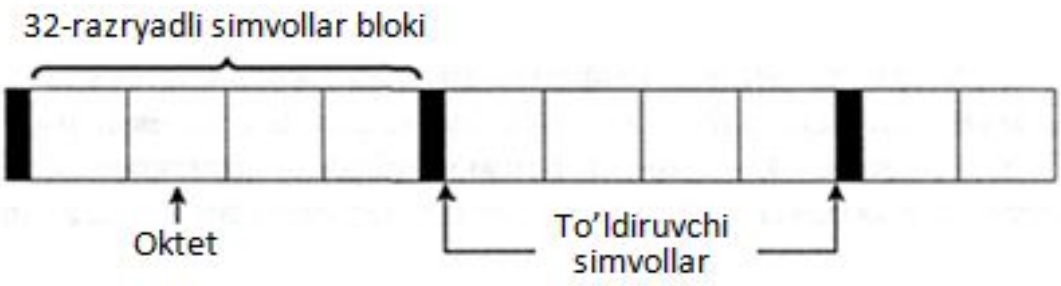
PLCP preambulasi ikki maydonchalardan iborat:

- *80 bit o'lchamli Syns maydonchasi*. 0 va 1 lar 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 sinxrolashtirilishini (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 3.2-rasmda keltirilgan. To‘ldiruvchi simvollar barcha 32-simvolli 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.



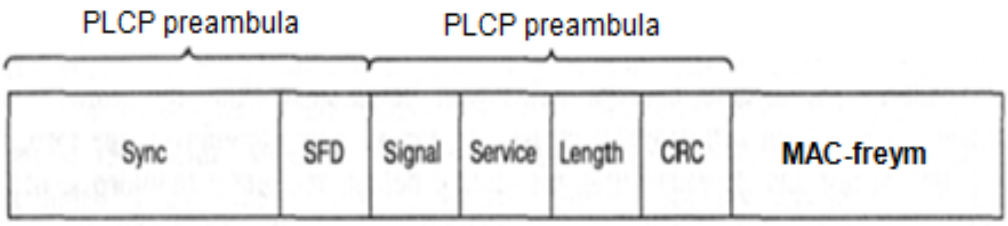
3.2-rasm. FHSS texnologiyasidagi skrembirlangan PSDU

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 3.3-rasmda keltirilgan.



3.3-rasm. PLCP nimdaraja DSSS freymi formati

PLCP preambulasi ikkita maydonchalardan tashkil topgan:

- *Birlardan iborat satr bo‘lgan 128 bit kenglikdagi Syns maydonchasi.* Bu maydonchaning vazifasi qabul qiluvchi stansiya uchun sinxronlashtirishni ta’minlash hisoblanadi;
- *16 bit kenglikdagi SFD maydoncha.* Unda o‘zga xos OxF3A0 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 zahiralashtirilgan.* Bu standart spesifikatsiyasini ishlab chiqish vaqtida noaniq qoldi. U standartning bo‘lajak modifikatsiyalarida kerak bo‘ladi;
- *MAS-freym qismini uzatish uchun zarur bo‘ladigan mikrosekundlar sonini ko‘rsatadigan 16 bit kenglikdagi Length maydonchasi;*
- *CRC maydoncha.* 16-bitli nazorat yig‘indisi.

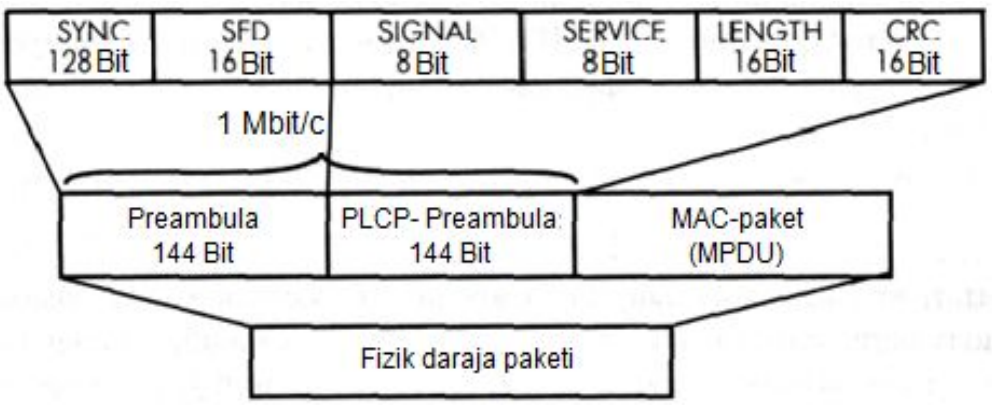
PLCP nimdaraja freymni bitlar oqimiga o‘zgartiradi va uni PMD nimdarajaga uzatadi. Butun PRDU ma’lumotlarni randomizatsiyaash maqsadida skrembirlash jarayoni orqali o‘tadi.

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).

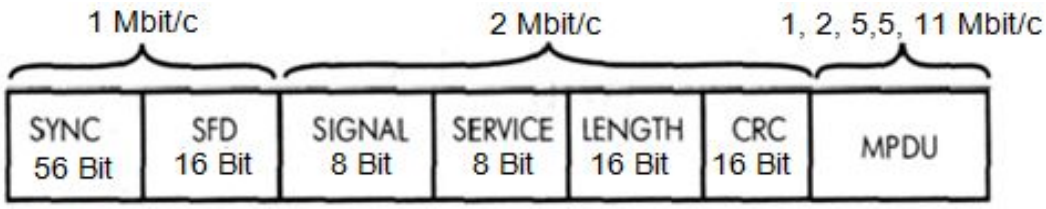
IEEE 802.11b standarti

Fizik darajada MAS-kadrlarga (MRDU) preambula va o‘z PLCP-sarlavhasidan iborat fizik daraja sarlavhasi qo‘shiladi (3.4-rasm). Preambula qabullagichni sozdash 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.



3.4-rasm. IEEE 802.11b tarmog‘i fizik darajasi kadrlari tuzilmasi

IEEE 802.11b standartda ikki uzun va qisqa turlardagi sarlavhalar ko‘zda tutilgan (3.5-rasm).



3.5-rasm. IEEE 802.11b tarmog‘i kadrlar qisqa sarlavhasi

Nazorat savollari

1. IEEE 802.11standartini tushuntiring
2. PLCP freym sarlavhasi nechta maydonchalardan iborat?
3. PLCP sarlavhasi nechta maydonchalardan tashkil topgan?
4. IEEE 802.11b tarmog‘i fizik darajasi kadrlari tuzilmasini tushuntiring

4-Маъруза

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

Reja:

1 IEEE 802.11a standarti

2. 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 maълumot 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 etarli 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.

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 modulyasiyalash tomonidan o‘zgartirildi. OFDM ko‘plab nimchastotalarda maълumotlarni parallel uzatishga imkon beradi. Bu halaqitlarga barqarorlikni oshiradi va bittadan ortiq maълumotlar oqimlari uzatilar ekan, yuqori o‘tkazish qobiliyati taъminlanadi.

IEEE 802.11a idealsharoitlarda 54 Mb/sgacha tezliknitaъminlashi 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 teliklarda ishlashi mumkin.

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 taъminlash va bu bilan 11 Mbit/s ulanish tezligini taъminlaydigan 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 taъminlaydi. IEEE 802.11g standartning teskari moslashuvchanligi DSSS modulyasiyalash rejimda va bog‘lanish tezligi sekundiga 11 megabitgacha cheklanganida yoki tezlik 54 Mbit/sgacha etishi mumkin bo‘lgan OFDM modulyasiyalash 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 maъlumotlarni uzatish tezligini deyarli to‘rt marttaga oshiradi. Nazariy jihatdan 802.11n maъlumotlarni birdaniga to‘rtta antennalar bo‘yicha uzatishni qo‘llash bilan 600 Mbit/sgacha maъlumotlarni uzatish tezligini taъminlay 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‘llash taъminlanadigan olingan (Legacy) rejim;
- 802.11b/g, 802.11ai 802.11n qurilmalarini qo‘llash taъminlanadigan aralash (Mixed) rejimi;
- “toza” 802.11n rejim (aynan bu rejimda 802.11n standarti taъminlaydigan oshirilgan tezlik va oshirilgan maъlumotlarni uzatish masofasi ustunliklaridan foydalanish mumkin).

802.11n standartning xomaki versiyasini (DRAFT 2.0) ko‘plab zamonaviyqurilmalar qo‘llaydi. Standartning yakuniy versiyasi (DRAFT 11.0) 2009 yilning 11 sentyabrida qabul qilingan va 300 Mbit/sgacha tezlik, MIMO sifatida maъlum bo‘lgan ko‘p kanalli kirish/chiqish va katta qamrab olishni taъminlaydi.

Standartning o‘ziga xos xususiyatlari

Maъlumotlarni real uzatish tezligi

Maъlumotlarni real uzatish tezligi doimo kanalli tezlikdan past bo‘ladi. Wi-Fi uchun ma’lumotlarni real uzatish tezligi odatda kam tomonga ikki marttadn 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).

Taъkidlash kerakki, 802.11b standartda ishlashda yoki u bilan moslashadigan rejimnitaъminlashda faqat uchta bir-birlarini qoplamaydigan, yaъni bir-birlariga halaqit qilmaydigan (odatda 1-nchi, 6-nchi va 11-nchi) kanallar mavjud bo‘ladi. Ya’ni, agar devorning ortida qo‘shnida ulanish nuqtasi 1-nchi kanalda ishlayotgan bo‘lsa, sizda esa uyda 3-nchi kanal bo‘lsa, u holda bu ulanish

nuqtalari bir-birlariga halaqit qiladi, bu bilan maъlumotlarni ulanish tezligini pasaytiradi.

Ikkkita chastotalar diapzonlari

802.11n standart bo‘yicha qurilmalar 2,4 yoki 5 GGs diapzonlarini ishlatishi mumkin, bu radiochastotali halaqitlar taъsirini 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 echim o‘tkazish qobiliyatini oshiradi. Taъkidlash kerakki, 2,4 GGs diapazonda faqat ikkita kesishmaydigan keng polosali kanalni joylashtirish mumkin.

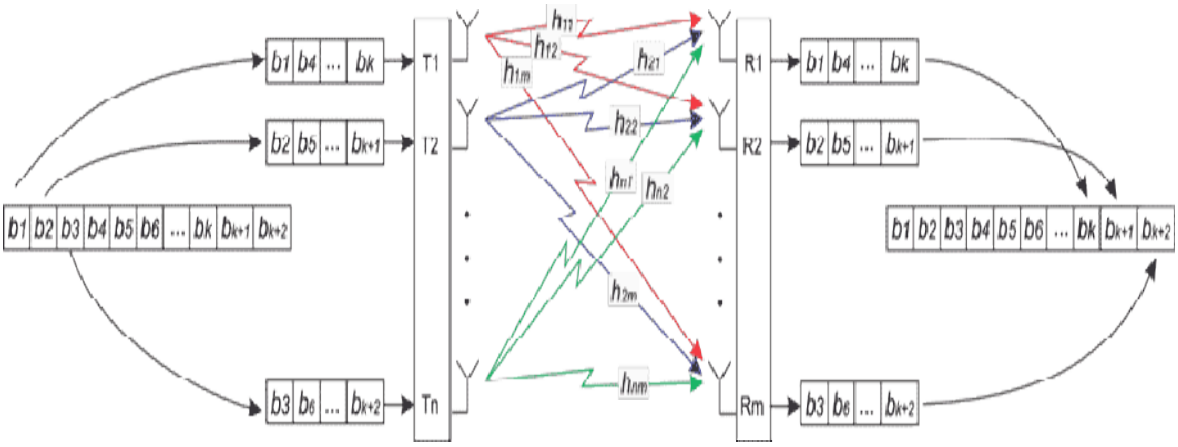
802.11n standarti muhim yangi joriy etish MIMO (ingl. *Multiple Input, Multiple Output* — «ko‘p kirishlar, ko‘p chiqishlar») kiritadi, u yordamida fazoviy multiplekslash – bir necha axborot oqimlarini bitta kanal bo‘yicha bir vaqtda uzatish, shuningdek signalni etkazilishi uchun halaqitlar taъsiri va maъlumotlarni yo‘qotilishini minimallashtiradigan, lekin bir necha antennalarning bo‘lishini talab qiladigan ko‘p nurli tarqatishdan foydalanish amalga oshiriladi. Aynan maъlumotlarni 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, yaъni 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 marttaga katta maksimal o‘tkazish oralig‘ini taъminlashi mumkin. Bu uzatkich maъlumotlarni oqimini mustaqil bitlar ketma-ketliklariga bo‘lishi va ularni antennalar massividan foydalanish bilan qayta uzatishi orqali erishiladi. Bunday uzatish texnikasi fazoviy multiplekslash deyiladi.

Taъkidlaymizki, barcha antennalar maъlumotlarni bir-birlariga bog‘liq bo‘lmagan holda o‘sha bir chastotalar dipazonida uzatadi.

n ta uzatish va *n* ta qabullash antennalaridan iborat bo‘lgan MIMO-tizimini ko‘rib chiqamiz (4.1-rasm).



4.1-rasm. MIMO texnologiyasining ishlatilishi prinsipi

Bunday tizimda uzatkich *n* ta o‘zaro bog‘liq bo‘lmagan signallarni *n* ta antennalarni qo‘llash 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 *R1* signalni quyidagi ko‘rinishda berish mumkin:

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

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

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

Yoki bu ifoda matritsali ko‘rinishda yozilsa:

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

bu erda $[H]$ — MIMO-aloqa kanalini tavsiflaydigan o‘tkazish matritsasi.

Qabullash tomonida dekoder barcha signallarni qayta tiklay olishi uchun u avvalo m x 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 erda $[H]^{-1}$ — $[H]$ o‘tkazish matritsasi teskari matritsa.

Taъkidlash 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.

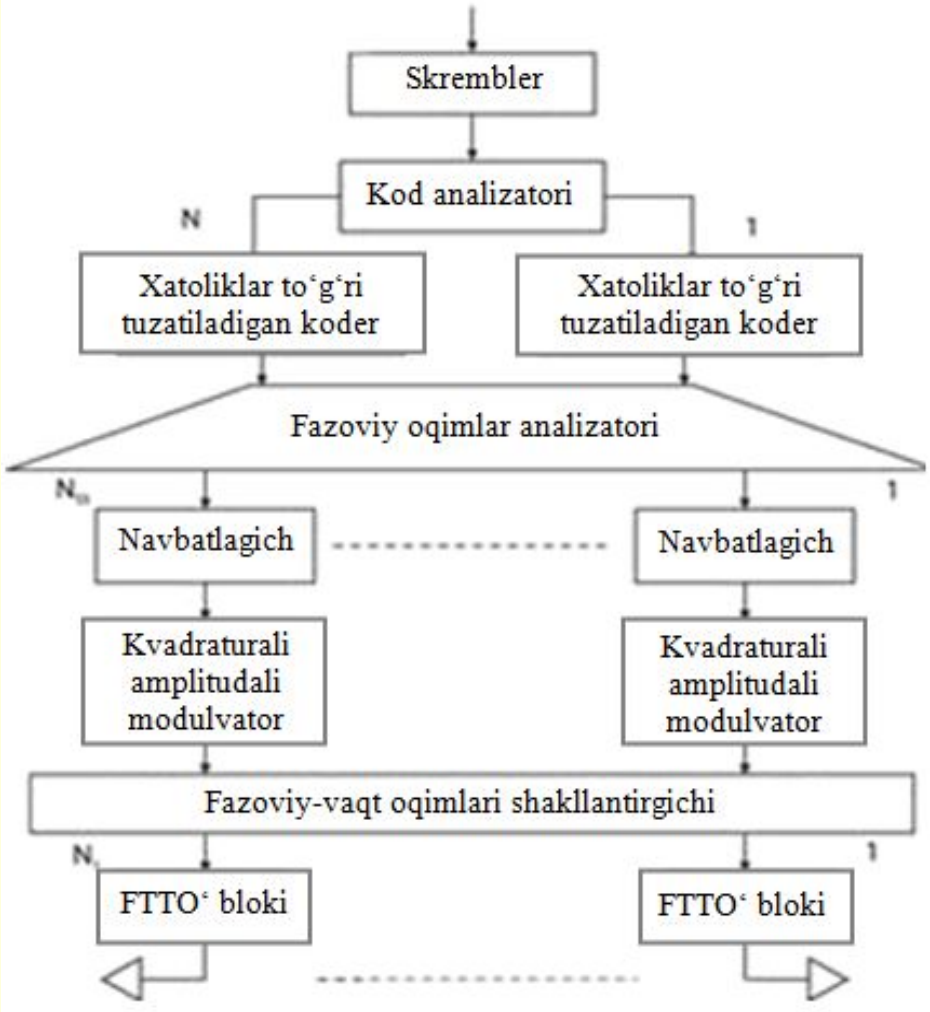
MIMO texnologiyasi kodlash usuliga hech qanday taъsir etmaydi va prnsip jihatdan istalgan maъlumotlarni fizik va mantiqiy kodlashusullari bilan birgalikda ishlatilishi mumkin.

802.11n uzatkichi va qabullagichi

IEEE 802.11n standartida ulanish nuqtasi va simsiz adapterda to‘rttagacha antennalardan foydalanishga ruxsat etiladi. Majburiy rejim ulanish nuqtasida ikkitta 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-rasmda tasvirlangan. Uzatiladigan maъlumotlar bir xil simvollarning uzun ketma-ketliklaridan qochish uchun kodga qo‘shimcha nollar va birlarni qo‘yadigan (psevdo-tasodifiy shovqin bilan

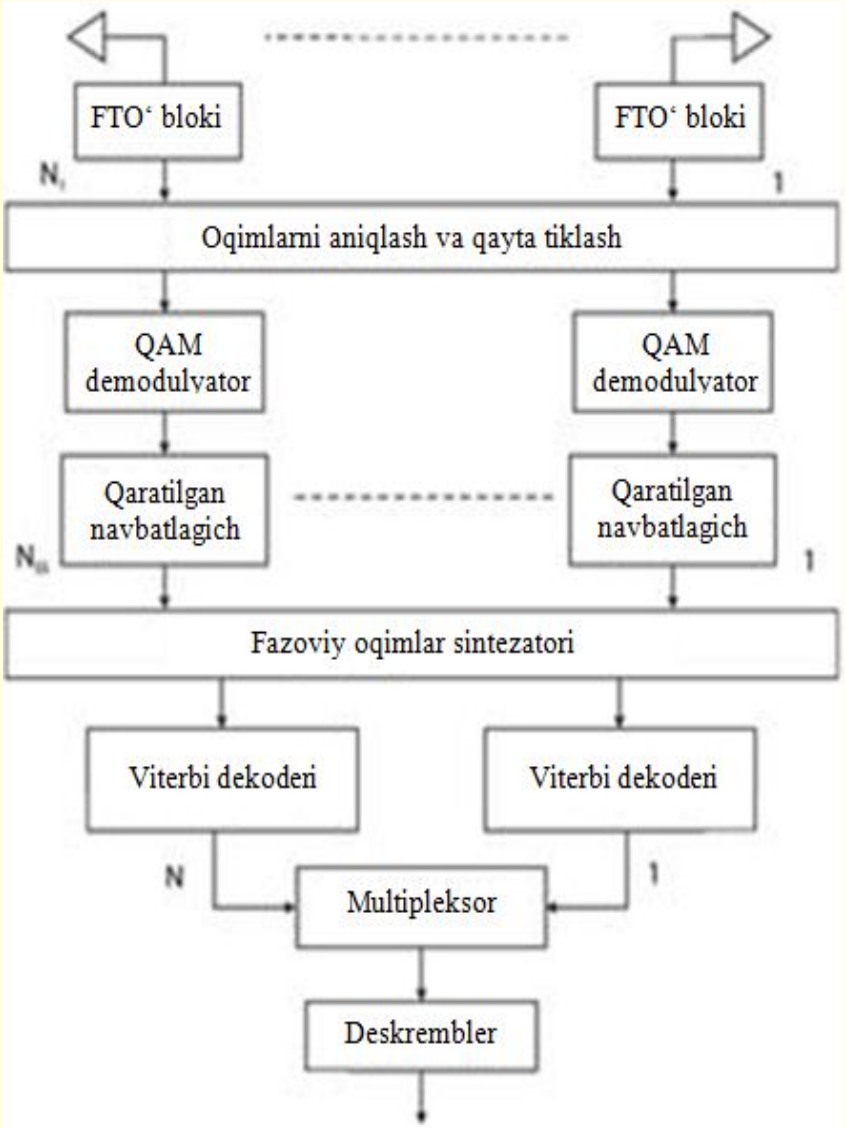
niqoblash) skrembler orqali o‘tadi. Keyin maъlumotlar N oqimlarga bo‘linadi va xatoliklar to‘g‘ri tuzatiladigan koderga (FEC) beriladi. Agar uchta yoki to‘rtta uzatish kanallari ishlatilsa, bir yoki ikkita antennalarli N = 1 oqimli tizimlar uchun N = 2 bo‘ladi.



4.2-rasm. MIMO-OFDM uzatkichining umumiy tuzilmasi

Kodlangan ketma-ketlik alohida fazoviy oqimlarga bo‘linadi. Har oqimdagi bitlar navbatlashadi (blokli xatoliklarni yo‘qotish uchun), keyin esa modulyasiyalanadi. Keyin Furъe tez o‘zgarirish 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 4.3-rasmda tasvirlangan.



4.3-rasm. MIMO-OFDM qabullagichining umumiy tuzilmasi

Antennalar

IEEE 802.11n qurilmalarida odatda maъlumotlarni 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

maъlumotlarni uzatmaydi, balki yuklaydi) sxemani ishlatadi. Maъlumotlarni uzatish tezligiga oshirilgan talablarli foydalanuvchilar 4×4 konfiguratsiyali antennalarli modellarni ishlatishi mumkin bo‘ladi.

Ethernet tarmog‘i orqali taъminot

IEEE 802.3af-2003 (PoE) tarmoq taъminoti standarti 3×3 va undan yuqori antennalar konfiguratsiyalarili ulanish nuqtalarining elektr taъminoti uchun zarur bo‘ladigan quvvatni taъminlamaydi. Uni almashtirishga maksimal quvvatni ikki marttaga oshirilishini ko‘zda tutadigan IEEE 802.3at-2009 keldi, bu 4×4konfiguratsiyali antennalarli qurilmalarni taъminlash uchun etarli bo‘ladi.

Tarmoqdagi zaif joylar

Bu standartni qo‘llaydigan ulanish nuqtalarida o‘tkazish qobliyati 100 Mbit/sdan ortishini hisobga olganda, Fast Ethernet kanallari tarmoq trafigi yo‘lida zaif joy bo‘libqolishi 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 802.11ntarmoqlarida yana bir qancha vaqt eskirgan standartlarni ishlatadigan mijozlar ishlab turadi, shuning uchun simsiz LHTlarni qurishda ularniqo‘llashniko‘zda tutish kerak bo‘ladi.

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.

Modulyasiyalash 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 uzati va 4 ta qabullash antennalarida erishish mumkin.

802.11n standarti modulyasiyalash indeksi va kodlash sxemalarini (ingl. *modulation and Coding Scheme. MCS*) 0 dan (eng sekin, lekin ishonchli rejimga mos keladi) 31 gacha (eng tezeor, lekin radiohalaqitlarga sezgir rejim) butun sonlar ko‘rinishida aniqlaydi. Indeks radiochastotani modulyasiyalash 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/sgacha nazariy maълumotlarni uzatish tezligini aniqlaydi.

Modulyasiyalash turi (masalan, 802.11dan BPSK yoki 802.11a dan QAM) va kodash tezligimaълumotlarni efirga uzatish tezligini aniqlaydi. Yangiroq modulyasiyalash turlari samaraliroq va yuqoriroq maълumotlarni uzatish tezliklarini taъminlashi mumkin, eskiroqlari esa teskari moslashuvchanlikni taъminlash xizmat qiladi. 300 Mbit/s maksimal bog‘lanish tezligiga erishish uchun ham ulanish nuqtasi, ham mijoznig qurilmasi ikkita fazoviy oqimni va ikkilangan 40 MGs kanal kengligini taъminlashi kerak.

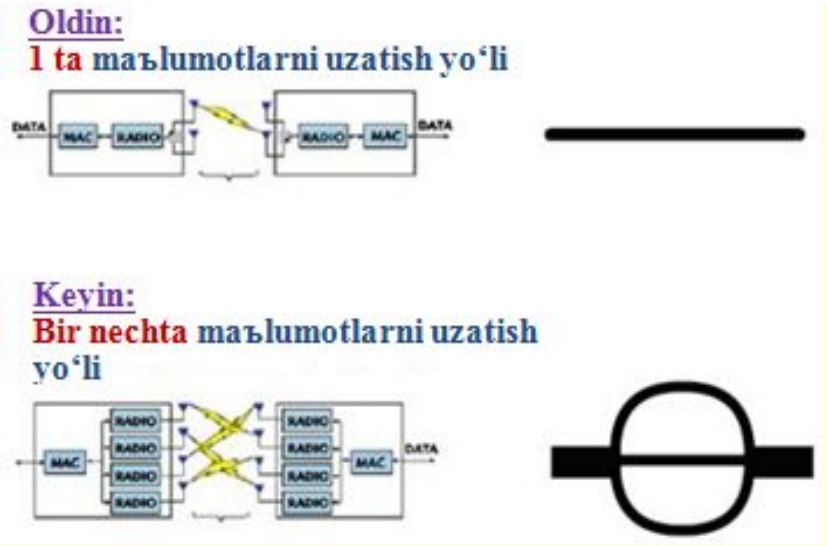
802.11n spetsifikatsiyasi 2009 yilning 11 sentyabrida tasdiqlangan

802.11n standartida maълumotlarni yuqoriroq tezliklarda uzatilishi omillari

Yuqorida aytilganidek, 802.11n standartida maълumotlarni uzatish teligini oshirish uchun uchta asosiy mexanizmlar qo‘llaniladi:

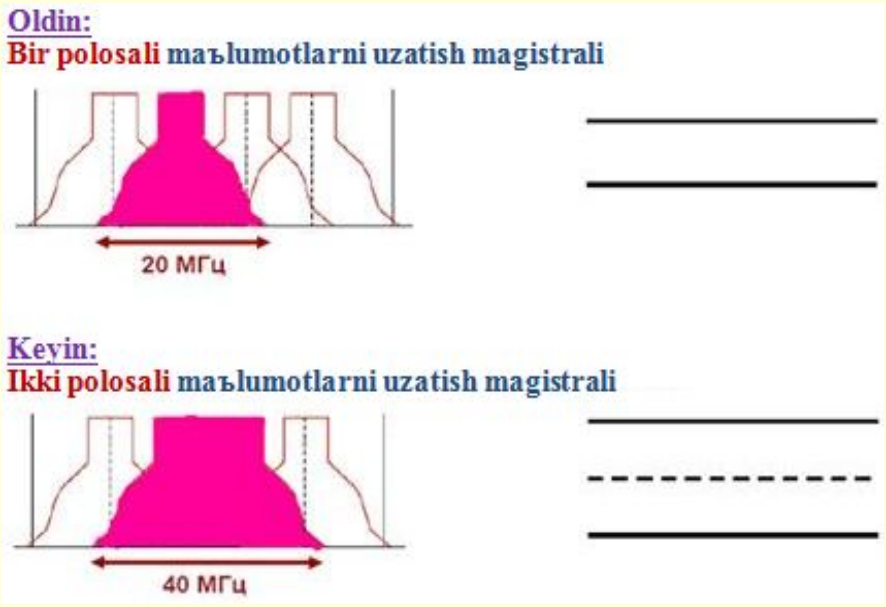
- bir necha qabullagich-uzatikichlar va radiosignalning maxsus uzatish va qabullash algoritmlarining qo‘llanilishi;
- signal chastotalar polosasini 20 dan 40 MGsgacha oshirilishi;
- tarmoqqa ulanish darajasi protokolini optimallashtirish.

Bu mexanizmlardan har birini ko‘rib chiqamiz.



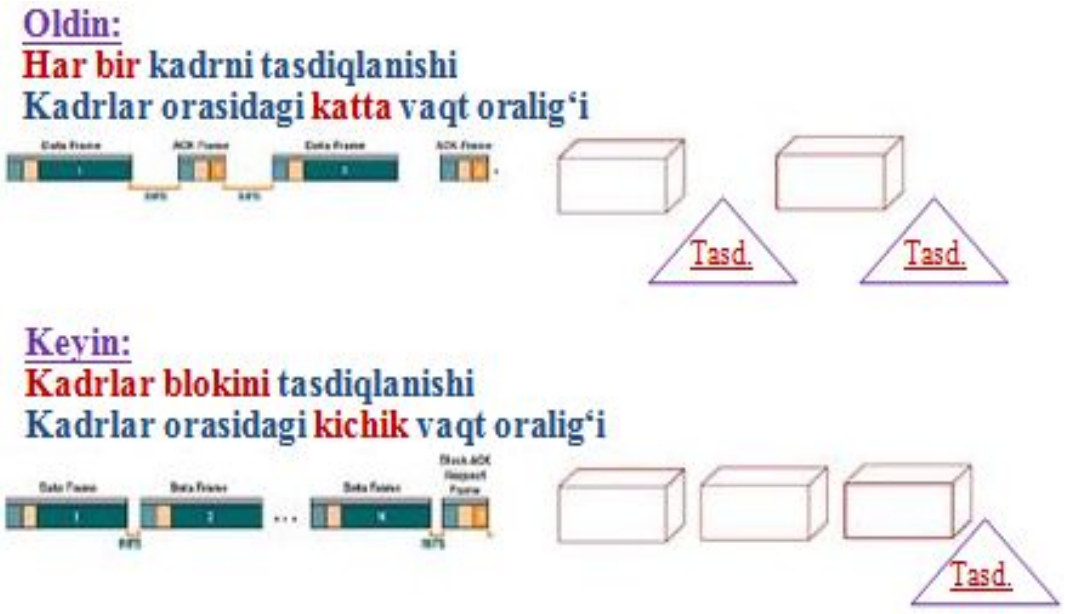
4.3-rasm. Maълumotlarni uzatish tezligini oshirilishining birinchi omili

Birinchi omil. MIMO qo‘llanilishi bilan o‘sha bir kanalda bir necha malumotlar 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.



4.4-rasm. Maълumotlarni uzatish tezligini oshirilishining ikkinchi omili

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 bohliq bo‘ladi. YAngi standartda 20 MGs bo‘yicha qo‘shni kanalarni birlashtirilishi va bunday tarzda o‘tkazish qobiliyatini deyarli ikki marttaga oshirilishi imkoniyati paydo bo‘ldi. Avtomagistrallarga o‘xshatish bilan aytish mumkinki, harakatlanish uchun mumkin polosalar soni ikki marttaga oshdi.



4.5-rasm. Maълumotlarni 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 br uzatilgan kadrni (maълumotlarni porsiyasini) qabul qilish qabul qilish tomonidan tasdiqlanishi kerak edi. Yangi versiyada blokli tasdiqlash imkoniyati kiritilgan. Maълumotlarni qabullagich bir necha muvaffaqiyatli qabul qilingan kadrlarga birdaniga bir necha tasdiqlashni uzatadi, bu kanalning umumiy o‘tkazish qobiliyatini xizmat xabarlari 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.

Nazorat savollari

1. Standartning o‘ziga xos xususiyatlarini tushuntiring
2. MIMO texnologiyasining ishlatilishi prinsipini tushuntiring
3. 802.11n standartida maълumotlarni yuqoriroq tezliklarda uzatilishi omillari nechta?
4. 802.11n standartida maълumotlarni yuqoriroq tezliklarda uzatilishi omillarining qanday farqi bor?

5-ma’ruza

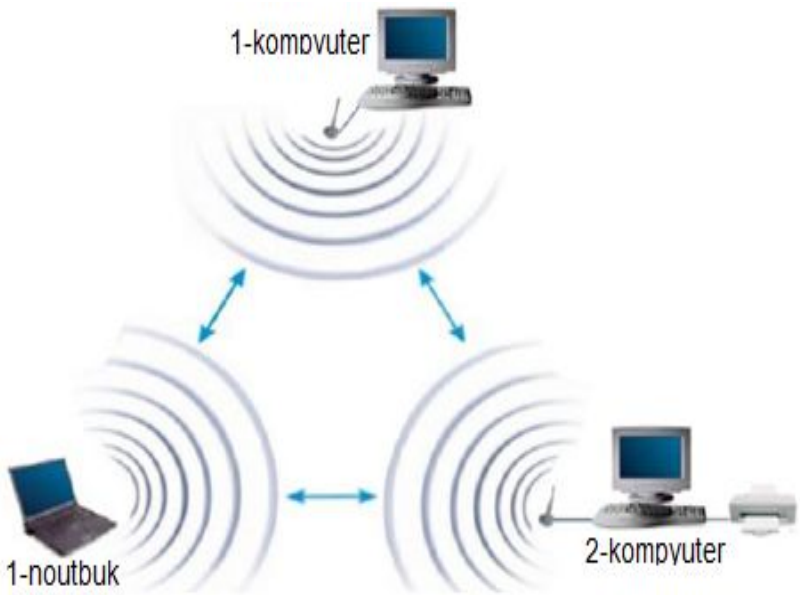
Simsiz tarmoqlarning tashkil etish va rejalashtirilish. Infratuzilmali rejim, WDS, WDS with AP rejimlar.Ad Hoc rejimi.

Reja:

1 Simsiz tarmoqlarning tashkil etish va rejalashtirilish.

2. 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 (5.1-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‘llanilishisiz 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.



5.1-rasm. Ad Hoc rejimi

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

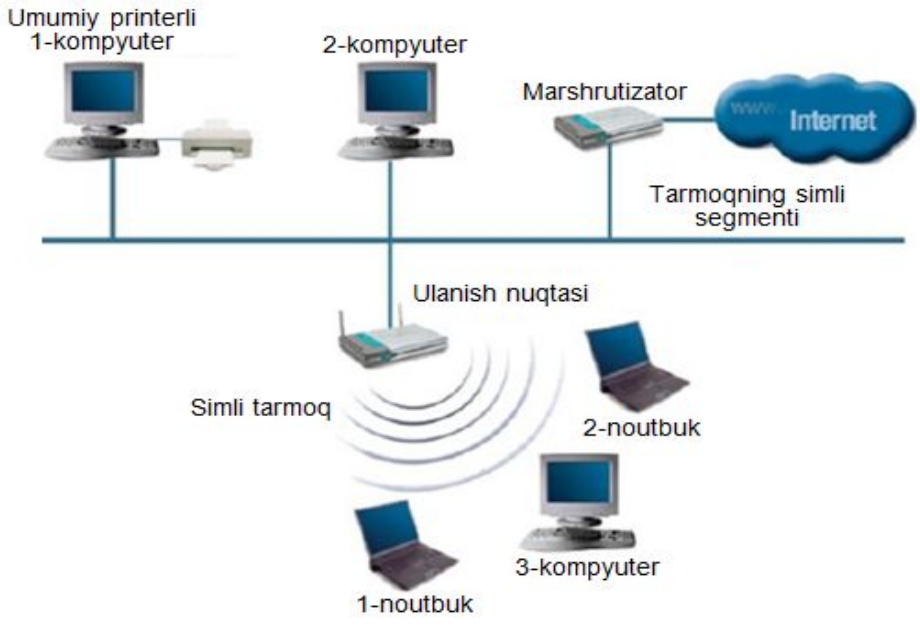
Lekin, shuni e’tiborga olish kerakki, Ad Hoc rejimi ishlatiladigan qurilmaga bog‘liq bo‘lmagan holda 11 Mbit/sekunddan ortiq bo‘lmagan tezlikdagi bog‘lanishni o‘rnatishga imkon beradi. Ma’lumotlarni almashtirish real tezligi pastroq bo‘ladi va 11/N Mbit/sekunddan ortiq bo‘lmagan tezlikni tashkil etadi, 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 Wreless Utility dasturi yordamida amalga oshirish mumkin.

Infratuzilmali rejim

Bu rejimda ulanish nuqtasi mijoz kompyuterlarining aloqasini ta’minlaydi (5.2-rasm). Ulanish nuqtasiga simsizkommutator 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.



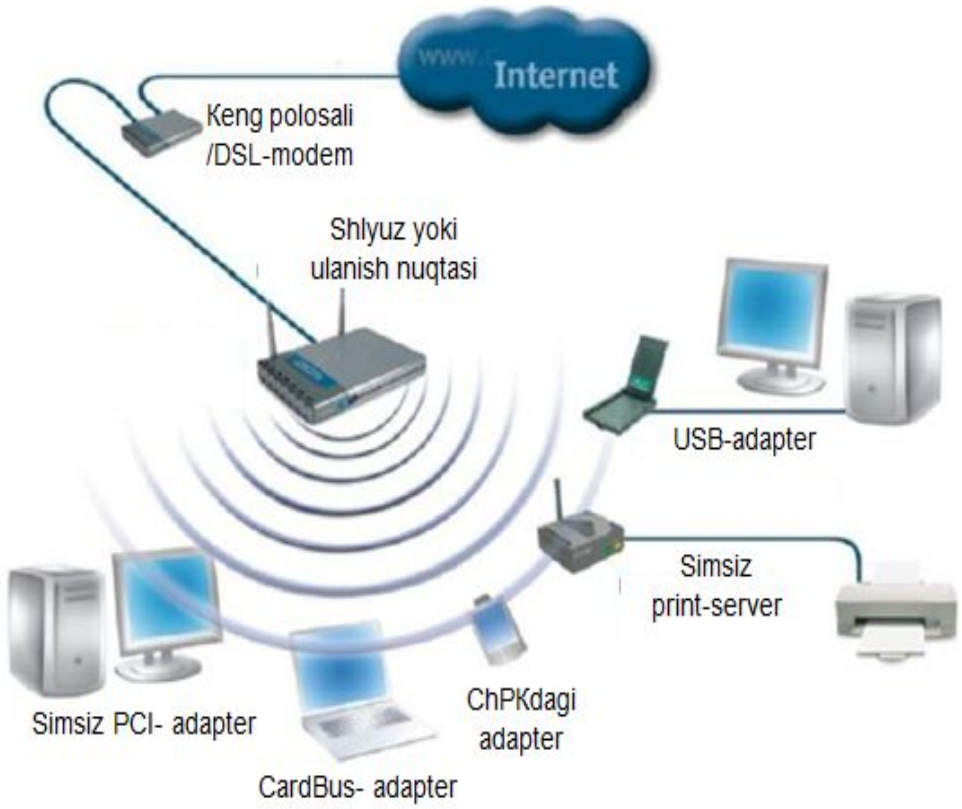
5.2-rasm. Infratuzilmali rejim

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.

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 (5.3-rasm).



5.3-rasm. Ofis tarmog‘i

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.

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.

Shuni e’tiborga olish zarurki, tarmoq kengaytirilganda va foydalanuvchilar soni ortganda aloqa tuzligi 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.

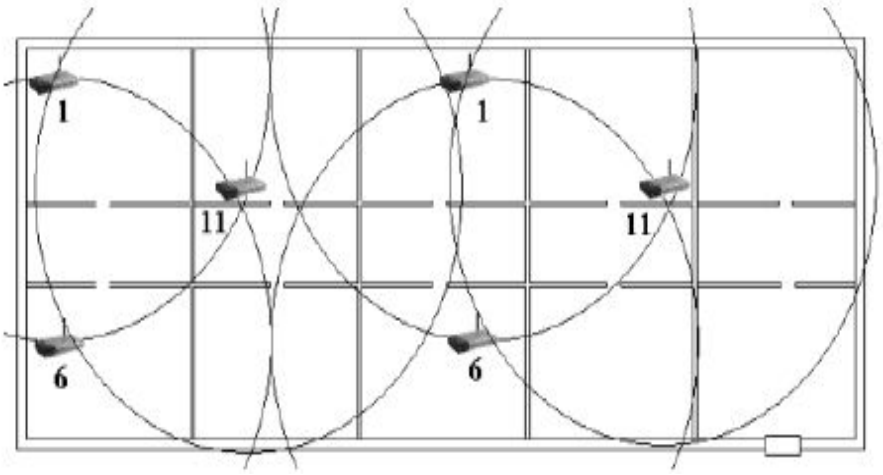
Tarmoqni kengaytirishda o‘zaro halaqitlar va uzatish tezligini kamyishidan qochish uchun qo‘shni ulanish nuqtalarining chastotalari bir-birlarini qoplamasligi kerak. Bunga chastota bo‘yicha 1, 6 va 11 qoplanmaydigan kanallarga qo‘shni nuqtalarni sozlash bilan erishiladi. Bunday tarzda, 1, 6 va 11 kanallarli 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 (5.6-rasm).

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

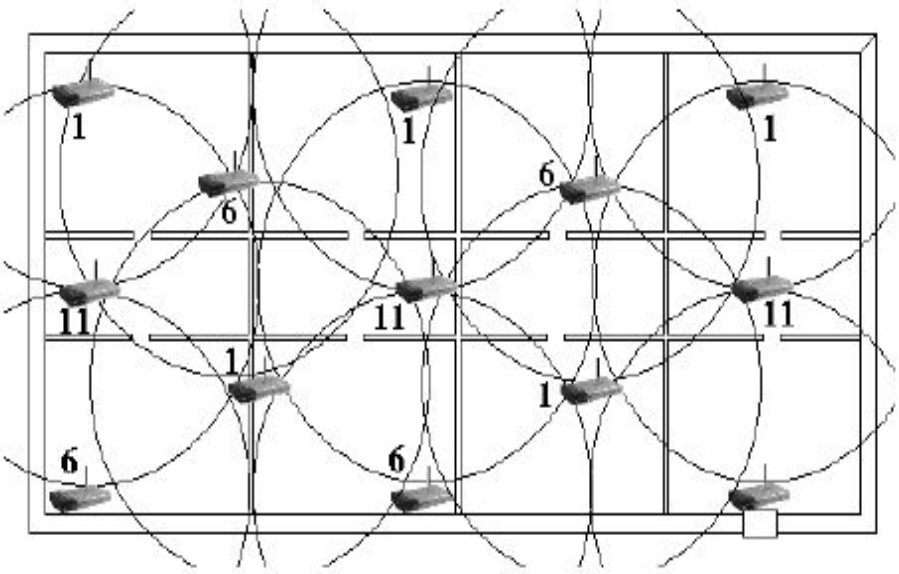
- bitta mijozga hisoblaganda hisoblangan tezlik;
- ishlatiladigan ilovalar turlari;
- ma’lumotlarni uzatishdagi kechikishlar.

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 (5.7-rasm).



5.6-rasm. Simsiz tarmoqni kengaytirish

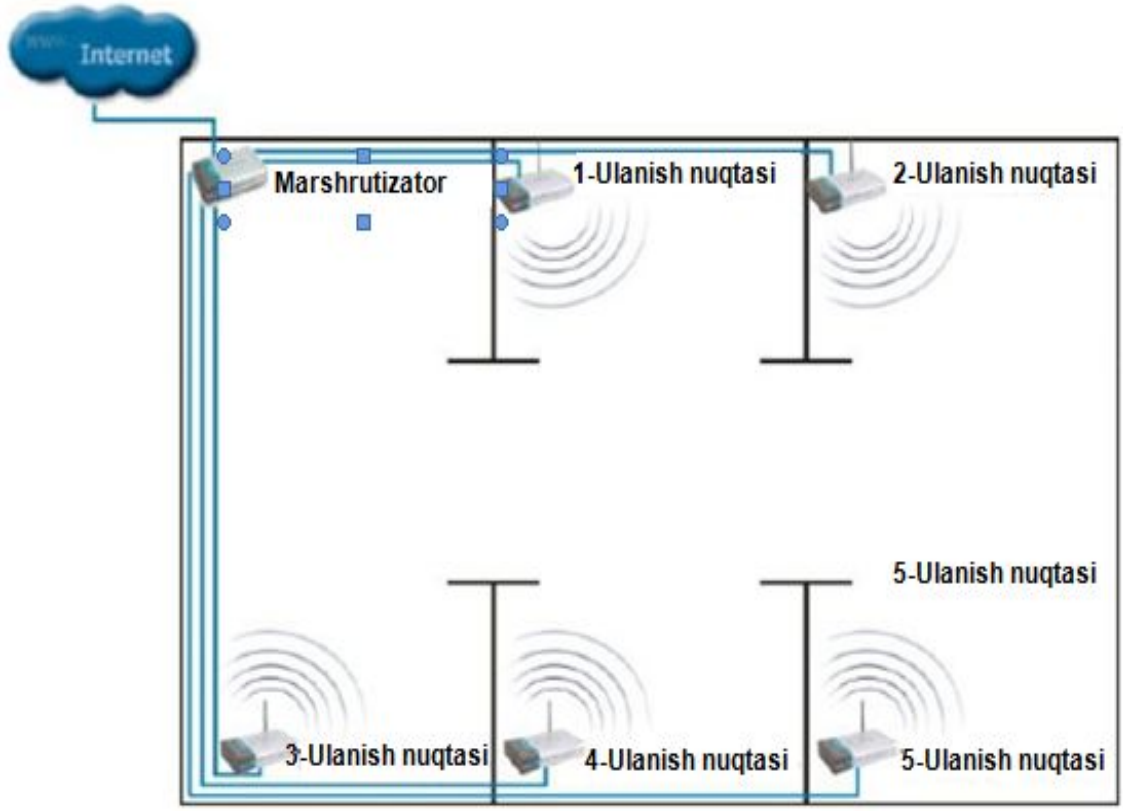


5.7-rasm. Simsiz tarmoqni maksimal tezlikli kengaytirish

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.

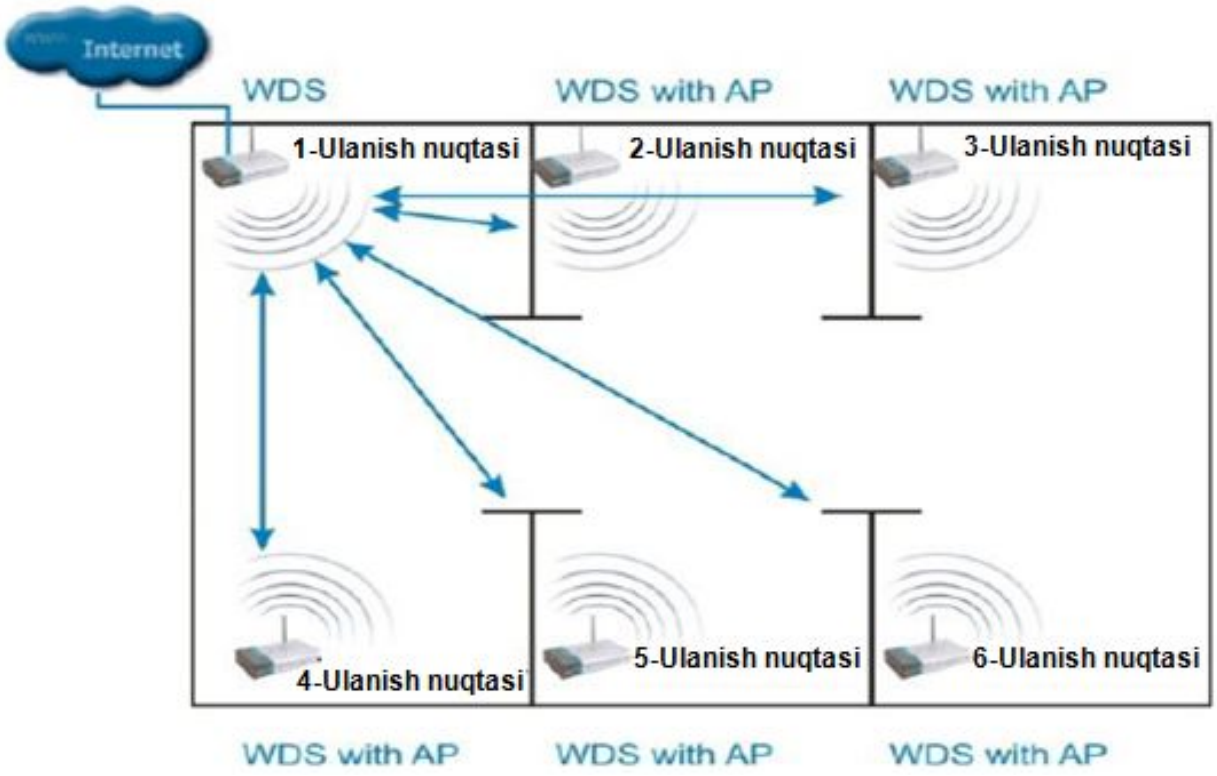
Ofisda barcha ulanish nuqtalarini lokal tarmoqqa birlashtirishni bir necha usullarda amalga oshirish mumkin. tashkil etishning eng oddiy va eng keng tarqalgan usuli simli infratuzilma orqali birlashtirish hisoblanadi (5.8-rasm).



5.8-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 avzalligi 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 (5.9-rasm).



5.9-rasm. WDS kengaytirilgan rejimdan foydalanishli ulanish nuqtalarini birlashtirish

Nazorat savollari

1. Aloqa sifatini oshirish uchun qanday bazaviy prinsiplarga rioya qilish kerak bo‘ladi?
2. Ofis tarmog‘ini tushuntiring.
3. Simsiz tarmoqni kengaytirishdagi eng muhim omillarni ayting.
4. Simli infratuzilma orqali ulanish nuqtalarini birlashtirishni tushuntiring.
5. Ad Hoc rejimini tushuntiring
6. Infratuzilmali rejimini tushuntiring

6-ma’ruza

Tarmoqlarning ishlash rejimlari va ularning tashkillashtirish xususiyatlari.

Reja:

1 Tarmoqlarning ishlash rejimlari

2. Tarmoqlarning 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‘li bo‘ladi. Aloqa sifatini oshirish uchun quyidagi bazaviy prinsiplarga rioyaqilish kerak bo‘ladi:

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 eletr ta’minoti manbalarini iloji boricha 1-2 metr masofaga uzoqlashtirish. Halaqitlarni kamaytirish uchun bu asboblar ishonchli yerga ulanishi kerak.

6. Agar 2,4 GGs 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 nomoyon bo‘ladi. Tushunib olish muhimki, ma’lum sharoitlarda alohida samaralar kuchliroq nomoyon bo‘ladi, masalan, sezilarli qaytarish xonada katta metall shkaflar bo‘lganida yoki antenna liftning shaxtasi va eshiklari yonida joylashganida kuchliroq nomoyon 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.

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 etib boradi, lekin yo‘nalishlari o‘zgargan signallar ko‘plab nusxalari ham va ko‘plab qaytarishlardan keyin mutlaqo oldindan bilib bo‘lmaydiganxarakteristiklarga (fazaga, amplitudagi va h.k.) ega bo‘lish bilan qabullash antennasiga etib borishi mumkin. Odatda qaytarilgan signallar uchun asosiy signalga qaragan katta yo‘lni bosib o‘tish zarurati tufayli qabullash antennasiga etib borishi uchun bir qanchako‘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 standartlartarmoqlari 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 koeffitsientili antennalardan foydalanish yordam beradi.

Zamonaviy Wi-Fi 802.11n standarti tarmoqlari uchun signalning ko‘r nurli tarqalishi muammolarini kompensatsiyalashning sezilarli ko‘p mexanizmlari mavjud. Bu erda 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 (6.1-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 hlavitlar manbalari bo‘lishi mumkin.

Elektr energichi 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.

6.1-rasm. Ulanish nuqtasiga halaqitlar manbalarini ta’siri

2,4 yoki 5 GGs dipazonlardan ishlaydigan radiotelefonlar

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

Simsiz yuqori chastotali videosignalni uzatkichlar

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

Simsiz dinamiklar

2,4 yoki 5 GGs dipazonlardan 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 dipazonda sezilarli bo‘lgan garmonik halaqitlarni hosil qiladi. YOpiq qopqoqli va ulangan tashqi monitorli noutbukdan foydalanishda halaqitlar etarlicha sezilarli bo‘lishi mumkin.

Etarli bo‘lmagan ekranlashtirilgan kabellar

Tashqi qattiq disklar yoki etarli bo‘lmagan ekranlashtirigan 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 dipazonda ishlaydigan simsiz asboblar ham, masalan, mikroto‘lqinli uzatkichlar, simsiz kameralar, radioenagalar va Wi-Fi tarmog‘i bo‘yicha ulangan qo‘shnilar qurilmalari halaqit quriladi.

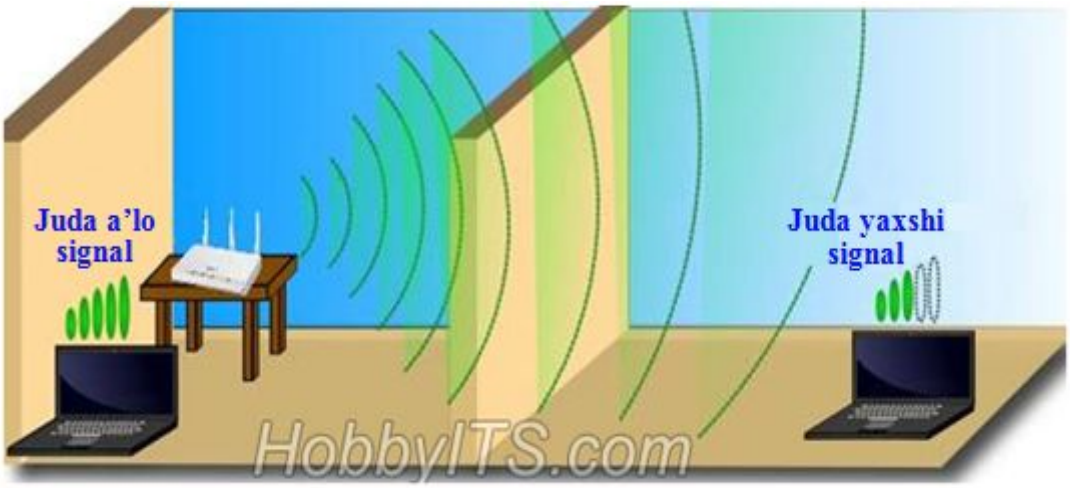
Hamma vaqt ham qurilma 2,4 yoki 5 GGs dipazonda ishlayotganligini birdaniga aniqlab bo‘lavermaydi. Ishchi dipazonlar haqidagi malumotlar qurilmaga ilova qilinadigan hujjatlarda bo‘lishi kerak. Bunday qurilmalar simsiz, ikki dipazonli yoki “Wi-Fini qo‘llaydigan” qurilmalar deyiladi.

Simsiz aloqa uchun to‘siqlar

Wi-Fi aloqa sifatiga binoda qurilmalarning joylashishi va atrofdagi binolar qurilgan qurilish materiallari ham ta’sir qilishi mumkin (6.2-rasm). Iloji boricha simsi aloqa uchun to‘siqlardan qochish kerak. Signal to‘siqlarsiz o‘tishi uchun Wi-Fi qurilmalarning joylashishini o‘zgartirish kerak.

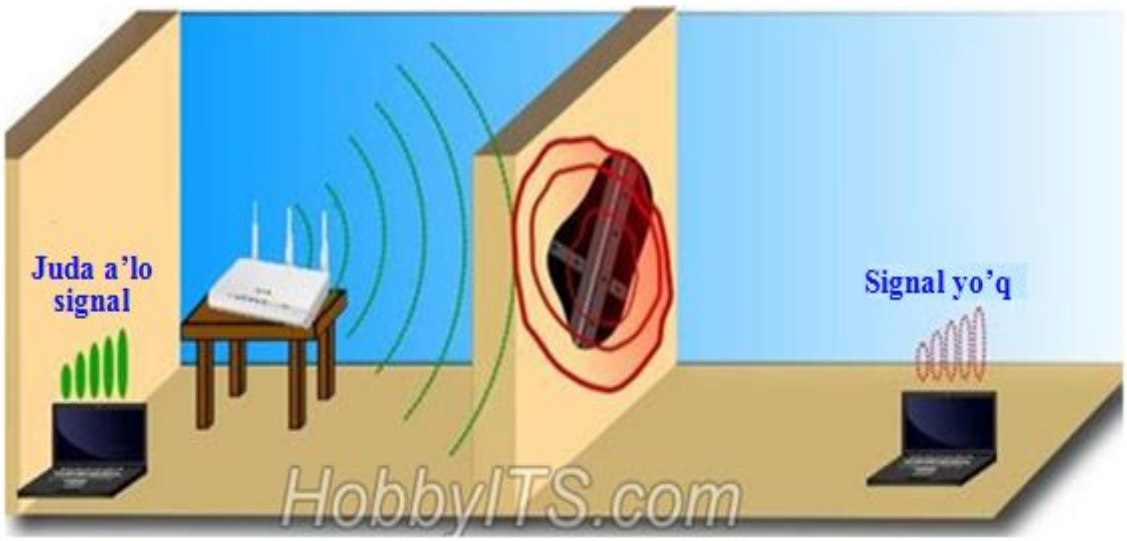
Misollar:

- 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.



6.2-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‘sib qo‘yishi mumkin. Natijada ulanish tezligi past bo‘ladi yoki Wi-Fi signal kuchsiz bo‘ladi yoki umuman Wi-Fi tarmoqqa ulanish bo‘lmaydi (6.3-rasm).



6.3-rasm. Metall almaturali devor tufayli signalning kuchsizlanishi

Quyida 1.3-jadvalda radiochastotalar signallarini qaytarish yoki yutish qobiliyatiga ega bo‘lgan materiallar sanab o‘tilgan.

6.1-jadval

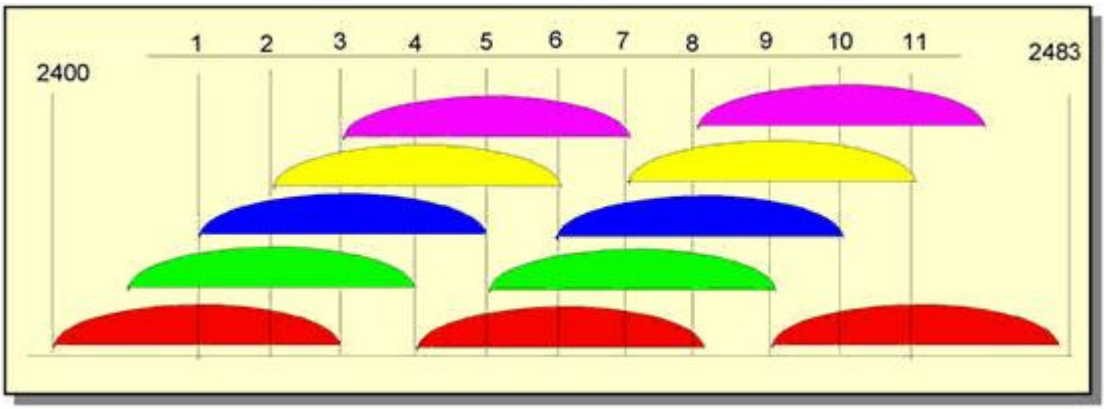
Radiochastotalar signallarini qaytarish yoki yutish qobiliyatiga ega bo‘lgan materiallar

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 intervallarli 40 MGs (IEE 802.11n) kenglikdagi 11 yoki 13 kanallar mumkin bo‘ladi. Wi-Fi chastotalar kanallarining birini ishatadigan simsiz qurilma qo‘shni kanallarga halaqitlarni hosil qiladi. Masalan, agar ulanish nuqtasi 6-kanalni ishlatsa, 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.



6.4-rasm. 11 ta kanallar spektrlari

6.4-rasmda 11 ta kanallar spektrlari tasvirlangan. Bitta qamrab olish xizmat ko‘rsatish zonasi chegaralaridagi ulanish nuqtalari kanallarni qoplanishini oldinini olishi kerak.

Ranglar bilan belgilash ksishmaydigan 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.

6.4-rasmdan ko‘rinib turibdiki, 1- va 2-kanallar sezilarli darjada 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. Aloqa sifatini oshirish uchun qanday bazaviy prinsiplarga rioyaqilish kerak bo‘ladi?
2. Wi-Fi tarmoqlarida signalning ko‘p nurli tarqalishini tushuntiring.
3. Ulanish nuqtasiga halaqitlar manbalarining qanday ta’siri bor.
4. To‘siqlardan signallarning o‘tishini tushuntiring.

7-ma’ruza

Wimax texnologiyasi. Asosiy xarakteristikalari. Ishlash printsplari va rejimlari.

Reja:

1 Asosiy xarakteristikalari.

2. Ishlash printsplari va rejimlari.

Worldwide Interoperability for Microware Acces (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 («**So‘nggi mil**» deb abonent uskunasini provayderning (aloqa operatorining) ulanish nuqtasi bilan bog‘lovchi kanal tushuniladi. Masalan, Internet tarmog‘iga ulanishda so‘nggi milya deb provayderning kommutatori portidan to abonentning marshrutizatori portigacha bo‘lgan qism nazarda tutiladi) 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.

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.

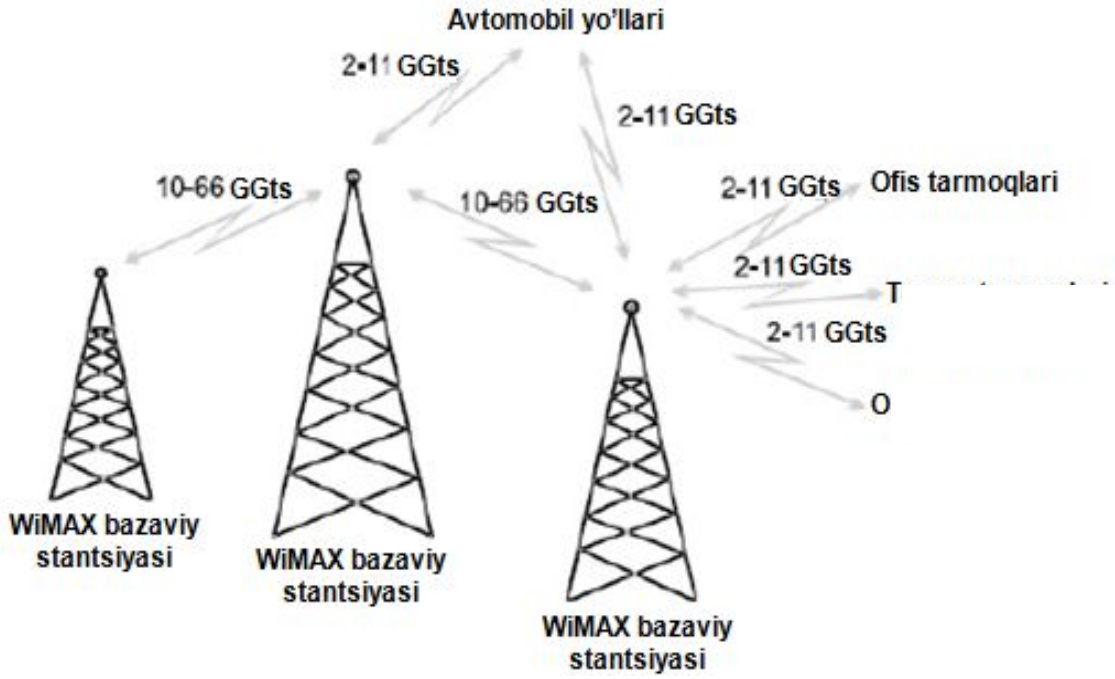
Wimax tizimlarining ishlash printsiplari

WiMAX tizimi quyidagi ikki asosiy qismlardan tashkil topgan:

1. WiMAX bazaviy stansiyasi baland ob'ektda yoki minoradi joylashishi mumkin.

2. WiMAX qabullagichi : qabullagichli antenna (7.1-rasm).

Bazaviy stansiya va mijoz qabullagichi orasidagi bog'lanish O'YuCh 2-11 GGs diapazonda amalga oshiriladi. Bu bog'lanish ideal sharoitlarda ma'lumotlarni 20 Mbit/sekund tezlikda uzatish imkoniyatini beradi va stansiya foydalanuvchidan ko'rish zonasi masofasida bo'lishini talb qilmaydi. WiMAX bazaviy stansiyasining bu rejimi keng ishlatiladigan 802.11 (Wi-Fi) standartga yaqin, bu WiMAX da ham chiqarilgan mijoz qurilmalarining moslashishiga ruxsat etadi.



7.1-rasm. WiMAX arxitekturasi

Qo'shni bazaviy stansiyalar orasida to'g'ri ko'rinishdagi 10-66 GGs o'ta yuqori chastotalardan foydalanishli radioaloqa doimiy bog'lanish o'rnatiladi. Bu bog'lanish ideal sharoitlarda ma'lumotlarni 120 Mbit/sekund tezlikda uzatish

imkoniyatini beradi. To‘g‘ri ko‘rinish bo‘yicha chegaralash, tabiiyki, avzallik emas, lekin u faqat tumanni butunlay qamrab olishda qatnashadigan bazaviy stansiyalarga qo‘yiladi, bu qurilmalarni joylashtirishda ishlatilishi mumkin stansiyalardan biri .

Minimum darajada bazaviy stansiya keng polosali katta tezlikli bog‘lanish orqali provayder tarmog‘iga doimiy ulanishi mumkin. Qancha ko‘p stansiyalar provayder tarmog‘iga ulanishga ega bo‘lsa, mu’lumoilrni uzatish tezligi va ishonchliligi shunchalik katta bo‘ladi. Lekin, hatto nuqtalar soni uncha katta bo‘lmaganda ham tizim sotali topologiya hisobiga yuklamani aniq taqsimlashga qodir bo‘ladi.

WiMAX tarmog‘ining ishlash rejimlari

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/sek. gacha yetadi, aloqa masofasi 50 kmgacha), bu standart turli variantdagi simli keng polosali abonent ulanish usullarining alternativ 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/sekundni tashkil etadi, aloqa masofasi – 5-10 kmga teng. IEEE 802.16e standarti BS va AQ (abonent qurilmasi) 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 stasionar 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.

Fiksatsiyalangan ulanish

Fiksatsiyalangan ulanish o‘z tuzilishiga ko‘ra keng polosali simli 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 120Mbit/sekunddan ortiqroq tezliklarda ma’lumot uzatishga erishish mumkin. Fiksatsiyalangan ulanish rejimi IEEE 802.16d-2004 standarti bilan tavsiflangan. Shuni alohida ta’kidlash lozimki, Fiksatsiyalangan 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 fiksatsiyalangan 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 uskunalar(, masalan, noutbuk, KPK) uchun ishlab chiqilgan va portativ uskunalar 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 40km/soat dan oshmasligi kerak. Shunday bo‘lsa ham, ushbu rejimdan AQ avtomobilda, velosipedda va yayov holatda chegaralangan tezlik bilan harakatlanganda foydalanishi mumkin. Ushbu rejimga kirish smartfon, kommunikator va ChPK lar uchun WiMAX texnologiyasidan foydalanishga mos ravishda amalga oshirilgan. Bunday ko‘chma ulanishli WiMAX rejimida ishlovchi uskunalarning chiqishi 2006 yildan boshlandi.

Mobil ulanish

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

1. Signalning ko‘p nurli tarqalishiga va shaxsiy xalakitlarga 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 cho‘zadi.
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 uskunasining 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 5 msda kichik paketlardan foydalanib ma’lumot uzatish ishonchliligi va paketlar sonini qo‘paytirish xarajatlari orasida o‘zaro kelishuvni ta’minlaydi.

WiMAX tarmoqlariga mobil xolatda ulanish turli darajadagi mobillikni ta’minlovchi har xil abonent uskunalari bilan ta’minlanadi. Ularga quyidagilar kiradi:

- binolar ichida qo‘llanilish uchun uskunalar, shuningdek ular klient uskunalari (*Customer Premises Equipment, CPE*) deb nomlanadi;
- Binolar tashqarisida qo‘llash uchun uskunalar, 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 1-jadvalda keltirilgan.

7.1-jadval.

WiMAX tarmoqlarining ishlash rejimlari

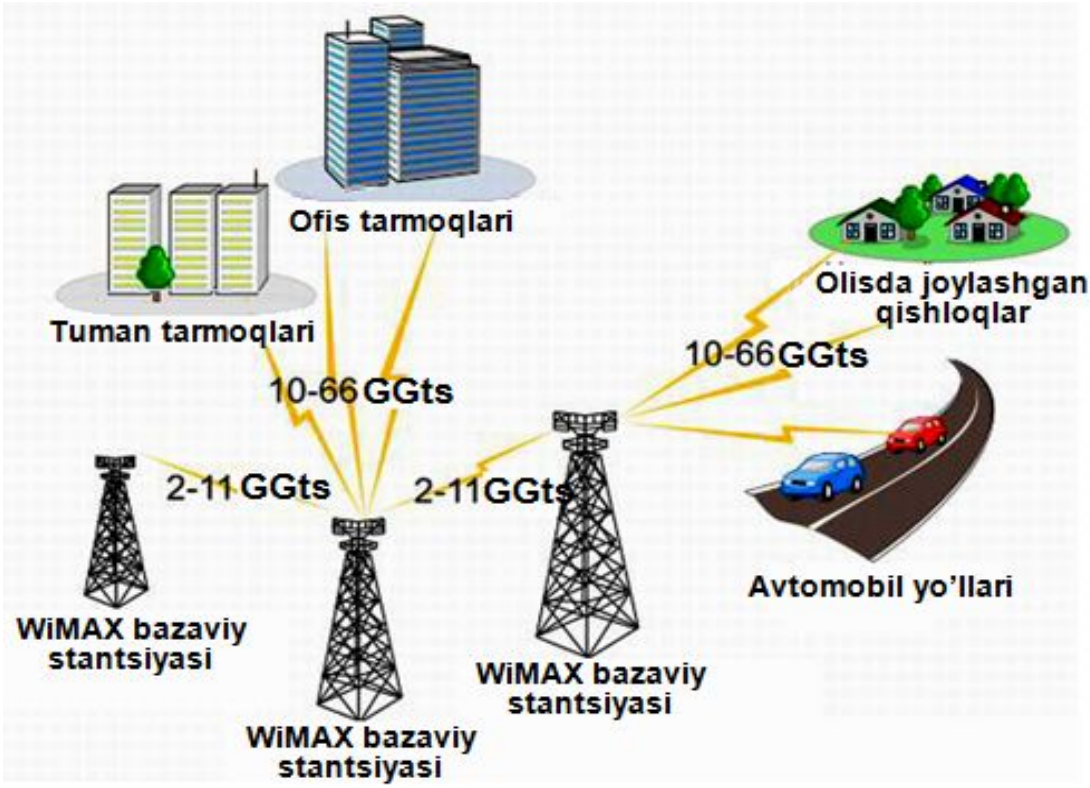
Ulanish turi	Uskuna turi	Uskunalar soni/abonent xarakati tezligi	“Xendover” ni qo‘llab-quvvatlash	802.16-2004 standar-ti	802.16a standarti
Turg‘un ulanish	Tashqarida va ichkarida joylashgan “xotspot” lar	Yakka uskuna/ turg‘un abonent	Yo‘q	Ha	Ha
Ko‘chma ulanish	Ichkarida joylashgan “xotspot” lar, portativ ShKlar uchun PCMCIA-adapterlar	Ko‘p sonli uskunalar/ abonent turg‘un	Yo‘q	Ha	Ha

Portativ ulanish	Portativ ShK lar uchun PCMCIA-adapterlar, kichik adapterlar	Ko‘p sonli uskunalar / piyoda tezligi	Dag‘al “xendover”	Yo‘q	Ha
Asosan mobil ulanish	Portativ ShK lar uchun PCMCIA-adapterlar, kichik adapterlar, ChPK, smartfonlar	Ko‘p sonli uskunalar / kichik tezlikda harakatlanuvchi transport vositasi	Dag‘al “xendover”	Yo‘q	Ha
To‘liq mobil ulanish	Portativ ShK lar uchun PCMCIA-adapterlar, kichik adapterlar, ChPK, smartfonlar	Ko‘p sonli uskunalar / katta tezlikda harakatlanuvchi transport vositasi	Yumshoq “xendover”	Yo‘q	Ha

WiMAX tarmog‘ini tashkil etishning o‘ziga xos xususiyatlari

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 va 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 (7.2-rasm.):

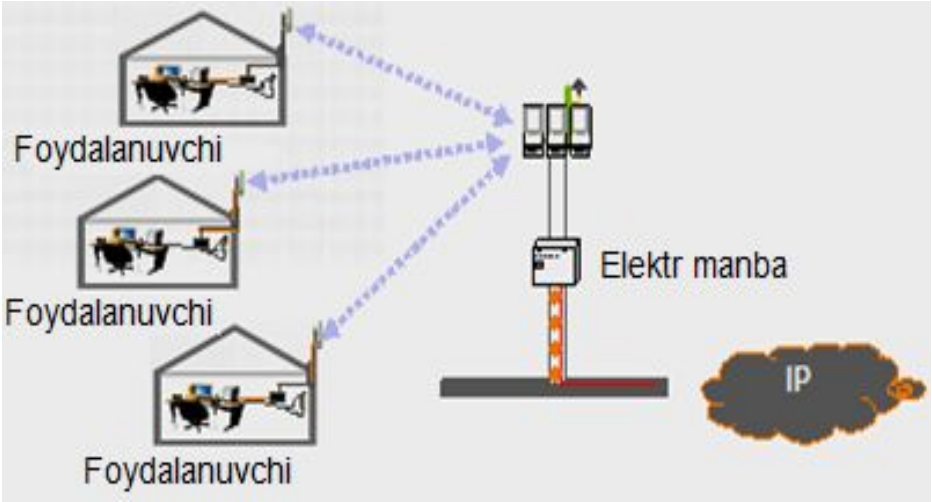


7.2-rasm. WiMAX tarmog‘i topologiyasi

WiMAX tizimlarida avval magistral liniyalarni tashkil etish uchun 10-66MGs dastota diapazonidan foydalanish qo‘zda tutilgan, hozirgi foydalaniladigan versiyalarida esa 2 dan 11 MGs dastota 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 uskunalari bilan “nuqta- ko‘p nuqta” topologiyada aloqani amalga oshiradi (7.3-rasm).

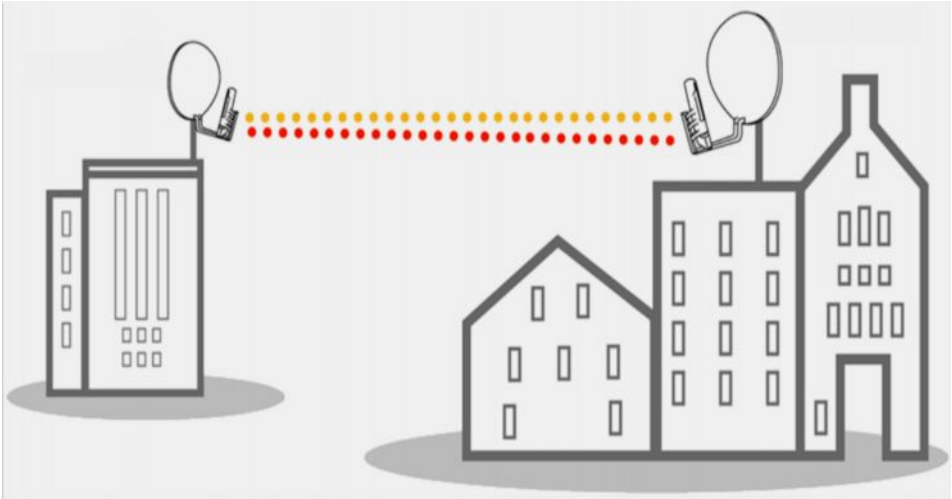
Bu chizma bo‘yicha BS WiMAX abonenti uskunalari yordamida foydalanuvchilar bilan bog‘lanadilar, keyin signal Ethernet-kabel standarti bo‘yicha yoki to‘g‘ridan-to‘g‘ri aniq kompyuterga, yoki IEEE 802.11 (Wi-Fi) ulanish nuqtasi orqali qabul qilinadi. Bu WiMAX orqali kabelli ulanishdan simsiz

ulanishga o‘tishda mavjud hudud yoki ofis tizimidagi lokal tarmoqlarning infrastrukturasini saqlab qolish imkonini beradi. Bundan tashqari kompyuterlar ulanishi uchun standart texnologiyalardan foydalanuvchi tarmoqlarni yoyishni maksimal darajada kengaytirish imkonini beradi.



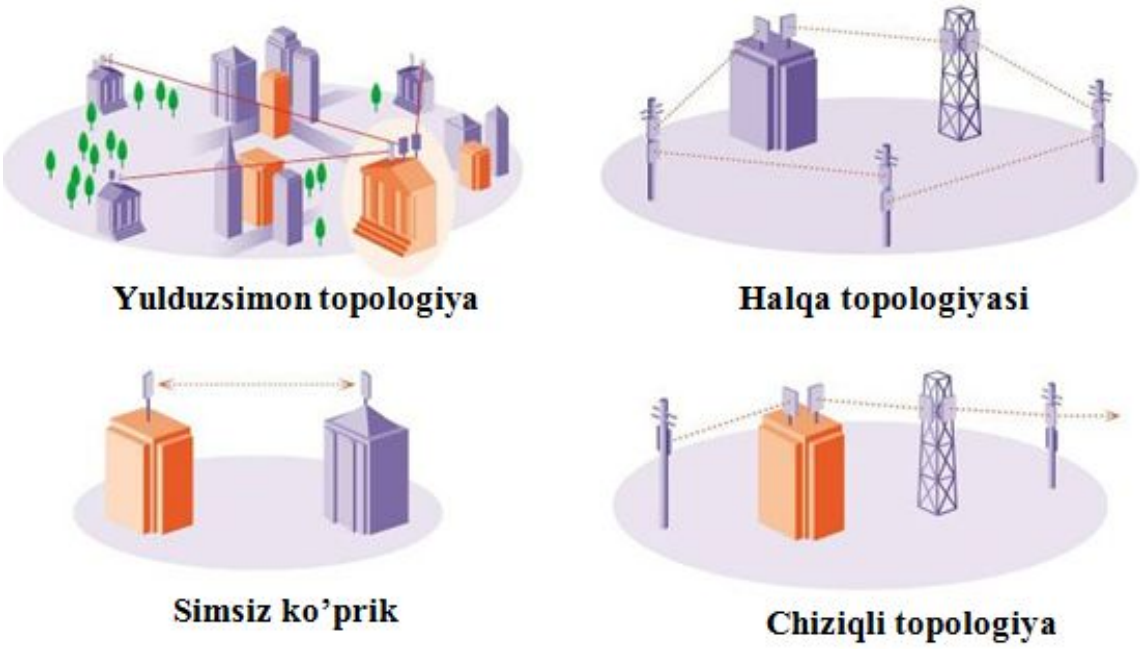
7.3-rasm. «Nuqta-ko‘p nuqta» rejimida WiMAX tarmog‘i topologiyasi

Uzoqlashtirilgan ob’ektlar orasida simsiz keng polosali aloqani tashkil qilish uchun «nuqta-nuqta» rejimidan foydalaniladi (7.4-rasm).



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

«Nuqta-nuqta» rejimida turli tarmoq ko‘rinishlari va ularning kombinatsiyalaridan foydalaniladi. 7.5-rasmda WiMAX tizimi uchun qo‘llaniluvchi turli ko‘rinishdagi tarmoq topologiyalari tasvirlangan.



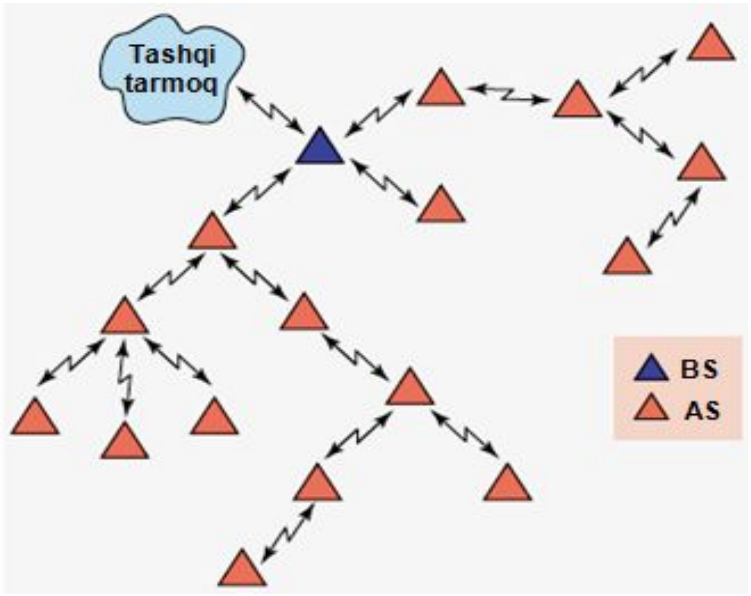
7.5-rasm. “Nuqta-nuqta” rejimidagi WiMAX tarmog‘ining ko‘rinishlari

WiMAX tarmoqlarida shuningdek **«mesh»** rejimida aloqa tashkil qilish mumkin,bunda AU to‘g‘ridan-to‘g‘ri bir-biri bilan aloqani amalga oshiradi, bazaviy stansiyasi esa asosiy tarmoqlar infrastrukturasi va mesh tarmoqlari o‘rtasida kommutator hisoblanadi. (7.6-rasm). **«mesh»** rejimini qo‘llash natijasida tarmoqning radioqoplam zonasi yuqori tezlikda ma’lumot uzatishni ta’minlash bilan 50 km gacha oshadi, bu holda bitta BS ning oddiy holdagi radiusi 5-10 kmni tashkil etadi.

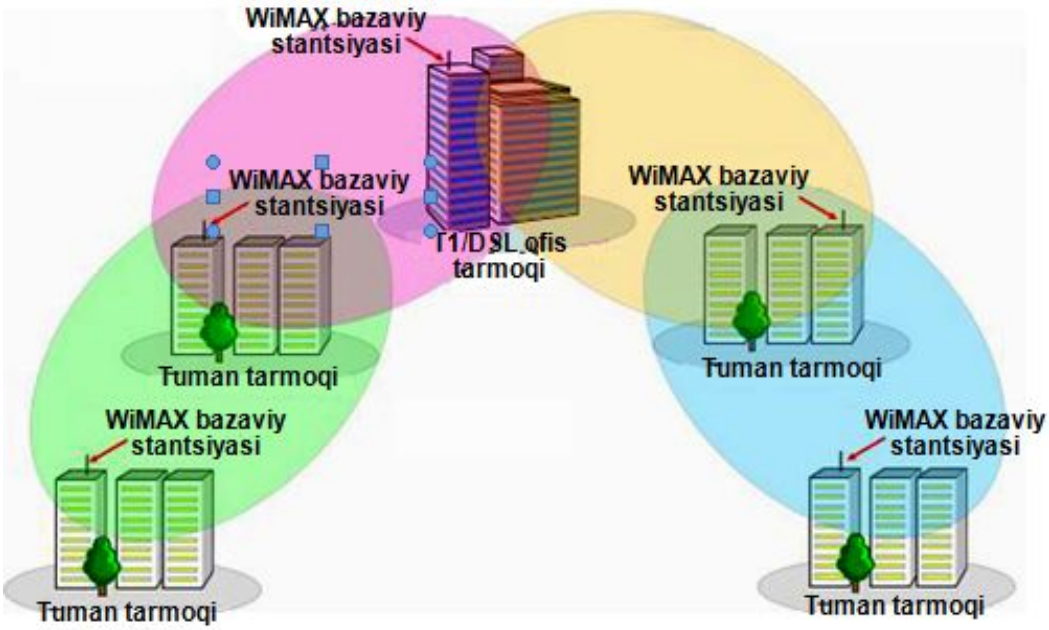
WiMAX tarmoqlari «ko‘p nuqta - ko‘p nuqta» rejimida qurilishi mumkin, shuningdek u «nuqta-ko‘pnuqta» rejimini ham ta’minlaydi. (7.7-rasm).

Bunda BS lokal trafikni tashkil qilish uchun radioterminal yoki takrorlagich bo‘lishi mumkin. Ma’lumotlar oqimi abonentga yetib borguncha, bir necha takrorligichlardan 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 fo‘llaniladi. Ular BS dan bir yoki bir necha abonent uskunalariga signal uzatadi. WiMAX tizimlari uskunalari o‘z ichiga abonent terminallarini, asosiy tarmoq uskunalarini, tugunlararo kanallarni va takrorlagichlarni oladi.



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



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

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

8-ma’ruza

Simsiz tarmoqlar xavfsizligiga tahdidlar va xavflar

Reja:

1 Simsiz tarmoqlar xavfsizligiga tahdidlar.

2. Simsiz tarmoqlar xavfsizligiga xavflar.

Simsiz aloqa tarmoqlarining axborot xavfsizligiga tahdidlar o‘z-o‘zicha emas, balki axborot tarmog‘ida bo‘lgan texnologiyalarning zaifliklari orqali nomoyon 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 haqiqiyligini 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 nomoyon 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) tabiy 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 va va 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 nomoyon bo‘ladi.

Ob’ektga xarakterli bo‘lgan zaifliklarni undan ajratib bo‘lmaydi va ishlash jarayoning 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 foydlanuvchisi yoki egasiga zarar etkazish) zaifliklarni ishlatishi mumkin. Bundan tashqari, tahdidlar manbalarining zarar etkazadigan 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 echilmagan. 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.

8.1- va 8.2-jadvallarda tahdidlarning asosiy turlari va ham signalli, ham axborot darajalaridagi tahdidlarning ishlatilishi sharoitlari haqida umumiy ma'lumotlar keltirilgan.

2-jadval

Simsiz tarmoqlarda signalli darajadagi tahdidlarning turlari va manbalari

Tahdidlar	Tahdidlarning ishlatilishi sharoitlari	Tizimning zaif elementi
Tabiy kelib chiqishdagi tahdidlar		
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
Inson faoliyati natijasidag vujudga keladigan (antropogen) tahdidlar		
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 appraturasining majudligi	Uzatish kanali
Ikkinchi darajali kanallardagi signalni qo‘lga kiritish	Asosiy kanal signalining past filtrlanishi	Ta’minot va erga 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 siganllarni qo‘lga kiritish	Qabul qilish va uzatish punktlarining foydalana olishliligi	Butun tizim

8.2-jadval

Simsiz tarmoqlarda axborot darajasidagi tahdidlarning turlari va manbalari

Tahdidlar	Tahdidlarning ishlatilishi sharoitlari	Tizimning zaif elementi
Ma’lumotlarni qo‘lga kiritish		
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 (kompрometatsiyasi), shifrlanmagan signal blokining olinishi	Ma’lumotlarni almashtirishni tashkil etish tizimi
Ma’lumotlarni buzish		
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
Boshqarishni qo‘lga kiritish		
Boshqarish ketma-ketliklarini abonentga uzatish	Master-kodlarni olishning, himoya qilish tizimlarining kodlarini obro‘sizlantirishning (kompрometatsiyasining) mumkinligi	Boshqarish tizimi
Boshqarish ketma-ketliklarini markaziy stansiyaga uzatish	Master-kodlarni olishning, himoya qilish tizimlarining kodlarini obro‘sizlantirishning (kompрometatsiyasining) mumkinligi, protsessorga va boshqarish dasturlariga foydalana olishning mumkinligiya	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 konfidensialliligini, 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 hisoblaadi. Tarmoq taqdim etadigan xizmatlarning har biri bo‘yicha tahdidlar har bir 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 8.3-jadvalda keltirilgan.

8.3-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 siganllari 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
Aboentning 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 konfidensialligigining 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. Mobil aloqa tarmoqlarining axborot xavfsizligini ta’minlash masalasi xavfsizlikka tahdidlar va zaifliklarni tahlil qilishni, ishlashishini monitoring qilishni va qarshi turishning mos choralarini ko‘rishni o‘z ichiga oladi.

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?

9-ma’ruza

Simsiz tarmoqlar xavfsizlik protokollari. WEP shifrlash mexanizmi.

Reja:

1 Simsiz tarmoqlar xavfsizlik protokollari.

2. WEP shifrlash mexanizmi.

Simsiz tarmoqlarda axborotlarning yaxlitligini va konfidensialligini ta’minlash uchun kriptografik vositalar qo‘llaniladi. Lekin, e’tiborsizlik kommunikatsiyalarning buzilishiga va jinoyatchilarning axborotlardan foydalanishiga olib keladi.

WEP bu 802.11 standartidagi tarmoqlarning xavfsizligini ta’minlash uchun yaratilgan kriptografik mexanizm hisoblanadi. Bu mexanizm barcha foydalanuvchilar ishlatadigan yagona statik kalit bilan ishlab chiqilgan. Kalitlarga boshqariladigan foydalana olish, ularning tez-tez o‘zgartirilishi va buzilishlarni aniqlanishi deyarli mumkin emas. WEP-shifrlashni tadqiq qilish zaif joylarni aniqladi, ular tufayli hujum uyushtiruvchi minimal tarmoq trafigini qo‘lga kiritganidan keyin kalitni to‘liq qayta tiklashi mumkin. Internetda jinoyatchiga kalitni bir necha soatlarda qayta tiklashga imkon beradigan vositalar bor. Shuning uchun WEP ga simsiz tarmoqda autentifikatsiyalash va konfidensiallik vositasi sifatida tayanish kerak emas. Bayon etilgan kriptografik mexanizmlar hech qaysilarini ishlatmagandan ko‘ra yaxshi, lekin ma’lum zaifliklarni hisobga olganda hujumlardan himoyalashning boshqa usullarizarur bo‘ladi.

Barcha simsiz kommunikasion tarmoqlar ta’sirlashish (bog‘lanishni o‘rnatish, aloqa sessiyasi va bog‘lanishni uzish) davrida yashirincha eshitish hujumlariga duchor bo‘ladi. Simsiz ulanish tabiatining o‘zi uni nazorat qilishga imkon bermaydi va shuning uchun uhimoyalashni talab qiladi. Kalitni boshqarish roumingda qo‘llanilganda va ochiq muhitda umumiy foydalanish holatlarida qo‘shimcha muammolarni keltirib chiqaradi.

Hujumlarning yashirinligi

Simsiz ulanish hujumning to‘liq yashirinligini ta’minlaydi. Tarmoqda joylashish o‘rnini aniqlashga imkon beradigan mos qurilma bo‘lmaganida hujum

uyushtiruvchi oson o‘z yashirinligini saqlashi mumkin va simsiz tarmoqning ishlash hududidagi istalgan joyda yashirinishi mumkin. Bunday holda jinoyatchini tutish qiyin va uni sudga berish undan ham qiyin.

Yaqin kelajakda Internetda xavsiz bo‘lmagan ulanish nuqtalari orqali yashirin kirishlarning keng tarqalishi tufayli hujumlarni tanib olishning yomonlashishi taxmin qilinmoqda. Hozirning o‘zida kirish maqsadida ishlatilishi mumkin bo‘lgan bunday nuqtalarning ro‘yxatlari e’lon qilingan ko‘plab saytlar mavjud. Ta’kidlash muhimki, ko‘plab firibgarlar tarmoqni ularning ichki resurslariga hujum qilish uchun emas, balki Internetga bepul yashirin ulanishni olish uchun o‘rganadi, ularga yashirinib boshqa tarmoqlarga hujum uyushtiradi. Agar aloqa operatorlari bunday hujumlarga qarshi ehtiyotkorlik choralarini ko‘rmasa, ularning Internetga ulanishidan foydalanishida boshqa tarmoqlarga yetkazilgan zararga ma’suliyatni zimmalariga olishi kerak.

Fizik himoyalash

Tarmoqqa simsiz ulanish qurilmasi, ulanish nuqtasi ham kichik hajmli va ko‘chma (ChPK, noutbuklar) bo‘lishi kerak. Ko‘pincha bunday qurilmalarning o‘g‘irlanishi shunga olib keladiki, jinoyatchi murakkab hujumlarni amalga oshirmasdan tarmoqqa kirishi mumkin, chunki 802.11 standartdagi asosiy autentifikatsiyalash mexanizmlari foydalanuvchining qayd etish yozuvlarini emas, balki fizik apparat qurilmasining qayd etilishiga mo‘ljallangan. Demak, bir tarmoq interfeysining yo‘qotilishi va ma’murga o‘z vaqtida xabar bermaslik shunga olib keladiki, jinoyatchi tarmoqqa ulanishni qiyinchiliksiz oladi.

Kriptografiya asoslari

Resurslar konfidensialligining zarur darajasini ta’minlash uchun ham tashkiliy choralar, ham texnik vositalar ishlatiladi. Ma’lumotlarning konfidensialligi uchun axborotlarni kriptografik muhofaza qilish vositalari ishlatiladi.

Ma’lumotlarni himoya qilish uchun kriptografik usullarning qo‘llanilishi axborotlarni muhofaza qilishning quyidagi mexanizmlarini ishlatishga imkon beradi:

a) kanallar bo‘yicha uzatiladigan ma’lumotlarni shifrlash;

b) kanallar bo‘yicha uzatiladigan axborotlar yaxlitligini nazorat qili;

c) tarmoq ob’ekti yoki sub’ektini identifikatsiyalash;

d) tarmoq ob’ekti yoki sub’ektini autentifikatsiyalash;

e) tarmoq resurslariga ruxsat etishni nazorat qilish va cheklash.

Kriptagrafik muhofaza qilish usullari tarmoqda yoki uning tashqarisida qo‘llanilishiga bog‘liq bo‘lmasdan xavfsizlikni ta’minlashning barcha hollarida zarur hisoblanadi. Ular axborotlarni va dasturlarni shifrlanishiga asoslangan. Dasturlashni shifrlanishi ularga o‘zgartirishlar kiritish imkoniyati bo‘lmasligiga kafolatni ta’minlaydi. Kriptografik ma’lumotlarni muhofaza qilish, ham ularni saqlash, ham ularni tarmoq bo‘yicha uzatishda amalga oshiriladi, binobarin, shifrlangan ko‘rinishda ma’lumotlarni saqlash ularning muhofazalanganlik darajasini oshiradi. Hozirgi vaqtda kriptografiya vositalarining ham dasturiy, ham yuqori unumdor apparatli ishlatilishi mavjud.

Simmetrik va assimetrik shifrlash

Shifrlash mexanizmi. Shifrlash uzatiladigan ma’lumotlarni yoki/va ma’lumotlar oqimi to‘g‘risidagi axborotlarni maxfiyligini ta’minlash mumkin:

- simmetrik (shifrlash va deshifrlash maxfiy kalitni ishlatish yo‘li bilan);

- asimmetrik (umumiy foydalanishdagi kalitni ishlatish bilan). Bunda shifrlash kaliti deshifrlash kalitini bilishi yoki aksincha bilishni ko‘zda tutmaydi. Bunday tizimlarning ikkita kaliti odatda “umumiy foydalanishdagi kalit” va “xususiy kalit” deyiladi.

Shifrlash mexanizmining bo‘lishi kalitlarni taqsimlanishini boshqarish mexanizmlaridan foydalanishni ko‘zda tutadi.

Simsiz tarmoqlar xavfsizligi mavzusini davom ettirish bilan shifrlash mexanizmlariga atroflicha to‘xtalamiz. Asosiy e’tibor WEP shifrlash mexanizmiga, uning avzalliklari va zaifliklariga qaratilgan. Aktiv va passiv tarmoq hujumlari, oqimli va blokli shifrlash prinsiplari atroflicha yoritiladi. Har bir usul o‘z ijobiy va salbiy tomonlariga ega, ular haqida bu so‘zlanadi.

Ko‘plab xavfsizlik texnologiyalari mavjud va ularning barchasi ma’lumotlarni himoya qilish sohasida siyosatning muhim komponentlari bo‘lgan autentifikatsiya qilish, ma’lumotlarning yaxlitligini saqlash va aktiv nazorat qilish yechimlarini taklif qiladi. Biz autentifikatsiya qilishni foydalanuvchi yoki oxirgi qurilmani (mijoz, serverlar, marshrutizatorlar, tarmoqlararo ekran va boshqalar) va uning joylashgan o‘rnini keyingi foydalanuvchilarni va oxirgi qurilmalarni mualliflashtirish bilan aniqlaymiz.

Ma’lumotlar yaxlitligi tarmoq infratuzilmasining xavfsizligi, perimetr xpvfsizligi va ma’lumotlarning konfidensialligi kabi sohalarni o‘z ichiga oladi. Aktiv nazorat qilish xavfsizlik sohasidagi o‘rnatilgan siyosatga rioya qilinayotganligiga ishonch hosil qilishga va barcha anomal holatlarni va ruxsat etilmagan ulanishlarga urinishlarni kuzatib borishga yordam beradi.

WEP shifrlash mexanizmi

WEP (Wired Equivalent Privacy-simli aloqa darajasidagi maxfiylik) shifrlash mexanizmi simmetrik oqimli shifrlash bo‘lgan RC4 (Rivest’s Cipher v.4-Rivest kodi) algoritmiga asoslangan. Avval ta’kidlanganidek, foydalanish ma’lumotlarini normal almashtirish uchun shifrlash kalitlari abonentda va radioulanish nuqtasida bir xil bo‘lishi kerak.

Algoritmning yadrosi kalit oqimni generatsiyalash funksiyasidan iborat. Bu funksiya bitlar ketma-ketligini generatsiyalaydi, ular keyin ochiq matn bilan 2 modul bo‘yicha qo‘shish orqali birlashtiriladi. Deshifrlash dastlabki matnni qayta tiklash bu kalit oqimni regeneratsiyalash va uni shifrogrammaga 2 modul bo‘yicha qo‘shishdan tashkil topadi. Algoritmning boshqa bosh qismi inisializatsiya funksiyasi hisoblanadi, u kalit oqimi generatorining bosh holatini yaratish uchun o‘zgaruvchan uzunlikdagi kalitni ishlatadi.

RC4 amalda bu uni blokining o‘lchami bilan aniqlanadigan algoritmlari sinfi hisoblanadi. Bu n parametr algoritm uchun so‘z o‘lchami hisoblanadi. Odatda n=8 bo‘ladi, lekin tahlil qilish maqsadlarida uni kamaytirish mumkin. Biroq xavfsizlik darajasini oshirish uchun bu kattalikning kattaroq qiymatini berish zarur. RC4 ning ichki holati 2n so‘zlari o‘lchamili massiv va har biri bir so‘z o‘lchamili ikkita

hisoblagichlardan tashkil topgan. Massiv S-blok sifatida ma'lum va u keyin S sifatida belgilanadi. U doimo bo‘lishi mumkin bo‘lgan 2n so‘zlar qiymatlari joy almashtirishlaridan iborat bo‘ladi. Ikki hisoblagichlar i va j orqali belgilangan.

RC4 inisializatsiya qilish algoritmi quyida keltirilgan.

Bu algoritm Keu da saqlangan va 1 bayt uzunlikka ega bo‘lgan kalitni ishlatadi. Inisializatsiya S massivni to‘ldirish bilan boshlanadi, keyin bu massiv kalitorqali aniqlanadigan joy almashtirishlar yo‘li bilan aralashtiriladi. S ustida faqat bitta amal bajarilishi bois S doimo kodli so‘zning barcha qiymatlaridan iborat bo‘ladi degan tasdiqlash bajarilishi kerak.

```
1.  Massivning boshlang‘ich to‘ldirilishi.
2.  for i=0 to 2n-1
3.  {
4.  S[i]=i
5.  j=0
6.  }
7.  Skremblirlash:
8.  for i=0 to 2n-1
9.  {
10. j=j+S[i]+Key[i mod1]
11. Joy almashtirish (S[i], S[j])
12. }
```

RC4 kalit oqimi generatori S da saqlanadigan qiymatlarning joylarini almashtiradi va har bir marta natija sifatida S dan yangi qiymatni tanlaydi. RC4 ning bitta siklida kalit oqimdan n-bitli K so‘z aniqlanadi, keyin u shifrlangan matnni olish uchun dastlabki matn bilan qo‘shiladi.

```
13. Inisializatsiya:
14. i=0
15. j=0
16. Generatsiyalash sikli:
17. i=i+1
```

18. j=j+S[i]

19. Joy almashtirish (S[i], S[j])

20. Natija: K=S[S[i]+ S[j]]

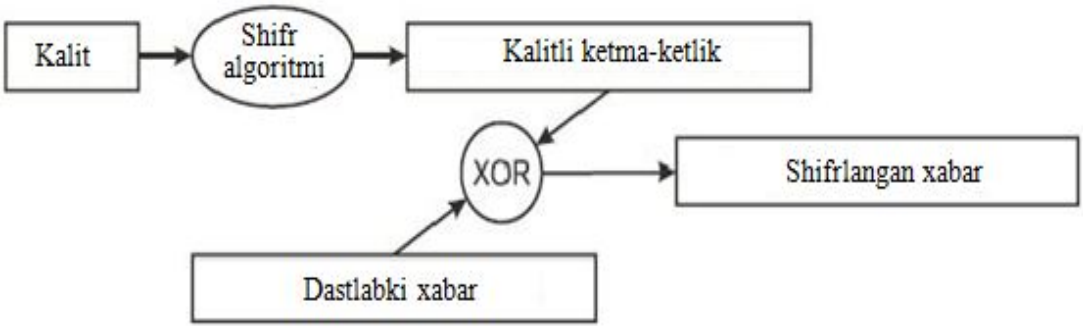
WEP-protokolning o‘ziga xos xususiyatlari:

- shifrlash kalitlarini oddiy terib ko‘rishga bog‘liq bo‘lgan hujmlarga barqaror, bu zarur kalitning uzunligi va kalitlarni almashtirilishi tezligiva inisializatsiyalovchi vektor orqali ta’minlanadi;
- har bir xabar uchun o‘z sinxronlashishi. Bu xususiyat buzilgan va yo‘qotilgan paketlar soni katta bo‘ladigan uzatish muhitiga ulanish darajasi protokollari uchun muhim hisoblanadi.
- samaradorligi: WEP ni oson ishlatish mumkin;
- ochiqligi;
- IEEE 802.11 standarti tarmoqlarida WEP-shifrlashni ishlatish majburiy hisoblanmaydi.

Ma’lumotlar oimini uzluksiz shifrlash uchun oqimli va blokli shifrlash ishlatiladi.

Oqimli shifrlash

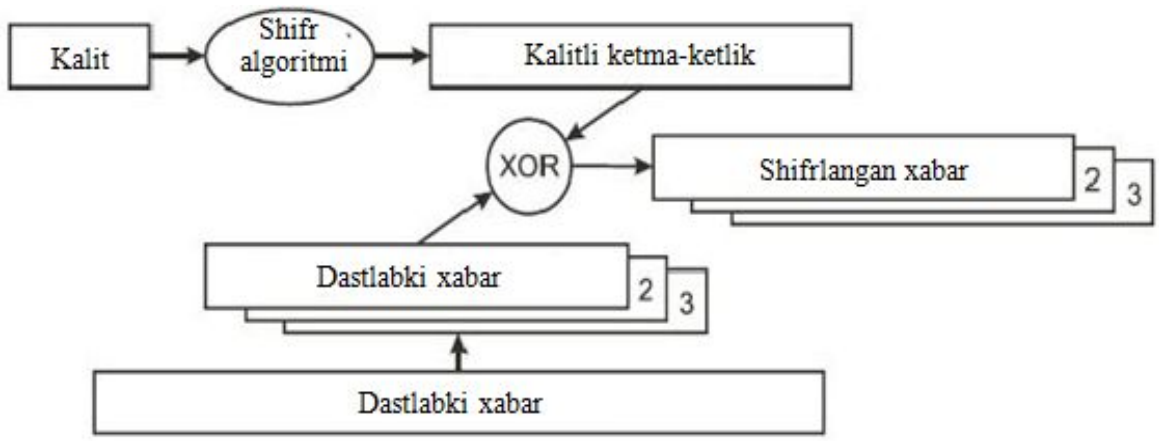
Oqimli shifrlashda oldindan berilgan kalit va dastlabki xabar asosida shifrlash algoritmi generatsiyalaydigan kalitli ketma-ketlikda 2 modul bo‘yicha (“inkor qiluvchi YoKI”, XOR funksiyasi) bitlab qo‘shish bajariladi. Kalitli ketma-ketlik shifrlanishi kerak bo‘lgan dastlabki xabar uzunligiga mos bo‘lgan uzunlikka ega bo‘ladi (9.1-rasm).



9.1-rasm. Oqimli shifrlash

Blokli shifrlash shifrlash jarayonida o‘zgarmaydigan oldindn 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 (9.2-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.

Oqimli shifrlash va blokli shifrlash elektron kodli kitob (YeSV) usulini ishlatadi. YeSV usul shu bilan xarakterlanadiki, kirishdagi o‘sha bir dastlabki xabar doimo chiqishda o‘sha bir shifrlangan xabarni hosil qiladi. Bu xavfsizlik tizimidagi bo‘shliq, shunga ko‘ra tashqaridagi kuzatuvchi shifrlangan xabardagi takrorlanadigan ketma-ketliklarni aniqlash bilan dastlabki xabar takibini nisbiy o‘xshashligini asoslangan ko‘zda tutish holatida bo‘ladi.



2-rasm. Blokli shifrlash

Ko‘rsatilgan kamchiliklarni tuzatish uchun quyidagilar ishlatiladi:

- inisializatsiya vektorlari (Initialization Vectors-IVs);
- teskari aloqa (feedback modes).

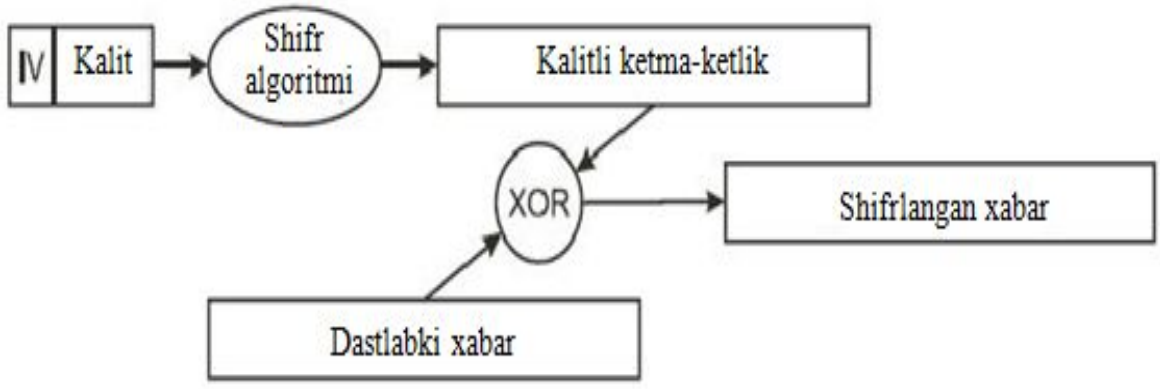
Shifrlash jarayoni boshlanguncha 40- yoki 104-bitli maxfiy kalit simli tarmoqqa kiradigan barcha stansiyalar orasida taqsimlanadi. Maxfiy kalitga inisializatsiya vektori qo‘shimcha qilinadi.

Inisializatsiya vektori (Initialization Vectors-IVs)

Inisializatsiya vektori kalitli ketma-ketlikni modifikatsiyalash (o‘zgartirish) uchun ishlatiladi. Inisializatsiya vektori ishlatilganda kalitli ketma-ketlik shifrlash algoritmi orqali generatsiyalanadi, uning kirishiga IV bilan qo‘shilgan maxfiy kalit beriladi. Inisializatsiya vektori o‘zgarganda kalitli ketma-ketlik ham o‘zgaradi. 3-rasmda dastlabki xabar shifrlash algoritmi orqali uning kirishiga maxfiy kalit va inisializatsiya 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 inisializatsiya vektorining yangi qiymatini ishlatilishini tavsiya qiladi.
Shunday qilib, ko‘p marta uzatiladigan o‘sha bir shifrlanmagan freym har bir marta ulkan shifrlangan freymni hosil qiladi.

Inisializatsiya vektori 24 bit uzunlikka ega va 40- yoki 104-bitli WEP shifrlash bazaviy kaliti bilan shunday qo‘shiladiki, shifrlash algoritmi kirishiga va 64- yoki 128-bitli kalit beriladi. Inisializatsiya vektori qabul qiluvchi tomon bu freymni muvaffaqiyatli dekodlashi uchun radiokanaldagi freym sarlavhasida shifrlanmagan ko‘rinishda bo‘ladi.



9.3-rasm. WEP shifrlash algoritmi

Odatda, 64- yoki 128-bitli uzunlikdagi kalitlar bilan WEP shifrlashdan foydalanish haqida gapirilishiga qaramasdan kalitning samarali uzunligi inisializatsiya vektori shifrlanmagan ko‘rinishda uzatilishi sababli faqat 40- yoki 104-bitni tashkil etadi. Qurilmada 40-bitli samarali kalitda shifrlash sozlanishlarida 5 baytli ASCII-simvollar (5·8=40) yoki 10 ta o‘noltilik sonlar (10·4=40) va 104-bitli samarali kalitda 13 baytli ASCII-simvollar (13·8=104) yoki 26 ta o‘noltilik sonlar (26·4=104) kiritiladi. Ba’zi qurilmalar 128-bitli kalit bilan ishlashi mumkin.

Nazorat savollari

1. WEP shifrlash mexanizmi nima uchun ishlatiladi?
2. WEP-protokolning o‘ziga xos xususiyatlarini tushuntiring.
3. Oqimli shifrlash nima?
4. Inisializatsiya vektori nima uchun ishlatiladi?

10-ma’ruza

Simsiz tarmoqlarda autentifikatsiyalash. WPA spetsifikatsiyasi.

Reja:

1 Simsiz tarmoqlarda autentifikatsiyalash.

2. WPA spetsifikatsiyasi.

Ma’lumotlarni himoyalalashda “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 xaqiqiyligini tekshirish protsedurasi uchun ishlatiladi.

Cimsiz tarmoqlarda autentifikatsiyalash standartlari bir nechtani tashkil etadi. Ulardan har biri o‘z kamchiliklariga va avzalliklariga ega. Har birida o‘zining murakkab ishlash prinsipi mavjud. Ko‘p sonli qo‘shimcha sxemalar, zarur sozlanishlarli D-Link AirPlus XtremeG Wreless Utility utilitlari skrinshotlarining bo‘lishi xarakterli hisoblanadi. Absolyut himoyalangan standartlar bo‘lmaydi va shuning uchun har bir autentifikatsiyalash mexanizmining zaifliklari masalalariga etibor qaratish kerak.

Cimsiz tarmoqlarda asosiy autentifikatsiyalash standartlari IEEE802.11, WPA, WPA2, va 802.1x standartlari hisoblanadi.

Oddiy xavfsizlikka ega 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. Cimsiz 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 abonenti talab qilinadigan simsiz lokal tarmoqqa ulanishni 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 SSID larga ega bo‘lishi mumkin.

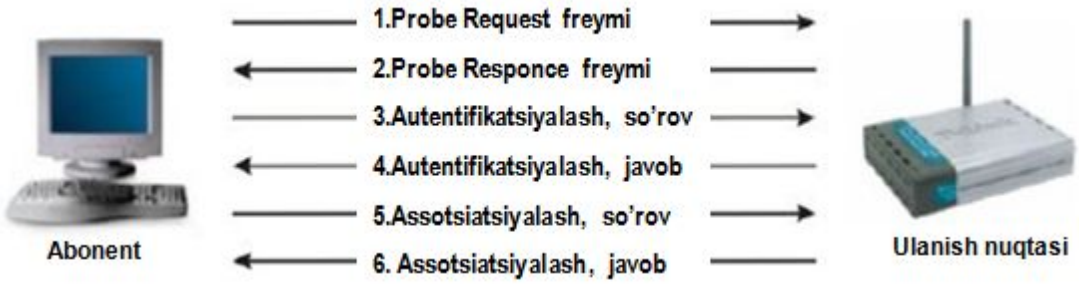
IEEE802.11 standartida abonentni autentifikatsiyalash prinsipi

IEEE802.11 standartida abonentni autentifikatsiyalash aniq bir abonentni tarmoq resurslariningfoydalanuvchisi emas, radioulanish abonent qurilmasini autentifikatsiyalashga mo‘ljallangan. IEEE802.11 simsiz lokal tarmoq abonentini autentifikatsiyalash jarayoni quyidagi bosqichlardan tashkil topgan (10.1-rasm):

1. Abonent (Client) Rrobe Request freymni barcha radiokanallarga yuboradi.
2. Har bir radioulanish nuqtasi (Access Point-AP) abonent joylashgan radio ko‘rinish zonasida Rrobe Responce javob freymini yuboradi.
3. Abonent o‘zi uchun avzal bo‘lgan radioulanish nuqtasini tanlaydi va unga xizmat ko‘rsatadigan radiokanalga autentifikatsiyalashga (Authentication Request) so‘rovni yuboradi.
4. Radioulanish nuqtasi autentifikatsiyalashning tasdiqlanishini (Authentication Rerlu) yuboradi.
5. Muvvafaqiyatli atentifikatsiya holatida abonent radioulanish nuqtasiga assotsiatsiya freymini (Association Request) yuboradi.
6. Radioulanish nuqtasi javobga assotsiatsiyani tasdiqlash freymini (Association Responce) yuboradi.
7. Abonent endi radioulanish nuqtasi va simli tarmoq bilan foydalanish trafiklarini almashtirishni amalga oshirishi mumkin bo‘ladi.

Aktivlashtirishda simsiz abonent o‘z radio ko‘rinish zonasida Rrobe Request boshqarish freymlari yordamida radioulanish nuqtalarini qidira boshlaydi. Rrobe 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 Rrobe Request freymida so‘ralgan parametrlarni qoniqtiradigan radioulanish nuqtalaridan har biri sinxronlashtiruvchi axborotlar va radioulanish nuqtasining joriy yuklanishi haqida ma’lumotlardan iborat Rrobe Responce freymi bilan javob beradi. Abonent qaysi radioulanish nuqtasi bilan ishlashini ular ishlay oladigan radio almashtirish tezliklari va yuklanishlarini taqqoslash yuli bilan aniqlaydi. Avzalroq radioulanish nuqtasi aniqlanganidan keyin abonent autentifikatsiyalash fazasiga o‘tadi.



10.1-rasm. 802 standart bo‘yicha autentifikatsiyalash

Ochiq autentifikatsiyalash

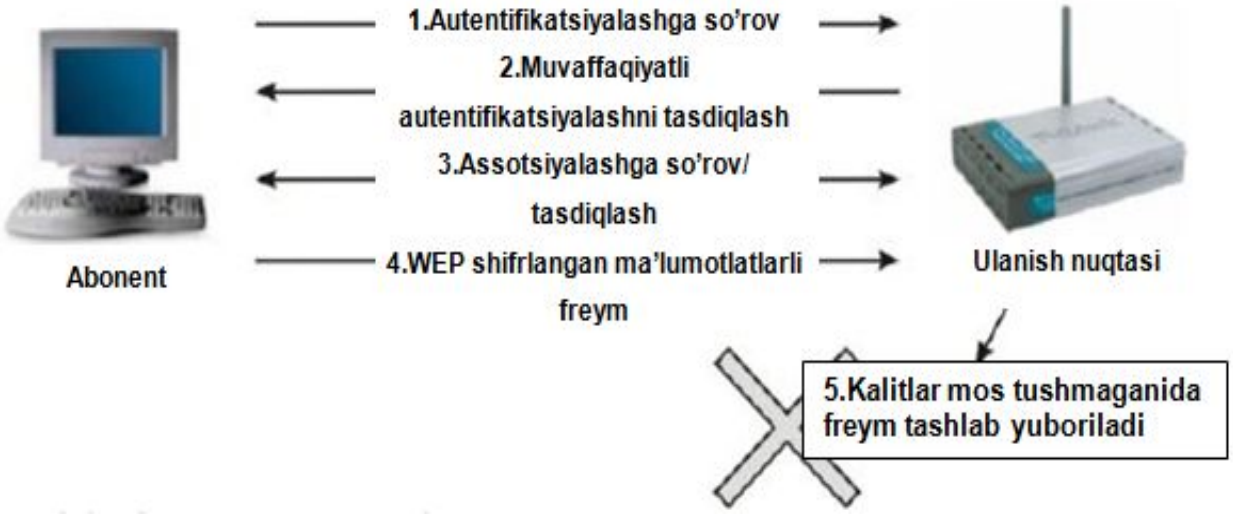
Ochiq autentifikatsiyalash birlamchi tushunishda autentifikatsiyalash algoritmi hisoblanmaydi. Radioulanish nuqtasi dalanishochiq autentifikatsiyalashning barcha so‘rovlarini qoniqtiradi. Bunday qaraganda bu algoritmdan foydalanish ma’nosiz ko‘rinadi, lekin shuni e’tiborga olish kerakki, 1997 yilda yaratilgan 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 (10.2-rasm).



10.2-rasm. Ochiq autentifikatsiyalash

Umumiy kalitli autentifikatsiyalash

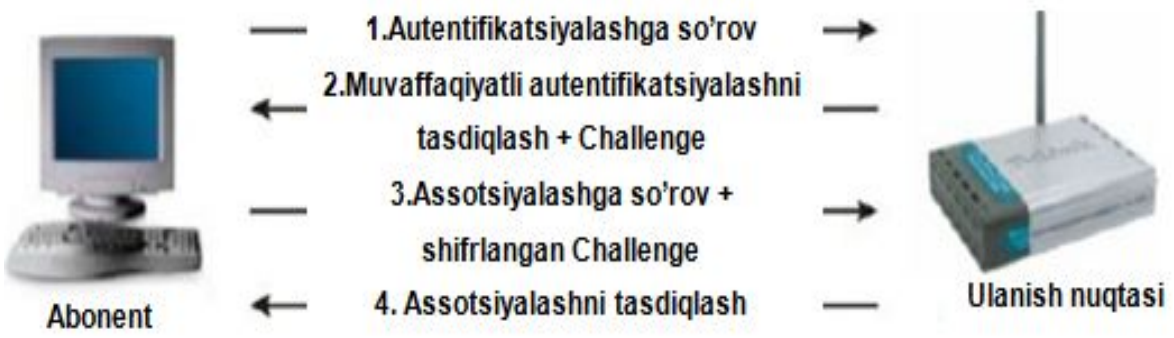
Umumiy kalitli autentifikatsiyalash IEEE802.11 standartining ikkinchi autentifikatsiyalash usuli hisoblanadi. Umumiy kalitli autentifikatsiyalash abonentda WEP shifrlash statik kalitini sozlanishini talab qiladi. Autentifikatsiyalash jarayoni 3-rasmda keltirilgan:

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.



10.3-rasm. Umumiy kalitli autentifikatsiyalash

MAS-manzil bo‘yicha autentifikatsiyalash

Uning MAS-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. MAS-manzil bo‘yicha autentifikatsiyalashda abonentning MAS-manzili legitiv abonentlar lokal saqlanadigan ruxsat etiladigan manzillar ro‘yxati bilan yoki autentifikatsiyalashning tashqi serveri yordamida taqqoslash amalga oshadi (10.4-rasm). MAS-manzil bo‘yicha autentifikatsiyalash begona abonentlarning ulanishi ehtimolligini kamaytirish uchun ochiq autentifikatsiyalashga va umumiy kalitli autentifikatsiyalashga qo‘shimcha sifatida ishlatiladi.

10.4-rasm. Tashqi server yordamida autentifikatsiyalash

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 ishlatililganda moslashuvchanligiga ta’sir etishi mumkin.

Ochiq autentifikatsiyalashning zaifliklari

Ochiq autentifikatsiyalash radioulanish nuqtalariga abonent legitiv yoki legitiv emasligini 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. 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 (5-rasm). WER shifrlash xabar matni bilan XOR operatsiyaning bitlab bajarilishi va kalitli ketma-ketlik yo‘li bilan amalga oshiriladi, buningnatijasida 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

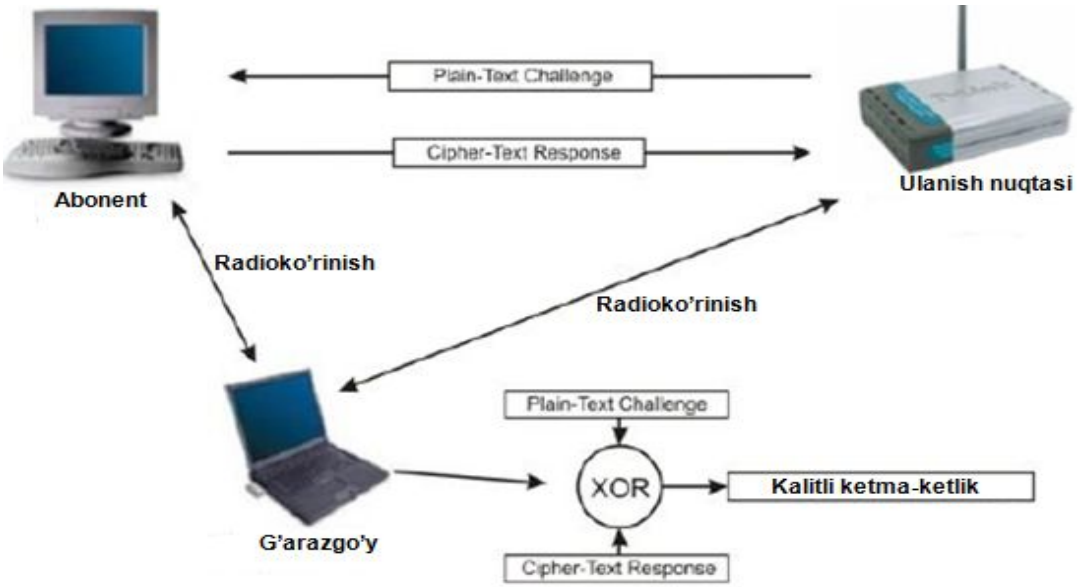
IEEE 802.11 standarti MAS-manzillarni uzatilishini va radioulanish nuqtasini ochiq ko‘rinishda bo‘lishini talab qiladi.Simsiz tarmoqda MAS-manzil bo‘yicha autentifikatsiyalashni ishlatilishi natijasida jinoyatchi autentifikatsiyalash usulini o‘z MAS-manzilini legitiv MAS-manzil bilan almashtirishi bilan aldashi mumkin. MAS-manzilni almashtirilishi lokal ma’murlashtiriladigan MAS-manzillardan foydalanishga ruxsat etadigan simsiz adapterlarda bo‘lishi mumkin. Jinoyatchi legitiv abonentlarning MAS-manzillarini aniqlash uchun IEEE 802.11 protokoli trafigi analizatoridan foydalanishi mumkin.

WPA spesifikatsiyasi

2001 yilning mayigacha 802 simsiz tarmoqlar uchun axborot xavfsizligi vositalarini standartlashtirish IEEE 802.11e ishchi guruhini joriy etilishiga kirdi,

lekin keyin bu muammo alohida bo‘linmaga ajratildi. Ishlab chiqilgan 802.11i standart uzatiladigan ma’lumotlarni shifrlash vositalarini, shuningdek, foydalanuvchilar va ishchi stansiyalarni markazlashtirilgan autentifikatsiyalashni ko‘zda tutish bilan 802.11 protokolining imkoniyatlarini kengaytirishga mo‘ljallangan.

Wi-Fi qurilmalarining asosiy ishlab chiqaruvchilari WEGA (Wireless Ethernet Compatibility Alliance), boshqacha nomlanganda Wi-Fi Alliance tashkiloti sifatida IEEE 802.11e standartini ratifikatsiyalanishini kutishdan charchab, IEEE bilan birgalikda 2002 yilning noyabrida Wi-Fi Protected Access (WRA) spesifikatsiyasini e’lon qildi, uning mosligi turli ishlab chiqarkvchilarning qurilmalarini moslashuvchanligini ta’minlaydi.



10.5-rasm. Umumiy kalitli autentifikatsiyalashning zaifligi

Yangi WRA xavfsizlik standarti WER taqdim etgandan ko‘ra katta xavfsizlik darajasini ta’minlaydi. U WER va 802.11i orasiga ko‘prik qo‘yadi va muhim avzallikka egaki, eskiroq qurilmalarning kichik dasturiy ta’minoti apparatli o‘zgartirishlar kiritilishisiz almashtirilishi mumkin. IEEE *kalitni yaxlitligining vaqtinchalik protokolini* (Temporal Key Integrity Protocol, TKIP) taklif etdi.

TKIP protokoli tomonidan kiritilgan TKIP asosiy takomillashtirishlar:

- *shifrlash kalitlarini har freymda o‘zgartirish.* WER-kalit tez o‘zgaradi va har bir freym uchun boshqa bo‘ladi;
- *xabarning yaxlitligini nazorat qilish.* Freymlar bilan yashirin manipulyatsiyalar va freymlarni qayta ishlatilishini oldini olish maqsadida ma’lumotlar freymlarining yaxlitligini samarali nazorat qilish ta’minlanadi;
- *kalitlarni boshqarishning takomillashtirilgan mexanizmi.*

Nazorat savollari

1. Oddiy xavfsizlikka ega IEEE802.11 standartini tushuntiring
2. 802.11 autentifikatsiyalash mexanizmlarining zaifliklarini tushuntiring
3. WPA spesifikatsiyasini tushuntiring
4. Umumiy kalitli autentifikatsiyalashning zaifligini tushuntiring

11-ma’ruza

Simsiz tarmoqlarda autentifikatsiyalash 802.11i (WPA2).

Reja:

1 WPA2 spetsifikatsiyasi.

2. Xavfsizlik tizimining umumiy ishlash prinsipi

Simsiz texnologiyalar uchun axborot xavfsizligini taъminlash masalalari juda muxim hisoblansada, birinchi Wi-Fi standartlari zaif ximoya 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‘zgarmaydigan) 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.

Xavfsizlik tizimining umumiy ishlash prinsipi 11.1-rasmda sxematik tasvirlangan.

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 maъlum bo‘lgan yangi IEEE 802.11i standarti paydo bo‘ldi. IEEE 802.11i standarti simsiz tarmoqlarning xavfsizligi uchun uzoq muddatli va kengaytirilgan echim 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 taъminlashni ko‘zda

tutgan “kuchaytirilgan tarmoq xavfsizligi” - RSN (ingl-n *Robust Security Network*) konsepsiyasini ishlatadi. Bu esa apparat qismida va dasturiy taъminotda o‘zgarishlarni talab qiladi va shu bilan RSN ga to‘liq moslashadigan tarmoqlarni WEP protokolini ishlatadigan mavjud jixozlar bilan moslashmaydigan qilib qo‘yadi. Shunday qilib, bir qancha vaqt ham RSN, ham WEP jixozlari qo‘llab quvvatlanadi, keyinchalik esa WEPli uskunalar ishlatishdan umuman chiqarib tashlanadi.

11.1-rasm. Xavfsizlik tizimining umumiy ishlash prinsipi

WPA2 (Wireless Protected Access ver. 2.0) – bu Wi-Fi simsiz tarmoqlarida maълumotlarni himoyalanishini taъminlaydigan 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

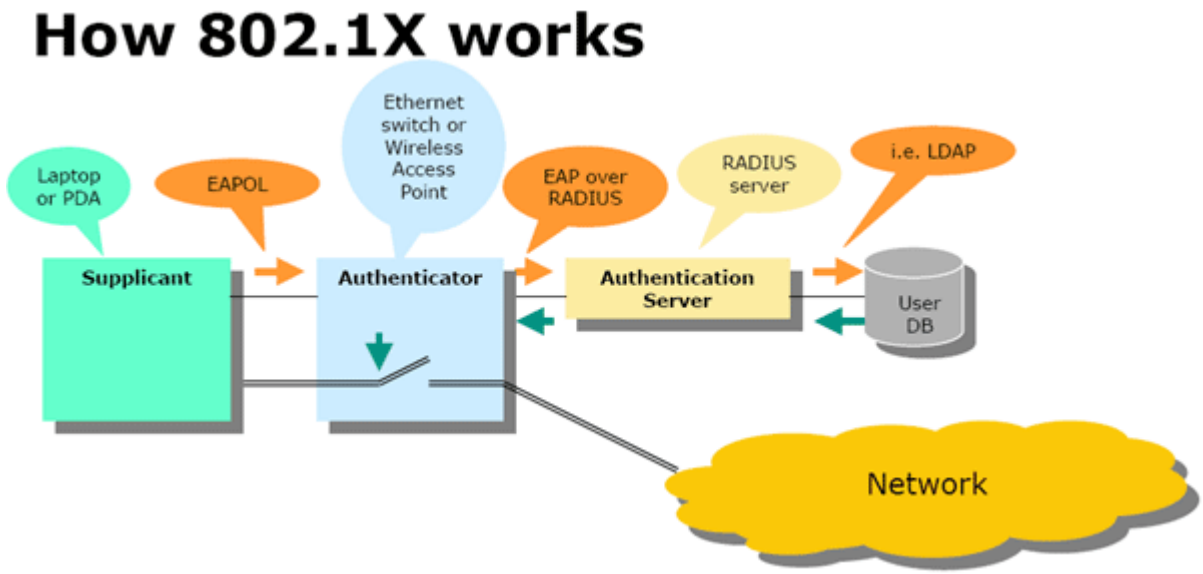
Standard) shifrlash algoritmini va 802.1X autentifikatsiyalashni majburiy ishlatilishini ko‘zda tutadi.

Bugungi kunga kelib korporativ tarmoqda ishonchli xavfsizlik mexanizmini taъminlash uchun WPA2 qo‘llanadigan qurilmalar va dasturiy taъminot ishlatilishi zarur (va shart). Oldingi protokollar avlodlari bo‘lgan WEP va WPA etarli bo‘lmagan kuchli himoyalashli 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 yaxlitligi 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. Taъkidlash zarurki, autentifikatsiyalash “port darajasida”, – yaъni foydalanuvchi faqat uning autentifikatsiyalanishi (hisobga olish maъlumotlari) 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 (11.2-rasm).



11.2-rasm. 802.1x: ishlash prinsipi

Autentifikatsiyalash funksiyasi EAP protokoliga yuklanadi, u o‘z-o‘zidan faqat autentifikatsiyalash usullari uchun karakas hisoblanadi. Protokolning o‘ziga xos xususiyati shundan iboratki, uni autentifikatorda (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 mijozmashinasida ishga tushirilgan dastur;
- Authenticator — ulanish tuguni, autentifikator (802.1x protokoli qo‘llanadigan simsiz ulansh nuqtasi yoki simli kommutator);

- Authentication Server —autentifikatsiyalash serveri (ooatda bu RADIUS-serveri).

Endi autentifikatsiyalash jarayonini o‘zini ko‘rib chiqamiz. U quyidagi bosqichlardan tashkil topgan:

1. Mijoz ulanish nuqtasi tomonga autentifikatsiyalashga so‘rovni (EAP-start message) jo‘natishi mumkin;

2. Ulanish nuqtasi (Autentifikator) mijozga javob sifatida uni autentifikatsiyalanishiga so‘rovni (EAP-request/identity message) jo‘natadi.

Autentifikator, agar uning portlaridan biri aktiv holatga o‘tganini ko‘rsa, mustaqil ravishda EAP-requestni jo‘ntadi.

3. Mijoz javob tariqasida kerakli maълumotlarli EAP-response packetni jo‘natadi, uni ulanish nuqtasi (autentifikator) Radius-server (autentifikatsiyalash serveri) tomoniga qayta yo‘naltiradi;

4. Autentifikatsiyalash serveri autentifikatorga (ulanish nuqtasiga) challenge-paketni (mijozning haqiqiyligi haqidagi maълumotlarni so‘rashni) jo‘natadi;

5. Keyin server va mijozni o‘zaro autentifikatsiyalash jarayoni bo‘lib o‘tadi. Paketlarni u yoqqa va bu yoqqa qayta uzatilishi bosqichlari soni EAP usuliga bog‘liq ravishda o‘zgaradi, lekin simsiz tarmoqlar uchun faqat server va mijozni o‘zaro autentifikatsiyalash (EAP-TLS, EAP-TTLS, EAP-PEAP) va aloqa kanalini oldindan shifrlanishili «strong» autentifikatsiyalash qo‘llanilsa bo‘ladi;

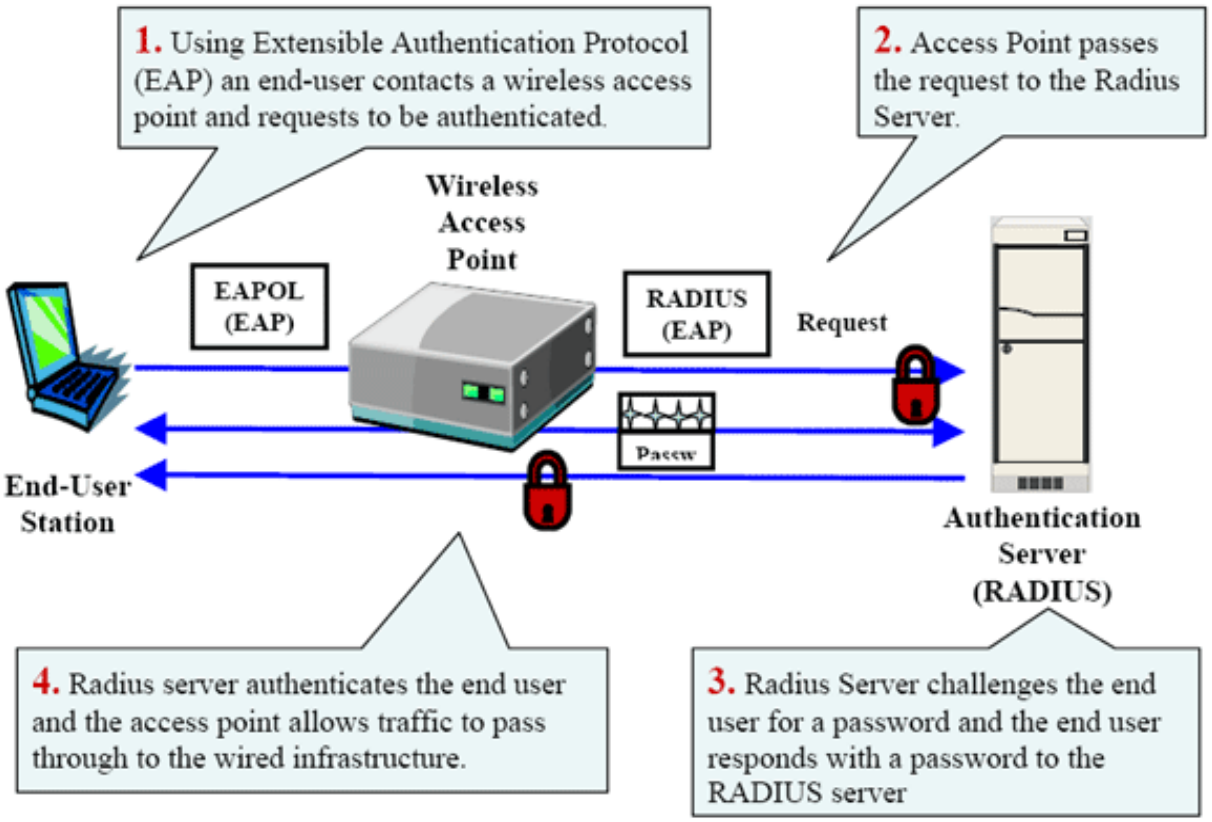
6. Keyingi bosqichda autentifikatsiyalash serveri mijozdan zarur maълumotlarni olishi bilan autentifikatorga xabar berish bilan foydalanuvchiga ulanishga ruxsat etadi (accept) yoki ruxsat etmaydi (reject).

Autentifikator (ulanish nuqtasi), agar RADIUS-server tomonidan ijobiy javob (Accept) kelgan bo‘lsa, Supplicant uchun portni ochadi;

7. Port chiladi, autentifikator mijozga jarayonni muvaffaqiyatli yakunlanganligi haqidagi xabarni uzatida va mijoz tarmoqqa ulanishni oladi.

8. Mijoz uzilganidan keyin ulanish nuqtasidagi port yana “yopiq” holatga o‘tadi.

Tavsif etilgan jarayon 11.3-rasmda keltirilgan.



11.3-rasm. Autentifikatsiyalash jarayoni

WPA2 protokollari ikkita personal (Personal) va korporativ (Enterprise) rejimlarda ishlaydi. **WPA2-Personal** rejimida ochiq matnda chiqarilgan parolli luqmadan 256-razryadli PSK kalit (PreShared Key) generatsiyalanadi. PSK kalit SSID (Service Set Identifier) identifikatori bilan simsiz qurilmalarning o‘zaro taъsirlashish uchun PTK (Pairwise Transient Key) vaqtinchalik seanslar kalitlarini generatsiyalash uchun ishlatiladi. WEP statik protokolidagi kabi WPA2-Personal protokoliga tarmoqning simsiz qurlmalarida kalitlarni tarqatish va saqlash zaruratiga bog‘liq maъlum 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, unig ko‘plab atentifikatsiyalash korporativ servislari bilan integratsiyalanishi esa ro‘yxatga olish yozuvlari asosida

ulanishni nazorat qilishga imkon beradi. Bu rejimda ishlash uchun foydalanuvchining nomi va paroli, xavfsizlik sertifikati yoki bir martalik parol kabi registratsion maълkmotlar 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 xzmat qiladi, u foydalanuvchilarni autentifikatsiyalashi va ham simli kommutatorlar uchun, ham simsiz ulanish nuqtalari uchun yaroqli bo‘lgan qurilmalarni qo‘llaydi.

WPA protokolidan farqli ravishda barqarroq AES shifrlash algoritmi ishlatiladi. WPAga o‘xshash WPA2 ham ikkita WPA2-PSK va WPA2-802.1x turlarga bo‘linadi.

Maълumotlarni yaxlitligi va konfidensialligini taъminlashning 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: kondensiallikni taъminlash 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 taъminlaydi. O‘zaro autentifikatsiyalash va kalitlarni etkazilishi IEEE 802.1x/EAP protokoli asosida amalga oshiriladi. Xavfsiz Independent Basic Service Set (IBSS) Ad-Hoc tarmoqlardagi xafsizlikni oshiradi. Rouming taъminlanadi.

Simsiz tarmoqlar xavfsizligini ta’minlashdagi CCMP mexanizmiga hissani 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).

Yaъni bu turdagi algoritmlarga WEP-shifrlashli yoki WEP-shifrlashsiz Open System va Shared Key autentifikatsiyalash kiradi.

RSNA-algoritmlarga quyidagilar kiradi:

- TKIP;
- CCMP;
- RSNA o‘rnatilishi vaterminallashtirilishi protsedurasi (shu jumladan IEEE 802.1x autentifikatsiyalashdan foydalanish);
- Kalitlarni almashlash protsedurasi.

Bunda CCMP algoritmi majburiy, TKIP esa opsional hisoblanadi va eski qurilmalar bilan moslashuvchanlikni taъminlash uchun mo‘ljallangan.

Standart orqali ikkita funsional modellar ko‘zda tutilgan:

- IEEE 802.1x bo‘yicha autentifikatsiyalashli, yaъni EAP protokoli qo‘llaniladigan;
- Autentifikator va mijozda yozilgan oldingan aniqlangan kalit yordamida (bunday rejim Preshared Key, PSK deyiladi). Bunday holda PSK kalit PMK kalitining rolini bajardi va ularni keyingi autentifikatsiyalash 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 maъlumotlarni 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 taъminlashi kerak. Bu algoritm FIPS PUB 197 spetsifikatsiyada aniqlangan AES shifrlash CCM-algoritmiga asoslangan. CCMPda ishlatiladigan barcha AES-jarayonlar 128-bitlli kalitli va 128-bitli o‘lchamli blokli AESni ishlatadi.

Standartdagi oxirgi yangi joriy etish ulanish nuqtalari orasidagi PMK kalitni keshlash protsedurasi va oldindan autentifikatsiyalashdan foydalanish bilan tezkor rouming texnologiyasini qo‘llash hisoblanadi.

PMK kalitni keshlash 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 haqiqiyliki 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, yaъni ulardan oldindan PMK kalitni olishi mumkin. Va agar keyinchalik u bog‘langan ulanish nuqtasi ishdan chiqsa yoki signal bunday tarmoq nomili qandaydir ulanish nuqtasidagidan kuchsizroq bo‘lsa, u holda mijoz keshlangan PMK kalitli tezkor sxema bo‘yicha qayta bog‘lanishni amalga oshiradi.

11.1-jadval.

Simsiz tarmoqlarda ishlatiladigan shifrlash protokollarining imkoniyatlari

Protokol	Open System	Shared Key	WPA-PSK	WPA-EAP	WPA2-PSK	WPA2-EAP
Shifrlash algoritmi	RC4	RC4	RC4	RC4	AES (CTR)	AES (CTR)
Autentifikatsi-yalash	Yo‘q	Presha-red Key	Presha-red Key	IEEE 802.1x	Presha-red Key	IEEE 802.1x
Kalitning uzunligi, bit	64 yoki 128	64 yoki 128	128 (shifr.), 64 (autent.)	128 (shifr.), 64 (autent.)	128	128
Kalitning takrorlanishi	24-bitli IV	24-bitli IV	48-bitli TSC	48-bitli TSC	48- bitli PN	48-bitli PN
Маълumotlarning yaxlitligi	CRC-32	CRC-32	Michael	Michael	AES (CBC-MAC)	AES (CBC-MAC)
Sarlavhaning yaxlitligi	Yo‘q	Yo‘q	Michael	Michael	AES (CBC-MAC)	AES (CBC-MAC)
Kalitlarni boshqarish	Butun tarmoq uchun statik			EAP asosida	Butun tarmoq uchun statik	EAP asosida

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 bolandi. Agar oldin barcha buzish vositalari faqat Unix-platformalarda ishlagan bo‘lsa, endi ularda ko‘pchiligi Windowsda, ayrimlari esa hatto Masda ishlashmoqda. Keyinchalik oddiy parolli luqmalardan foydalanish bilan WPA-PSK va LEAPni birmuncha vaqtdabuzishga imkon beradigan real ishlaydiga vositalar yaratildi. Simsiz tarmoqlar ham “Xizmat ko‘rsatishni rad etish” turdagi hujumlardan himoyalanmagan bo‘lib qolmoqda.

Uchta asosiy hujumlar guruhi mavjud:

Fizik darajada. Ulanish nuqtasining ishchi chastotasidagi quvvatli nurlanish manbaidan foydalanish (signalni bo‘g‘ish);

Xizmat freymlari qo‘llaniladigan hujumlar. Xizmat freymlari uzatilganida ulanish nuqtasi va mijoz o‘zar autentifikatsiyalashni bajarmaydi, shuninguchun buzuvchi MAC-mnzilni almashtirib qo‘yishi va qonuniy mijoz nomidan freymlarni jo‘natishi mumkin.

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.

11.2-jadval

Tarmoqning turiga bog‘liq ravishda turli xavfsizlikni taъminlash usullarining qo‘llanilishii

Tamoq 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	+	–	+

Simsiz tarmoqning turiga bog‘liqravishda 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 amalgaoshirilishiuchun dastlab WPA2ni buzish kerak bo‘ladi. Ulanishli variantdan turli usullar orqali himoyalanish mumkin:

- Kommutatordagi ishlatilmaydigan portlarni o‘chirish;
- Lokal tarmoqda IEEE 802.1x autentifikatsiyalashni ishlatish;

- Port Security funksiyasini qo‘llash (kommutatorda qaysi portlarga qanday MAS-manzillar ulanishi mumkinligini ko‘rsatish);
- Simsiz ulanish 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 ulanish nuqtalaridan foydalanish.

Nazorat savollari

1. 802.1x: ishlash prinsipini tushuntiring
2. Autentifikatsiyalash jarayonini tushuntiring
3. IEEE 802.1x so‘rovlaridan foydalanish orqali hujumlarini tushuntiring
4. Ulanishli variantdan turli usullar orqali himoyalanishini tushuntiring

12-ma’ruza

Uzatiladigan ma’lumotlarning butunlik va konfedentsialligi texnologiyasi

Reja:

1 Uzatiladigan ma’lumotlarning yaxlitligi

2. Maъlumotlarning 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. Tarmoq xavfsizligini taъminlash vositalarining katta qismi aynan bu turdagi buzishlarni oldini olishga yo‘naltirilgan.

Axborot xavfsizligi sohasidagi asosiy xarakteristikalar:

1. Maъlumotlarning konfidensialligi;

2. Maъlumotlarning yaxlitligi;

3. Maъlumotlarning mumkinligi hisoblanadi.

Maъlumotlarning konfidensialligi bu maъlumotlarga ulanishga ega bo‘lgan shaxslar doirasiga maъlum cheklashlarni kiritilishini ko‘zda tutadi. Konfidensiallik darajasi oshkora qilinmaydigan, cheklangan shaxslar doirasiga mo‘ljallangan, sir hisoblanadigan maъlumotlarni bo‘lishiga bog‘liq ravishda maъlumotlarning egasi tomonidan subъektiv aniqlanadigan qandaydir shartli xarakteristika (o‘ta muhimlik, mutlaqo maxfiy, maxfiy, xizmat manfaatlari uchun, bosish uchun emas va h.k.) orqali ifodalanadi. Tabiiyki, o‘rnatilgan maъlumotlar konfidensialligi darajasi ularni aborot tizimlarida ishlov berilishida va simsiz tarmoq bo‘yicha uzatilishida saqlanishi kerak.

Simsiz aloqa tarmoqlari axborot xavfsizligini taъminlash maqsadida xalqaro tashkilotlarning satandartlari 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 taъsir 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 taъsir qiladi. Bir tomondan tarmoqning himoyalanganligi ortadi, boshqa tomondan esa qo‘shimcha qurilmalarning hajmi ortadi, bu o‘z navbatida ishonchlilikni, unumdorlikni kamayishiga olib keladi va foydlanuvchilarning foydlana olishga 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 himoyalanmagan amaliy dasturiy vositalarni rad etishga majburlaydi.

Rivojlangan mamlakatlarning xalqaro tajribasi ko‘rsatadiki, simsiz aloqa tarmoqlari axborot xavfsizligi muammosining echimi mos qonunlar, standartlar va meъyoriy-uslubiy hujjatlar ko‘rsatmalari va talablariga asoslanishi kerak.

Qonunchilik talablarining so‘zsiz bajarilishi va simsiz aloqa tarmoqlari axborot xavfsizligi sohasidagi zarur meъyoriy-huquqiy hujjatlarni o‘z vaqtida ishlab chiqish va qabul qilish axborot xavsizligini buzilishini oldini olishning kuchli qonuniy-huquqiy chorasi hisoblanadi, shuning uchun bugungi kunda axborot xavfsizligini taъminlashning turli jihatlarining ichidan eng muhimi va dolzarbi axborot xavfsizligining meъyoriy-huquqiy taъminlanishi masalasi hisoblanadi.

Simsiz aloqa tarmoqlarining axborot xavfsizligiga umumiy talablar tarmoq egasi yoki bu tarmoqda aylanadigan maъlumotlar egasi tomonidan axborot xavfsizligi tashkil etuvchilari – konfidensiallik, yaxlitlik va foydalana olishgliklarning 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 echadigan masalalarga muvofiq dasturiy texnik vositalarga va protokollarga majburiy talablarga tranformatsiyalanadi.

Zamonaviy simsiz aloqa tarmoqlarini qurishda vujudga keladigan muhim muammo ishonchliligi, yashovchanligi va barqarorligi bilan bir qatorda ularning axborot xavfsizligini taъminlash 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 taъminlashning mos choralarini va mexanizmlarini yaratilishini ko‘zda tutadi. Xalqaro tajriba ko‘rsatadiki, simsiz aloqa tarmoqlarining axborot sohasiga buzuvchining taъsir etishi ularning hayot siklining texnologik va ekspluatatsiya qilish bosqichlarida amalga oshirilishi mumkin, shuning uchun ularning axborot xavfsizligini taъminlash 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.), yaъni noxush oqibatlarga olib keladigan maъlum vaqt tugashi bo‘yicha yoki tashqi komanda bo‘yicha ruxsat etilmagan taъsir etishlarni amalga oshirishga qodir bo‘lgan vositalarga ega bo‘lmaslik xossalarini xarakterlaydi.

Axborot xavfsizligining boshqa xarakteristikasi maъlumotlarning yaxlitligi, yaъni maъlumotlarni ruxsat etilmagan buzilishi va soxtalashtirilishini oldini olish taъminlanadigan maъlumotlarning holati hisoblanadi.

Shuningdek, foydalanuvchilarga ular uchun mo‘ljallangan maъlumotlarni to‘siqlarsiz va o‘z vaqtida olish taъminlanadigan maъlumotlarning mumkinligi – maъlumotlar va ularni tashuvchining holati ham muhim rol o‘ynaydi.

Maъlumotlarga ruxsat etilmagan shaxslarni ularga ulanishi, operatorlar, foydalanuvchilar yoki dasturlarning atayin yoki atayin bo‘lmagan xatoliklari, qurilmalarning uzilishlari tufayli aъlumotlarning noto‘g‘ri o‘zgartirilishi bu maъlumotlarning eng muhim xususiyatlarini buzilishiga olib keladi va ularni yaroqsiz va hatto xavfli qiladi. Uning ishlatilishi moddiy va maъnaviy zararga olib

kelishi mumkin, shuning uchun maъlumotlarni himoyalash tizimini yaratilishi dolzarb masala bo‘lib qoladi. Maъlumotlarning xavfsizligi deganda maъlumotlarni keraksiz oshkora qilinishidan (konfidensiallikni buzilishidan), buzilishidan (yaxlitlikni buzilishidan), yo‘qotilishidan va mumkinlik darajasini kamayishidan, shuningdek ularning noqonuniy ko‘paytirilishidan maъlumotlarning himoyalanganligi tushuniladi.

Maъlumotlarning konfidensialligi ularni ruxsat etilmagan ochilishidan himoyalashni taъminlaydi va quyidagi shakllardan tashkil topishi mumkin:

1. Bog‘lanishning konfidensialligi n-nchi bog‘lanish bo‘yicha uzatishda n-nchi foydalanuvchining barcha maъlumotlarining konfidensialligini taъminlaydi;

2. Bog‘lanishsiz konfidensiallik bog‘lanish o‘rnatilishisiz n-nchi daraja xizmatlarining bitta maъlumotlar blokida uzatiladigan n-foydalanuvchining barcha maъlumotlarining konfidensialligini taъminlaydi;

3. Tanlanma maydonlarning konfidensialligi bog‘lanish o‘rnatilishisiz n-nchi daraja xizmatlarining bitta maъlumotlar blokida yoki n-nchi bog‘lanish bo‘yicha uzatilishida n-foydalanuvchining tanlanma maydonlarining konfidensialligini taъminlaydi;

4. Maъlumotlar oqimining konfidensialligi maъlumotlar oqimini tahlil qilishda olinadigan maъlumotlarning konfidensialligini taъminlaydi;

5. Qayta tiklanishli bog‘lanishning yaxlitligi istalgan modifikatsiyalash, qo‘yilmalar, butun maъlumotlar bloklari ketma-ketligidagi istalgan maъlumotlarning yo‘qotilishi va takrorlanishlari va qayta tiklanishi imkoniyatlari aniqlanadigan n-nchi bog‘lanish bo‘yicha n-foydalanuvchining barcha maъlumotlarining 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 maъlumotlar blokida n-

foydalanuvchining maъlumotlari tanlanma maydonlarining yaxlitligini taъminlaydi;

8. Bog‘lanishsiz yaxlitlik bog‘lanishsiz n-nchi xizmatlarning bitta maъlumotlar blokining yaxlitligini taъminlaydi va modifikatsiyalash dalilini aniqlash shaklini qabul qiladi;

9. Bog‘lanishsiz tanlanma maydonlarning yaxlitligi bog‘lanishsiz uzatiladigan xizmatlarning bitta maъlumotlar blokidagi tanlanma maydonlarning yaxlitligini taъminlaydi;

10. Manba tasdiqlanadigan rad etishlarda himoyalash oluvchini jo‘natuvchining maъlumotlarni jo‘natilishi dalilini yoki ularning tarkibini xato rad etishga urnishlari qarshi himoyalaydigan maъlumotlarni kelib chiqishining zarur isbotlari bilan taъminlaydi;

11. Etkazish tasdiqlanadigan rad etishlarda himoyalash jo‘natuvchini oluvchining maъlumotlarni olinishi dalilini yoki ularning tarkibini xato rad etishga urnishlari qarshi himoyalaydigan maъlumotlarni etkazilishining zarur isbotlari bilan taъminlaydi.

Maъlumotlarni almashlash seansida himoyalashga, shu jumladan maъlumotlarning konfidensialligiga, yaxlitlik va autentifikatsiyalashga maxsus talablarning aniqlanishi himoyalash maъmuriy boshqaruvi yoki amaliy daraja maъmuriy boshqaruvi orqali amaliy daraja beradigan maъlumotlar asosida amalga oshirilishi mumkin.

Axborot xavfsizligini taъminlash bir martalik ish bo‘lmasligi 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, yaъni axborotlarni ruxsat etilmagan olinishidan himoya qilish;

– yaxlitlik, yaъni axborotlarni va resurslarni ruxsat etilmagan buzilishidan himoya qilish;

– foydalana olishlik, yaъni axborotlarni va resurslarni ruxsat etilmagan blokirovkalanishidan (to‘silishidan) himoya qilish.

Simsiz aloqa tarmoqlarining axborot xavfsizligiga tahdidlarning o‘sib 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 echilishini talab qiladigan quyidagi muammolar xarakterli hisoblanadi:

– turli simsiz aloqa tarmoqlari uchun axborot xavfsizligini taъminlashning o‘zaro muvofiqligining, shu jumladan standartlar, protokollar, axborot resurslarining mavjud emasligi;

– eъlon qilinmagan imkoniyatlarga (“qo‘yilmalar” va boshqalar) potensial bo‘lgan horijiy ishlab chiqarish texnik vositalaridan keng foydalanish;

– huquqbuzarlikning asosli bazasini yaratish uchun zarur bo‘ladigan simsiz aloqa tarmoqlarining ishlatilishini hujatlashtirilishi uslubiyatini etarli darajada ishlab chiqilmaganligi;

– simsiz aloqa tarmoqlarining umumiy foydalanishdagi telekommunikatsiya tarmoqlariga ulanishida va o‘zaro ishlashida axborot xavfsizligini taъminlash bo‘yicha kompleks echimlarning mavjud emasligi;

– eъlon qilinmagan funksiyalarni ishlatadigan va tarmoqlarning normal ishlashini buzadigan komponentlar va dasturlarning joriy etilishi imkoniyati;

– tarmoq ishlatilgan muhofaza qilish mexanizmlari tomonidan axborot xavfsizligini taъminlash jarayoniga berilgan talablarni bajarilmasligi;

– xavfsizlik talablariga muvofiq sertifikatlanmagan texnik vositalarning ishlatilishi.

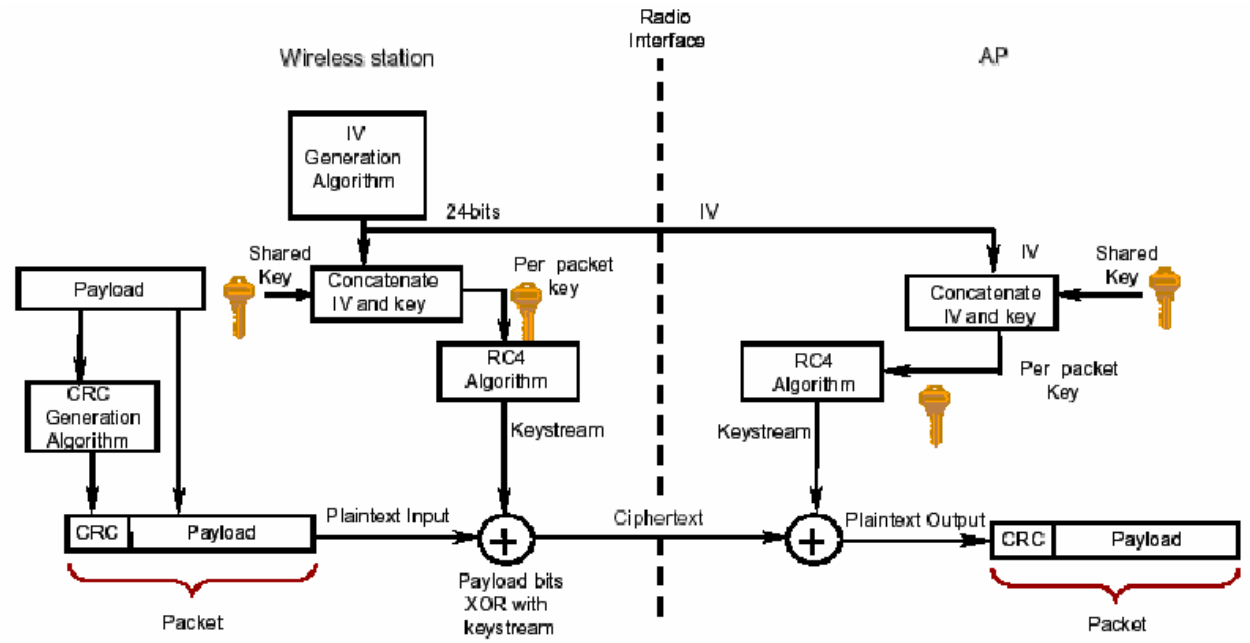
802.11 standartda maъlumotlarning *konfidensialligi*

802.11 standartda maъlumotlarning konfidensiallik radiointerfeys uchun kriptografik usuldan foydalanish orqali taъminlanadi. WEPda konfidensiallikni

taъminlanishi uchun psevdo-tasodifiy kalitli ketma-ketlikni generatsiyalaydigan simmetrik RC4 oqimli shifrlash algoritmi ishlatiladi. Bu asosiy oqim uzatiladigan maъlumotlarga oddiy 2 modul (XOR) bo‘yicha qo‘shiladi. WEP usuli bщyicha maъlumotlar radiokanal bo‘yicha uzatilishida ochilishidan himoyalanishi mumkin.WEP TCP/IP, IPX, HTTP va boshqalar trafiklarini himoyalash uchun 802.11 WLAN darjalardan yuqorida joylashgan barcha maъlumotlarga o‘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 12.1-rasmda tasvirlangan.



12.1-rasm. 802.11 standartida faqat 40-bitli kalitlarni qo‘llash agoritmi

802.11 standartda maъlumotlarning yaxlitligi

IEEE 802.11 spetsifikatsiyasi radiomijozlar va ulanish nuqtalari orasidagi uzatiladigan maъlumotlar yaxlitligini taъminlash vositalarini tavsiflaydi. Bu xavfsizlik chorasi radiokanal bo‘yicha uzatilishi vaqtida buzuvchi orqali buzilgan istalgan xabarlarni inkor qilish uchun qo‘llaniladi. Bu usul ortiqcha siklli kodlar

yordamida nazorat qilishni ishlatadi. 1-rasmda tasvirlanganidek, CRC-32 (yoki FCS kadrni tekshirish ketma-ketligi) uzatishdan oldi foydali maълumotlarning har bir kadri uchun hisoblanadi.

Bunday tarzda yig‘ilgan 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 bo‘lmasa, u holda bu yaxlitlikni buzilganligini bildiradi va paket yshqotiladi.

Konfidensiallikni taъminlash bilan holdagi kabi 802.11 standartdagi yaxlitlik kalitning uzunligiga bog‘liq bo‘lmagan holda ayrim hujumlar turlariga nisbatan zaif. WEPda yaxlitlikni taъminlash sxemasidagi fundamental kamchilik shu hisoblanadiki, oddiy CRC, masalan, xesh-funksiya kabi kriptografik xavfsiz mexanizm hisoblanmaydi.

Nazorat savollari

1. Axborot xavfsizligi sohasidagi asosiy xarakteristikalarini tushuntiring
2. Maълumotlarning konfidensialligi qanday shakllardan tashkil topgan?
3. 802.11 standartda maълumotlarning *konfidensialligi*ni tushuntiring
4. 802.11 standartda maълumotlarning yaxlitligini tushuntiring

13-ma’ruza

Boshqa keng polosali ulanish texnologiyalari: RFID, ZigBee.

Reja:

1 RFID radiochastotali identifikatsiyalash texnologiyasi

2. ZigBee texnologiyasi

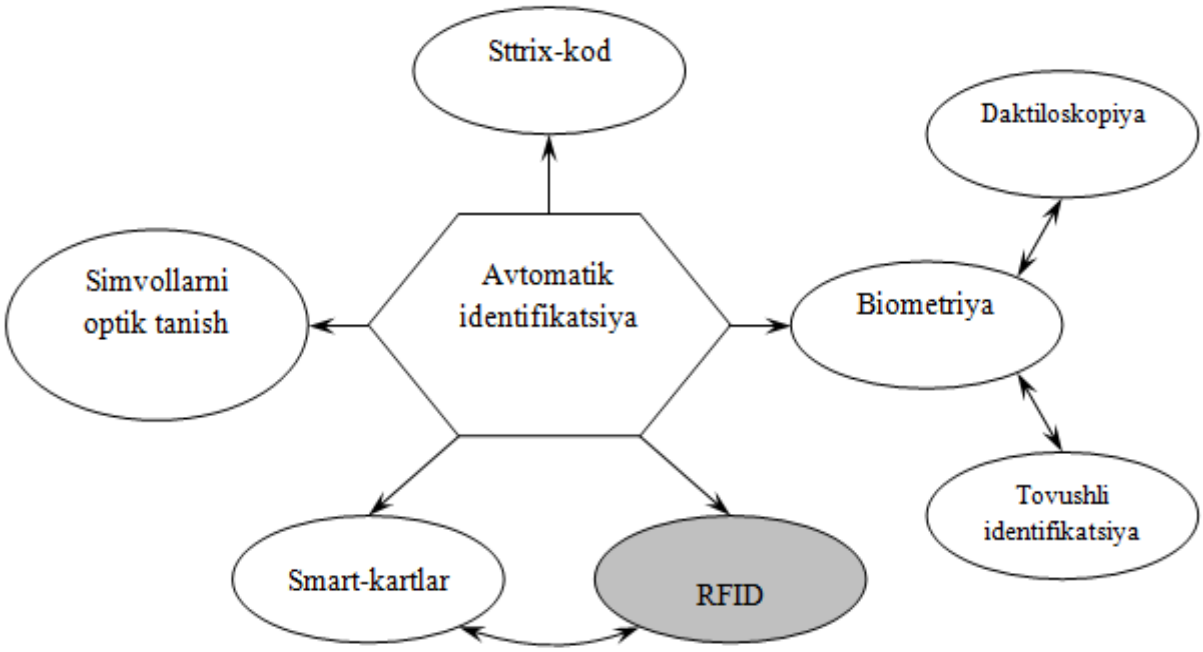
RFID radiochastotali identifikatsiyalash texnologiyasi

Radiochastotali identifikatsiyalash, bu aloqa radiochastota kanali yordamida obъektlarni avtomatik identifikatsiyalash va ro‘yxatga olish guruhiga kiradigan mustaqil yo‘nalish hisoblanadi (13.1-rasm).

RFID – bu anъanaviy belgilash tizimlariga qaraganda ko‘p ikoniyatlarni 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.

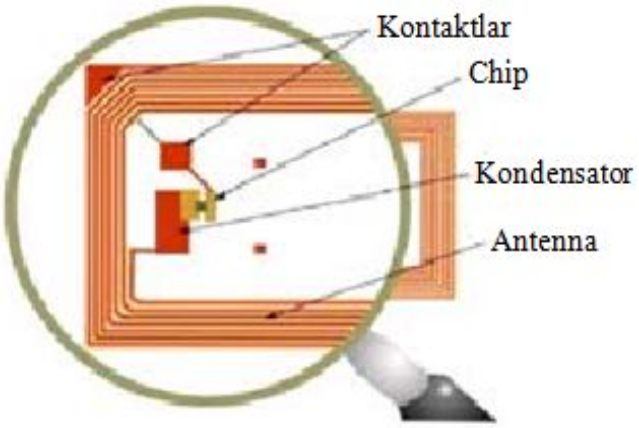
RFID tizimlari ikkita asosiy aloqa turlaridan biriga muvofiq dupleks (FDX)/yarim dupleks (HDX) yoki impulsli rejim desa ham bo‘ladigan ketma-ket tizimlar (SEQ) prinsipi bo‘yicha ishlaydi [18].



13.1-rasm. Avtomatik identifikatsiyalash texnologiyalarining bo‘linishi

Yarim dupleks va dupleks rejimlarda transponderning javobi o‘qigich qurilmaning radiochastotasi (elektr maydoni) aniqlanganida uzviladi. Binobarin, bu javob signali etarlicha kuchsiz bo‘lishi mumkin, boshqa quvvatliroq manbalardan halaqitlar fonida qabullagich-uzatkich signalini ajratishga imkon beradigan usullarga tayanish zarur. Transponderdan maъlumotlarni o‘qish qurilmasiga uzatishda yuklama modulyasiyasi degan modulyasiya amaliy ishlatiladi, unda nimtashuvchidan tashqari o‘qish qurilmasi ishchi chastotalarining ikkinchi darajali garmonikalari ishlatiladi.

Radiochastotli yorliq (13.2-rasm) qabullagich, uzatkich va maъlumotlarni saqlash uchun xotiradan iborat [23]. Radiochastotli o‘qish qurilmasi on–line rejimidan ishlaydigan qabullagich va uzatkichdan iborat. Uzatkich maъlum chastotali elektromagnit maydonni generatsiyalaydi. Bu maydon RFID yorliqlarga tushganida, u RFID dan siganlni “aniqlaydi” va undagi tovar haqida yozilgan maъlumotlarni uzatadi. Signal skanerning RFID antennasida qabul qilinadi, ishlov berish uchun kompyuterga retranslyasiya qilinadi. Tovarni radiochastotaviy identifikatsiyalash uchun to‘g‘ri ko‘rinish sharti shart emas, shuning uchun RFID yorliqlar tez va oson o‘qiladi, bu vaqtni tejashga imkon beradi.



13ю2-rasm. Radiochastotali yorliqning tashqi ko‘rinishi

Radiochastotali belgi bir yoki bir necha santimetr kvadratlarli maydonda yuzlab bayt maъlumotlardan iborat boʻlishi mumkin. RFID belgilar ham faqat maъlumotlarni oʻqish uchun, ham maъlumotlarni yozish va oʻqish uchun ishlatiladi. RFID belgilarda saqlanadigan maъlumotlar oʻzgartirilishi, toʻldirilishi va hatto boshqasi bilan almashtirilishi mumkin. RFID belgilar tovar haqida eng batafsil maъlumotlarga ega boʻlishi mumkin: davlat, ishlab chiqaruvchi, artikul, tur, rang, oʻlcham, chiqarilishi sanasi, seriya raqami va h.k.. Yana shuni taъkidlash kerakki, radiochastotali belgilar oʻgʻirliklardan himoyalash funksiyasini bajaradi va ularni buzish qiyin, deyarli mumkin emas, bu ularning oʻzoq vaqt xzmat muddatini taъminlaydi.

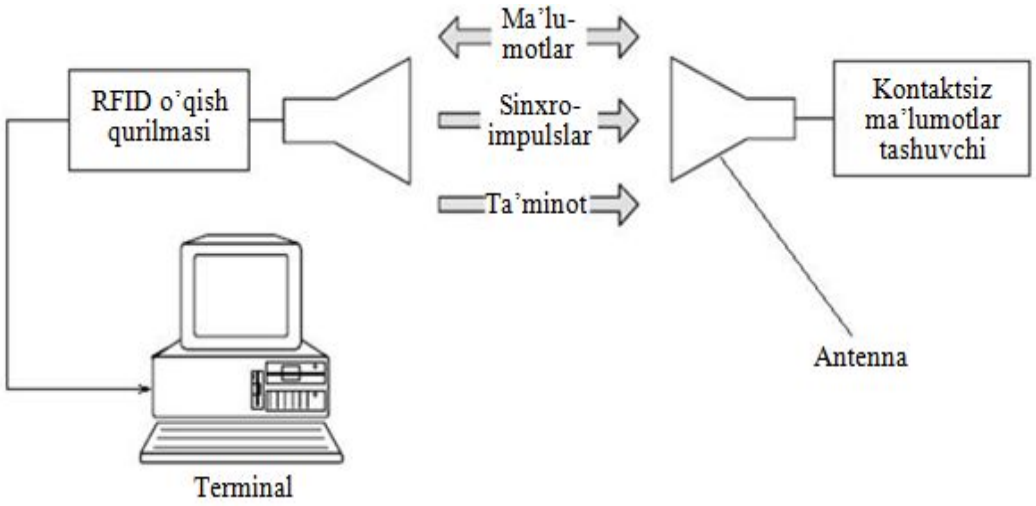
Radiochastotali identifikatsiyalash usulining oʻziga xos xususiyatlari quyidagilar:

- bu usul kontaktli hisoblanadi va toʻgʻri koʻrinishni talab qilmaydi;
- elektron belgini yashirin oʻrnatish imkoniyati;
- qiyin iqlimiy sharoitlarda va zararli muhitlarda ishlash;
- maъlumotlarni oʻqishning yuqori tezligi;
- ishlatishning cheklanmagan muddati (passiv identifikatsiyalash uchun);
- kodli maъlumotlarning katta miqdori;
- oʻqish/yozish imkoniyati.

RFID tizimlar smart-kartalar bilan yaqin bogʻlangan. Ulardagi maъlumotlar smart-kartalardagi kabi elektron tashuvchida saqlangan. Lekin, smart-kartalardan farqli ravishda RFID-belgi va oʻqish qurilmasi orasidagi maъlumotlarni almashtirish elektromagnit maydonlar yordamida va galvanik elementlar ishlatilmasdan boʻlib oʻtadi.

Antenna RFID-belgi belgini aktivlashtiradigan va bu belgiga maъlumotlarni yozish va oʻqishga imkon beradigan elektromagnit toʻlqinlarni nurlantiradi. Antenna belgi va qabullagich-uzatkich orasidagi oʻziga xos kanal hisoblanadi, u butun maъlumotlarni uzatish va olish jarayonlarini nazorat qiladi. Antennalar oʻlchamlari va shakllari boʻyia farq qiladi. Ular antennaning taъsir etish zonasidan

o‘tadigan prdmetlar yoki odamlardan maъlumotlarni 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 demodulyasiyalanadi, rasshifrovka qilinadi va keyingi ishlov berish uchun kompyuterga uzatiladi (3-rasm).



13.3-rasm. RFID tizimning asosiy komponentlari

Ma’lumotlarni to‘plash va boshqarish tizimlarida ishlatish uchun mo‘ljallangan simsiz texnologiya hisoblanadi. U past energiya iste’moliga, ma’lumotlarni uzatish ishonchliligiga va ma’lumotlarni himoyalanishiga 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.

ZigBee texnologiyasi

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 – modulyasiyalash turi (BPSK va O-QFSK), chastotalar diapazonlari va ularga mos uzatish tezliklari tavsifiga ega. ZigBee spetsifikatsiyasi 10 dan 75 metrlargcha 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 standariga uchta 2,4 GGs (16 ta kanallar), 915 MGs (10 ta kanallar) va 868 MGs (1 ta kanal) chastotalar diapzonlaridagi 27 ta kanallar biriktirilgan. Bu efir dipazonlari uchun maksimal ma’lumotlarni uzatish tezliklari mos ravishda 250 kbit/s, 40 kbit/s va 20 kbit/slarni 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) tegishliligini aniqlash uchun qo‘shimcha 16-bitli tarmoq manzilini (PAN-ID) bo‘lishini ko‘zda tutadi.

ZigBeening o‘ziga xos xususiyati shundan iboratki, u nafaqat oddiy “nuqta-nuqta” yoki “yulduz” bog‘lanishlari, balki retranslyasiya qilish va ma’lumotlarni uzatish samarali marshrutini qidirishni qo‘llay oladigan “daraxt” va “yacheykali tarmoq” topologiyalarili murakkab tarmoqlar uchun mo‘ljallangan. ZigBee tarmoqlari o‘z-o‘zidan tashkil bo‘ladigan va o‘z-o‘zidan tiklanadigan tarmoqlar hisoblanadi. O‘rnatilgan dasturiy ta’minot tufayli ularning qurilmalari ta’minot yoqilganida o‘zlari bir-birlarini topishni biladi. Qandaydir qurilma ishdan chiqqanida ular xabarlarni uzatish uchun yangi marshrutlarni qidira oladi.

ZigBee tarmoqlari uchta asosiy turlardagi tugunlar - koordinatorlar, marshrutizatorlar va oxirgi qurilmalarga ega. Koordinator majburiy qurilma bo‘lib, u tarmoqni hosil qiladi, tarmoq uchun chastotalar kanali nomerini va identifikatorni tanlaydi. Keyin unga marshrutizatorlar va oxirgi qurilmalar ulanadi, ularning sonini oshirish mumkin.

Texnologiyaning avzalliklari shu hisoblanadiki, ZigBee-qurilmalar 70-80 metrlardan ortiq masofalarga zatishni ta’minlay olmasada, ular trafik uchun tennel sifatida Wi-Fi va Bluetooth qurilmalari kanallarini (agar ular ko‘rinish zonasida bo‘lsa) ishlatishi mumkin. Energiya iste’moliga kelganda, bitta uncha katta bo‘lmagan batareya nazariy jihatdan ZigBee-qurilmaning ishlash qobiliyatini saqlash uchun bir necha oylar va hatto yil davomida etishi kerak. Standartning boshqa avzalliklari orasidan yaxshi mastablanuvchanlikni, uzilishlar hollarida o‘zi tiklanishi imkoniyati va sozlashning oddiyligini aytib o‘tish kerak. 64-bitli manzillashtirish qo‘llanilganida yagona tarmoqqa 60 mingtadan ortiq ZigBee-qurilmalarni birlashtirish mumkin.

Past o‘tkazish qobiliyati va kichik ishlash radiusi ZigBee tarmoqlarni multimediali ma’lumotlarni (oqimli video yoki audio) translyasiyalash uchun yoki olisdagi ofislarning o‘zaro aloqasi uchun qo‘llanilishiga imkon bermaydi. Buning uchun ma’lumotlarning simsiz keng polosali uzatish WiMAX texnologiyasi mavjud. ZigBee-qurilmalarni asosiy qo‘llanilishi sohasi monitoring, xavfsizlik, tibbiyot apparaturalari holatini nazorat qilish tizimlari va boshqalar hisoblanadi. ZigBee kontrollerlarili xabarlagichlar yirik tashkilotlarda texnik qo‘llab-quvvatlash

xizmatlarining ishini soddalashtirishi mumkin. Bu holda shtatdan tashqari vaziyat yuz berganida muhandislarga yaroqsizlikning sababini aniqlash uchun sensorlarni, masalan, noutbuk yoki cho‘ntak kompyuteri yordamida tekshirishni tez amalga oshirish etarli bo‘ladi. Spu bilan birga simsiz aloqa va avtonom ta’minot manbalarini qo‘llanilishi qo‘riqlash tizimlari va monitoring qilish komplekslarining ishonchliligini oshiradi, chunki jinoyatchi bitta kuch kabelini uzish bilan butun simsiz aloqa tarmog‘ini ishdan chiqara olmaydi.

Shuningdek, ZigBee aloqa “raqamli uyning” ajralmas qismi bo‘lishi ko‘zda tutilmoqda. Binobarin, ZigBee kontrollerlarini nafaqat xavfsizlik va signalizatsiya tizimlari xabarlagichlari, balki maishiy texnika, shu jumladan konditsionerlar, videomagnitofonlar, televizorlar va hatto oddiy yoritish o‘chirgichlari oladi. Bu unifikatsiyalangan masofadan boshqarish pulti yoki mobil telefon yordamida barcha asboblarning ishlashini nazorat qilishga imkon beradi.

Bundan tashqari, ZigBee-kontrollerlar aloqa kanallarining o‘tkazish qobiliyatlariga yuqori talablarni qo‘ymaydigan turli kompyuter qurilmalariga o‘rnatilishi mumkin. Ular, masalan, joystiklar, sichqonchalar va boshqalar bo‘lishi mumkin. Tibbiyot sohasida ZigBee simsiz aloqa operatsiyalarni o‘tkazgan bemorlar yoki og‘ir ahvolda bo‘lgan insonlar holatini kuzatib borishga yordam beradi. Simli xabarlagichlar o‘rniga bemorlarning qo‘llariga bosim, harorat, yurak qisqarishlari chastotalari sensorlarili elektron braslet taqilishi va kerakli davriylikda olinadigan ko‘rsatishlar markaziy serverga tashlanishi mumkin, u xavf tug‘ilganida palata va joy nomeri ko‘rsatiladigan trevoga signalini berishi mumkin.

Tabiiyki, ZigBee-qurilmalar uchun boshqa ko‘plab qo‘llanilish sohalari ham topiladi. Istiqbolda ZigBee simsiz tarmoqlari Bluetooth texnologiyasiga jiddiy raqobatni hosil qilishi kerak. 13.1-jadvalda ZigBee aloqaning asosiy texnik parametrlari keltirilgan.

13.1-jadval

ZigBee aloqaning asosiy texnik parametrlari

Xususiyatlari/Funksiya	Xarakteristika
Aloqa turi	Radioto‘lqinlar
Chastotalar dipazoni	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)

Nazorat savollari

1. Avtomatik identifikatsiyalash texnologiyalarining bo‘linishini tushuntiring.

2. RFID tizimning asosiy komponentlarini tushuntiring.

3. ZigBeening o‘ziga xos xususiyatini tushuntiring.

4. ZigBee aloqaning asosiy texnik parametrlarini tushuntiring.

14-ma’ruza

Boshqa keng polosali ulanish texnologiyalari: Bluetooth, NFC.

Reja:

1 Bluetooth texnologiyasi

2. NFC texnologiyasi

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 (14.1-rasm).

Mavjud qurilmalar uchun standart Bluetooth-bog‘lanish profillarini ishlatadigan uncha qimmat bo‘lmagan o‘rnatiladigan 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 qo‘llaniladi. Ma’lumotlarni to‘plash va boshqarish tizimlarida ko‘pincha SPP ketma-ket porti profili ishlatiladi.

14.1-rasm. Bluetooth tizimi

Bluetooth protokoli nuqta-nuqta va nuqta-ko‘p nuqta topologiyalarini qo‘llaydi. Ikki yoki undan ortiq o‘sha bir kanalni ishlatadigan qurilmalar

pikotarmoqni (piconet) tashkio etadi. Bunda qurilmalardan biri asosiy (Master) sifatda, qoganlari esa bo‘ysunuvchi (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.

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).

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.

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 asinxron 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 bog‘lanishda qurilmalardan biri etakchi (master). Boshqasi esa etaklanuvchi (slave) hisoblanadi. Kompyuter tomonida master joylashadi. SHuning uchun o‘rnatiladigan tizimlar uchun ko‘pincha etaklanadigan sifatda konfiguratsiyalangan Bluetooth-modullar ishlatiladi.

Ketma-ket port profili Bluetooth qurilmalari bilan quyidagi operatsiyalarning bajarilishini ko‘zda tutadi.

- Bluetooth-qurilmalarni topish;
- ikkita Bluetooth-qurilmalarning bog‘lanishini o‘rnatish;
- “ochiq” kanal rejimida ma’lumotlarni uzatish.

Etaklanadigan Bluetooth modul ta’minot yoqilganida topish uchun mumkin” holatda bo‘ladi. Etakchi Bluetooth modul ta’minot yoqilganida etaklanadigan qurilmalarni qidirishni boshlaydi va bo‘sh etaklanadigan qurilma topilganida unga ulanishga urinadi. Etaklanadigan qurilma PIN-kodni so‘raydi, etakchi qurilma javob beradi. Agar PIN-kodlar mos tushsa, u holda qurilmalar o‘z manzillari bilan almashadi, juftlikni tashkil etadi va ma’lumotlarni almashlashni bajarishi mumkin. SHunday qilib, bog‘lanishni o‘rnatilishi avtomatik bo‘lib o‘tadi.

Etaklanadigan va etakchi qurilmalar olisdagi modulb so‘rovlarga javob bermaganida vaziyatni turlicha qayta ishlaydi. Etaklanadigan qurilma bu holda bog‘lanish yo‘qotilgan hisoblaydi va yana topish uchun mumkin bo‘ladi. Etakchi Bluetooth modul oldin o‘rnatilgan bog‘lanishga qoladigan bo‘lib qoladi. U oldingi hamkorini unutishi uchun unga tashqi chiqishga bekor qilishi impulsini berish kerak.

Bluetooth texnologiyasi Bluetooth Special Interest Group (SIG) tijorat uyushmasi tomonidan qo‘llab-quvvatlanadi va rivojlantiriladi. U Bluetooth spetsifikatsiyalarini e’lon qiladi, qurilmalarning sertifikatlashtirilishini tashkil etadi, Bluetooth savdo belgisini himoya qiladi va texnologiyani targ‘ib qiladi.

Quyidagi spetsifikatsiyalar mavjud:

● 2.0 + EDR (Enhanced Data Rate) versiya spetsifikatsiyasi bugungi kunda eng keng tarqalgan va ishlatiladigan spetsifikatsiya hisoblanadi. Bu spetsifikatsiya oldingi versiyalarga qaraganda uzatiladigan ma’lumotlar tezligini oshirishga va energiya iste’molini qisqartirishga imkon berdi, ikkita qurilmalar orasida aloqani o‘rnatilishi protsedurasini soddalashtirdi;

● Bluetooth 2.1 spetsifikatsiyasida qurilmalarning xarakteristikalarini kengaytirilgan so‘rovi texnologiyasi (uyg‘unlashtirishda ro‘yxatni qo‘shimcha filtrlash uchun), shuningdek bitta akkumulyator zaryadlanishidan qurilmalarning ishlash davomiyliklarini 3-10 martta oshirishga imkon beradigan energiyani tejash Sniff Subrating texnologiyasi qo‘shilgan. Bundan tashqari, YAngilangan spetsifikatsiya ikkita qurilmalar orasida bog‘lanishni o‘rnatilishini sezilarli soddalashtiradi va tezlashtiradi, bog‘lanish uzilmasdan shifrlash kalitlarini

yangilanishini amalga oshirishga imkon beradi, shuningdek ko‘rsatilgan bog‘lanishlarni Near Field Communication texnologiyasidan foydalanish tufayli himoyalanganroq qiladi;

● 3.0 High Speed (HS) versiyadagi Bluetooth spetsifikatsiyasi Bluetooth SIG kompaniyalar guruhi tomonidan 2009 yilning aprelida tasdiqlangan.

Yangi spetsifikatsiya hozirda ma’lum Wi-Fi texnologiya orqali ishlatiladigan IEEE 802.15.11 standartni simsiz ma’lumotlarni uzatish fizik darajasi sifatida ishlatilishiga ko‘rsatma beradi. Bu tanish va ishlatishda oddiy bo‘lgan interfeys Bluetooth klassik interfeysini yuqoriroq ma’lumtlarni uzatish tezliklarida ishlatilishiga imkon beradi. 3.0 (HS) spetsifikatsiyaning ikkinchi o‘ziga xos xususiyati energiya iste’molini qat’iy nazorat qilishni kiritilishi hisoblanadi, bu olib yuriladigan apparaturalar uchun juda muhim hisoblanadi.

Bluetooth texnologiyasi rivojlanishda davom etmoqda. Bataraeyalardan bir necha yillar ishlay oladigan ultra past energiya iste’molili Bluetooth qurilmalarini ishlab chiqishga imkon beradigan "Bluetooth Low Energy" spetsifikatsiyaning tasdiqlanishi kutilmoqda.

Sanab o‘tiganlardan tashqari, Bluetooth SIG ishchi guruhi ko‘plab boshqa standart profillarni aniqladi:

• Generic Access Profile (umumiy foydalanishdagi profil) – qurilmalar orasidagi aloqani ta’minlash, 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 emulyasiyalashga 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" sifatidaishlatilishiga

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 emulyasiyalashga 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

Xulosada ta’kidlash kerakki, Bluetooth texnologiyasiga juda katta qiziqish nomoyon 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 ho‘jaliklari va boshqa sohalar eng istiqbolli hisoblanadi.

NFC

Bu kichik masofalarga ma’lumotlarni simsiz uzatish texnologiyasi hisoblanadi. Uzatish modeli elektromagnit maydonni hosil qiladigan qurilma-

initsiator va qurilma-nishonni o‘z ichiga oladi. Qurilma-nishon ham aktiv (masalan, boshqa mobil aloqa qurilmasi yoki to‘lov terminali), ham passiv (RFID radio-belgi, kontaktsiz karta yoki jevakcha) bo‘lishi mumkin. Radio-belgilar va kontaktsiz kartalarning mavjud formatlari qo‘llanadi.

Passiv nishon bilan ishlashda qurilma-initsiator uzluksiz nurlantiradi, qurilma-nishon esa faqat bunday tarzda hosil qilingan elektromagnit maydonni modulyasiyalaydi. Passiv qurilma-nishonni, shunday tarzda, qabullagich-uzatkich (transponder) sifatida ko‘rish mumkin. Aktiv nishon bilan ishlashda qurilmalar o‘z nurlanishini javobni kutish vaqtiga uzish bilan uzatish tartibini navbatlashtiradi.

Simsiz kartali tizimlarda ishlashga o‘xshash NFC texnologiyasi asosidagi tizimlarda aloqa bir-birlarining yaqin maydonlari chegaralarida bo‘lgan ikkita ramkali antennalar orasida o‘rnatiladi. Aloqa umumiy mumkin va litsenziyalanmaydigan ISM Band (Industrial, Scientific and Medical radio Band, Sanoat, Ilmiy va Tibbiyot radiochastotalari) radiochastotalar chegaralarida 13,56 MGs tashuvchi chastotada bo‘lib o‘tadi. Axborot signali energiyasining katta qismi 14 kGsdagi chastotalar polosasida bo‘ladi, lekin amplitudaviy modulyasiyalash ishlatilganida polosaning to‘liq kengligi 1, 8 MGsga etishi mumkin.

Standart ixcham antennalarda maksimal bo‘lishi mumkin ma’lumotlarni uzatilishi masofasi 10 smni tashkil etadi.

NFC texnologiyasi orqali signalni ikkita kodlash turi ishlatiladi.

Ulardan birinchisida aktiv qurilma ikkilik ma’lumotlarni 100% amplitudaviy modulyasiyali ikki darajali kodlash (shuningdek inglizcha adabiyotlarda Miller kodlashi deyiladi) ishlatiladi. Bunday rejimda uzatish tezligi 106 Kbit/sni tashkil etadi.

Ikkinchisida, aktiv qurilma 10% amplitudaviy modulyasiyali nolinchi sathga qaytishsiz kod (manchester kodi deyiladigan) ishlatiladi. Bunday rejimda malumotlarni uzatish tezligi 212 yoki 424 Kbit/sni tashkil etishi mumkin.

Passiv qurilma har doim 10% amplitudaviy modulyasiyali manchester kodini ishlatadi.

Binobarin, NFC qo‘llanadigan qurilmalar bir vaqtda ma’lumotlarni uzatishi va qabul qilishi mumkin, ularga koliziyalarni aniqlash kerak bo‘ladi. Kolliziyalarni aniqlash uzatilgan va olingan signallarning chastotalarini taqqoslashga asoslangan va ular mos tushganida olingan signal yaroqsizga chiqariladi.

NFC texnologiyasi ma’lumotlarni kriptografik himoyalashga standartlarni o‘z ichiga oladi va u yuqori darajalar protokollari orqali ta’minlanishi ko‘zda tutiladi.

NFC texnologiyasi mobil aloqa qurilmalarida qo‘llaniladi. Uchta asosiy ishlatish usullari amalga oshiriladi:

Kartani emulyasiyalash: NFC qo‘llanadigan qurilma simsiz kartani emulyasiyalash uchun ishlatiladi.

O‘qigich rejimi: NFC qo‘llanadigan qurilma aktiv rejimda ishlaydi va passiv qurilmalardan, masalan radio-belgidan ma’lumotlarni o‘qiydi.

Nuqta-nuqta rejimi: NFC qo‘llanadigan ikkita qurilma aktiv rejimda ishlaydi va o‘zaro ma’lumotlarni almashlash uchun texnologiyani ishlatadi.

Tavsiflangan rejimlar uchun jamoat transportida yo‘l haqini mobil to‘lovi, NFC qo‘llanadigan mobil qurilmalardan kredit/debet karta sifatida, reklama oynalaridan radiobelgilardan qo‘shimcha ma’lumotlarni o‘qish uchun foydalanish kabi ko‘plab qo‘llanishlar bo‘lishi mumkin.

NFC texnologiyasidan foydalanish bilan Bluetooth 2. 1 yoki Wi-fi kabi boshqa simsiz aloqa texnologiyalaridan foydalaniladigan o‘zaro ta’sirlashishni oddiy va tez sozlash mumkin. NFC texnologiyasini poezd, samolyot, konserlar va boshqalarga chiptalarni elektron bron qilish uchun, “elektron pullar” bilan hisoblashish uchun, sayohatchi xaritasi, shaxsni tasdiqlash guvohnomasi, xavfsizlik tizimlarida kontaktsiz kartalar sifatida (shu jumladan mehmonxanalar nomerlari, avtomobillar, maishiy qulflar kalitlari o‘rniga) qo‘llash mumkin. NFC qo‘llanadigan qurilmalarni birja savdosi, kontentni sotib olish, dasturiy arzonlashtirishlar va bonuslar va boshqalar uchun ishlatish mumkin.

NFC texnologiyasining afzalliklari bog‘lanishni o‘rnatilishining yuqori tezligi, past energiya iste’moli va sozlashning oddiyligi hisoblanadi.

Hisoblashlarda NFCning o‘ziga xos qo‘llanilishlari uchun muhim avzalligi himoyalanganlik va ko‘p sonli odamlar bo‘ladigan savdo markazlarida ishlatilishi oddiyligini ta’minlaydigan uncha katta bo‘lmagan ishlash masofasi ham hisoblanadi.

Bundan tashqari, NFC texnologiyasining avzalligi mavjud radiobelgilar standartlarini (RFID) qo‘llanilishini ta’minlash hisoblanadi. Lekin tez-tez passiv qurilmalar bilan o‘zaro ta’sirlashishda (xuddi RFID yoki o‘chirilgan telefonlar) NFC-chiplarning energiya iste’moli sezilarli ortadi.

Bluetooth yoki Bluetooth Low Energy kabi boshqa zamonaviy ma’lumotlarni simsiz uzatish texnologiyalariga qaraganda NFC ma’lumotlarni uzatish tezligi bo‘yicha sezilarli yutqazadi. Bundan tashqari, kichik ishlash masofasi ham aynan NFC aktiv qurilmalar orasida ma’lumotlarni uzatilish uchun ishlatilishidaga kamchilik sifatida qaralishi mumkin.

Elektron hisoblashlar nuqtaini nazaridan NFCning kamchiligi o‘rnatilgan kriptografiy ma’lumotlarni himoyalashni yo‘qligi hisoblanadi. Bu kamchilik, ammo ishlatiladigan kodlash usullari orqali qisman kompensatsiyalanadi, REB vositalari orqali ma’lumotlarni buzilishidan himoyalashni kafolatlamasada, uzatiladigan ma’lumotlarni rusat etilmagan modifikatsiyalanishidan himoyalaydi.

Hamma joylarda texnologiyani joriy etish hali bo‘lib o‘tmadi, mobil aloqa operatorlari va boshqa mobil echimlar bozori o‘yinchilari faqat NFC asosidagi o‘z tijorat echimlarini testlamoqda. Lekin barcha sanab o‘tilgan sohalarda NFCning joriy etilishi savdoda, xavfsizlik tizimlari va reklamada sezilarli o‘zgarishlarni bildirishi mumkin. Uncha katta bo‘lmagan xaridlarga to‘lovlarni soddalashtirish va tezlashtirish, xarid-sotish jarayonidan fizik pullarni chiqarilishi, ayniqsa tijort banklarining mumkin kredit siyosati bilan birgalikda fizik shaxslar pul aylanmalari vositalari tezligini sezilarli oshirilishini bildiridi, bu o‘z navbatida, iqtisodiy o‘sish uchun sezilarli potensialni bildiradi.

Nazorat savollari

1. Bluetooth texnologiyasining xususiyatlarini tushuntiring.
2. Bluetooth texnologiyasi afzalliklarini tushuntiring.

3. NFC texnologiyasining xususiyatlarini tushuntiring.
4. NFC texnologiyasining afzalliklarini tushuntiring.

15-ma’ruza

Antennalar.

Reja:

1. Antennani aniqlash
2. Radiosignalning tarqalishi

Antennalarni to‘g‘ri o‘rnatish va sozlash ma’lum bilimlarni talab qiladi. Yo‘naltirilganlik diagrammalari va antennalarning polyarizatsiyasi haqida tushunchalarga ega bo‘lish zarur. Boshlang‘ich bosqichda kuchaytirish koeffisientini to‘g‘ri hisoblash xatoliklardan va ishlatishda antennalarning noto‘g‘ri ishlatilishidan qochishga imkon beradi. shuningdek, signalni uzatilishida unga salbiy ta’sir qiladigan turli buzilishlar turlarini hisobga olish zarur bo‘ladi.

Antennani aniqlash

Antennani bo‘shliqdan elektromagnit energiyani nurlantirish yoki tutish uchun ishlatiladigan o‘tkazgich sifatida aniqlash mumkin. Signalni uzatish uchun uzatkichning radiochastotaviy elektr impulslari antenna yordamida atrof-muhitga nurlantiriladigan elektromagnit energiyaga o‘zgartiriladi. Signalni olishda antennaga keladigan elektromagnit to‘lqinlar energiyasi radiochastotaviy elektr impulslarga o‘zgartiriladi va qabullagichga beriladi.

Ikki tomonlama aloqada o‘sha bir antenna signalni ham qabul qilish, ham uzatish uchun ishlatiladi. Bunday yondashish mumkin, chunki istalgan antenna teng samaradorlikda energiyani atrof-muhitdan qabul qiluvchi terminallarga va uzatuvchi terminallardan atrof-muhitga yetkazib beradi.

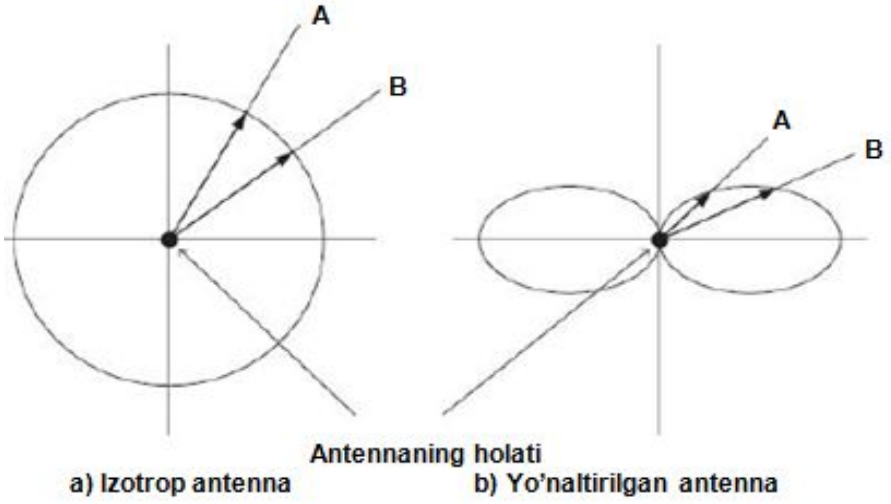
Antennani to‘g‘ri sozlash uchun uning bir necha xarakteristikalarini ko‘rib chiqamiz.

Yo‘naltirilganlik diagrammasi

Antennalar energiyani barcha yo‘nalishlarda nurlantiradi. Lekin, ko‘p hollarda turli yo‘nalishlar uchun signalning uzatilishi samaradorligi bir xil emas. Antennaning samaradorligini aniqlashning eng keng tarqalgan usuli *yo‘naltirilganlik diagrammasi* hisoblanadi, u fazoviy koordinatalarga antennaning nurlantirish xususiyatlarining bog‘liqligidan iborat. Antennaning yo‘naltirilganlik

diagrammasi uch o‘lchamli diagrammaning ikki o‘lchamli kesimi sifatida tushuniladi.

Yo‘naltirilganlik diagrammasining eng oddiy turlaridan biri izotrop antenna deyiladigan ideal holatga mos keladi. *Izotrop antenna* deganda barcha yo‘nalishlarda energiyani bir xil nurlantiradigan nuqta tushuniladi. Izotrop antenna uchun yo‘naltirilganlik diagrammasi antennaning holati bilan mos tushadigan sferadan iborat (15.1a-rasm). Antennadan yo‘naltirilganlik diagrammasining istalgan nuqtasigacha masofa bu yo‘nalishda antenna nurlantiradigan energiyaga to‘g‘ri proporsional bo‘ladi. 15.1b-rasmda yana bir ideallashtirilgan holat bo‘lgan bir ajratilgan yo‘nalishli nurlantirishli yo‘naltirilgan (gorizontal o‘q bo‘ylab) antenna keltirilgan.



15.1-rasm. Yo‘naltirilganlik diagrammalari

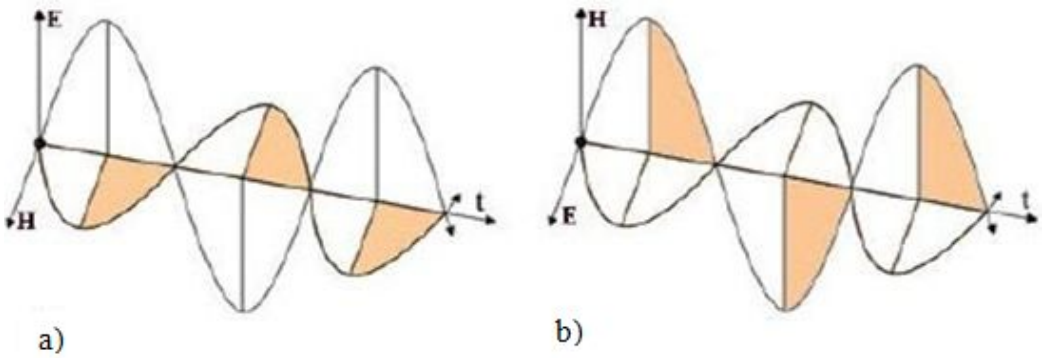
Diagrammaning o‘lchami ixtiyoriy bo‘lishi mumkin. Har bir yo‘nalishda proporsiyaga rioya qilish muhim. Nisbiy masofa asosida berilgan yo‘nalishdagi keltirilgan quvvatni aniqlash uchun antennaning joylashtirilgan nuqtadan yo‘naltirilganlik diagrammasi bilan kesishgan joyga mos og‘ish bo‘rchagi ostida to‘g‘ri chiziq o‘tkaziladi. 1b-rasmda ikki antennalar uchun ikkita signalni uzatish burchaklari (A va B) taqqoslangan. Izotrop antennaga yo‘naltirilmagan doiraviy diagramma mos keladi. A va B vektorlar kattaligi bo‘yicha teng bo‘ladi.

Antennalarning polyarizatsiyasi

Antennaning muhim xarakteristikasi uning *polyarizatsiyasi* hisoblanadi. Radioulanish tizimlarida vertikal, gorizontal va doiraviy (chap va o‘ng aylanishli) polyarizatsiyali antennalar ishlatiladi (15.2-rasm).

Polyarizatsiyani hisobga olish elektromagnit moslashuvchanlik masalalarini yechishda, xizmat ko‘rsatish zonalarini rejalashtirishda va boshqalarda qo‘shimcha energetik avzalliklarni olishga imkon beradi. Ma’lum bo‘shliqni chegaraviy darajagacha ulanish nuqtalari bilan to‘ldirishdan keyin o‘zaro radiohalaqitlar tarmoqlarning normal ishlashiga halaqit bera boshlaydi, bunda antennalarning polyarizatsiyasini o‘zgartirish yetarli bo‘ladi, bundan keyin radiotarmoqni rivojlantirishni davom ettirish mumkin.

Tekis elektromagnit to‘lqinda vertikal elektr Ye va magnit N vektorlar har bir vaqt momentida bo‘shliqda ma’lum tarzda joylashadi. Elektromagnit maydon polyarizatsiyasi uning fazoviy-vaqt xarakteristikasi hisoblanadi va fazoning qayd etilgan nuqtasida elektr maydon vektorining uchi bilan tavsiflanadigan traektoriyasi ko‘rinishida aniqlanadi. Polyarizatsiyali antennalarda orqa tomonida mil (strelka) ko‘rinishidagi ko‘rsatkich mavjud bo‘lib, u zarur polyarizatsiyani aniqlaydi.



15.2-rasm. Vertikal (a) va gorizontal (b) polyarizatsiya

Doiraviy yoki siklik polyarizatsiyada elektromagnit maydon X o‘qi atrofida ma’lum sikl yoki qadam bilan fazoning turli nuqtalarida vertikal yoki gorizontal polyarizatsiyani qabul qilib aylanadi. Bunday polyarizatsiya turi nisbatan kam qo‘laniladi.

Antennalarning kuchaytirish koeffisientlari

Kuchaytirish koeffisienti antennaning yo‘naltirilganligi o‘lchami hisoblanadi. Bu parametr ma’lum yo‘nalishda nurlantirilgan signal quvvatini ideal yo‘naltirilmagan antenna istalgan yo‘nalishda nurlantiradigan signal quvvatiga nisbati sifatida aniqlanadi.

Antennaning kuchaytirish koeffisienti dipol antennaga nisbatan dB da, izotrop antennaga nisbatan esa dBu da beriladi.

Birinchi marta ishlatilgan signal intensivligini o‘lchashlar uchun desibel o‘lchov birligi Aleksandr Grem Bell sharafiga atalgan. Desibellardagi qiymatlar logarifmik shkala bo‘yicha hisoblanadi, bu kengkuchlanishlar va toklar diapazonlarida xarakteristikalarning o‘ziga xosligini ta’minlashga imkon beradi.

$$B=bel=\log_{10}[P_1/P_2]=2\log_{10}[V_1/V_2]$$

$$dB=desibel=10\log_{10}[P_1/P_2]=20\log_{10}[V_1/V_2]$$

bu yerda P_1-o‘lchangan quvvat, Vt; P_2-etalon quvvat, Vt; V_1-o‘lchangan kuchlanish, V; V_2-etalon kuchlanish, V.

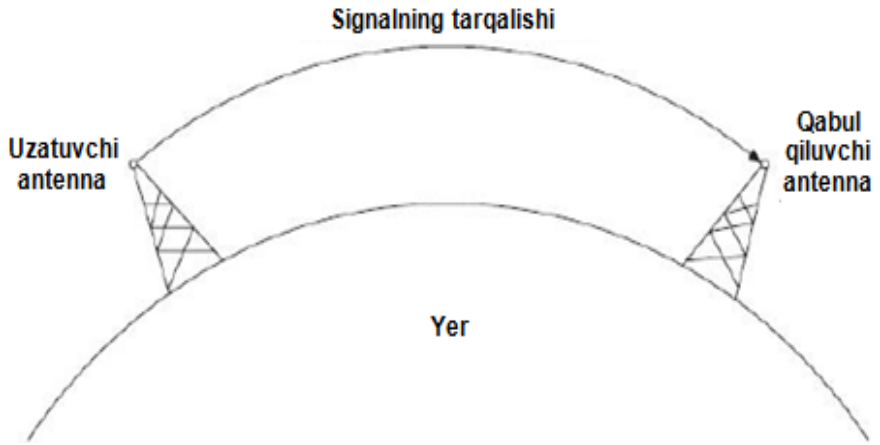
Signalning tarqalishi

Antennadan nurlantirilgan signal tarqalishida Yerning sirtida og‘ishi, yuqori atmosfera qatlamlaridan qaytishi yoki to‘g‘ri ko‘rinish liniyasi bo‘ylab tarqalishi mumkin.

Elektromagnit to‘lqinlar difraksiyasi

Signalning tarqalishi yo‘li Yer sirtida og‘ishida u yoki bu darajada planetaning shaklini takrorlaydi (15.3-rasm). Uzatish to‘g‘ri ko‘rinish chegaralaridan ancha ortadigan sezilarli masofalarga amalga oshirilishi mumkin. Bu samara 2 MGs gacha chastotalar uchun o‘z o‘rniga ega. Bu chastotalar polosasiga tegishli bo‘lgan signallarning yer sirtining egriligini takrorlashi qobiliyatiga elektromagnit to‘lqinlar difraksiyasi omili ta’sir qiladi. Bu hodisa to‘siqlar bo‘lganida elektromagnit to‘lqinlarning o‘zini tutishiga bog‘liq.

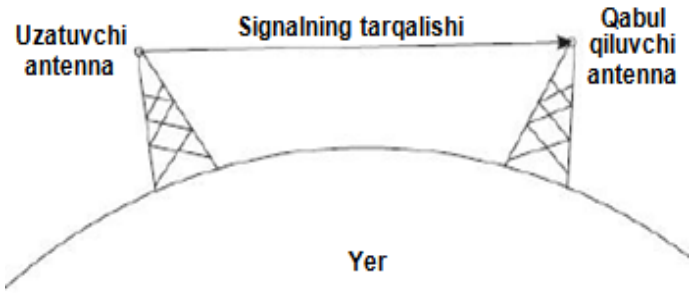
Ko‘rsatilgan diapazondagi elektromagnit to‘lqinlarning atmosferada tarqalishi shunday amalga oshadiki, yuqori atmosfera qatlamlariga bu to‘lqinlar yetib bormaydi.



15.3-rasm. Yer atrofi to‘lqinlarining tarqalishi (2 MGs chastotagacha)

To‘g‘ri ko‘rinish liniyasi bo‘ylab to‘lqinlarning tarqalishi

Agar radiosignal chastotasi 30 MGsdan ortsa, u holda ularning yer sirtida og‘ishi va atmosferaning yuqori qatlamlaridan qaytishi mumkin bo‘lmaydi. Bu holda aloqa to‘g‘ri ko‘rinish chegaralarida amalga oshirilishi kerak (15.4-rasm).



15.4-rasm. Ko‘rinish liniyasi bo‘ylab to‘lqinlarining tarqalishi (30 MGs dan yuqori chastotalarda)

Nazorat savollari

1. Yo‘naltirilganlik diagrammasi nitushuntiring
2. Antennalarning polyarizatsiyasini tushuntiring
3. Antennalarning kuchaytirish koeffisientlarini tushuntiring
4. To‘g‘ri ko‘rinish liniyasi bo‘ylab to‘lqinlarning tarqalishini tushuntiring

16-ma’ruza

Raqamli aloqa tizimlaridagi “signal-shovqin” nisbati

Reja:

1. Raqamli aloqa tizimlaridagi “signal-shovqin” nisbati
2. Frenel zonasini hisoblash

Simsiz aloqa kanali ishlash uzoqlik masofasini hisoblash

Bo‘sh fazoda uzoqlik masofasini hisoblash formulasini keltiramiz:

$$FSL=33+20(lgF+lgD)$$

FSL (Free Space Loss)-bo‘sh fazodagi yo‘qotishlar, dB; F-aloqa tizimi ishlaydigan kanalning markaziy chastotasi, MGs; D-ikki nuqta orasidagi masofa, km.

FSLtizimning yig‘indi kuchaytirishi orqali aniqlanadi. U quyidagi tarzda hisoblanadi:

$$Y_{dB}=R_{t.dBmVt}+G_{t.dBu}+ G_{r.dBu}-R_{min.dBmVt}- L_{t.dB}+L_{r.dB}$$

bu yerda $R_{t.dBmVt}$-uzatkichning quvvati; $G_{t.dBu}$-uzatuvchi antennaning kuchaytirish koeffisienti; $G_{r.dBu}$-qabul qiluvchi antennaning kuchaytirish koeffisienti; $R_{min.dBmVt}$-bu tezlikda qabullagichning sezgirligi; $L_{t.dB}$-signalning uzatish traktining koksial kabelida va raz’emlaridagi yo‘qotilishi; $L_{r.dB}$- signalning qabul qilish traktining koksial kabelida va raz’emlaridagi yo‘qotilishi.

Har bir tezlik uchun qabullagich ma’lum sezgirlikka ega. Uncha katta bo‘lmagan tezliklar (masalan, 1-2 Mbit) uchun sezgirlik kamroq -90 dBmVt dan -94 dBmVt gacha bo‘ladi. Yuqori tezliklar uchun sezgirlik ancha katta bo‘ladi. Misol sifatida 16.1-jadvalda 802.11a,b,g oddiy ulanish nuqtalarining bir necha xarakteristikalari keltirilgan.

1-jadval.

Sezgirlikni ma’lumotlarni uzatish tezligiga bog‘liqligi

Tezlik	Sezgirlik
54 Mbit/sekund	-66 dBmVt
48 Mbit/sekund	-71 dBmVt
36 Mbit/sekund	-76 dBmVt
24 Mbit/sekund	-80 dBmVt
18 Mbit/sekund	-83 dBmVt
12 Mbit/sekund	-85 dBmVt
9 Mbit/sekund	-86 dBmVt
6 Mbit/sekund	-87 dBmVt

Radiomodullarning turiga boo‘liq ravishda sezgirlik birmuncha o‘zgarishi mumkin. Ayonki, turli tezliklar uchun maksimal aloqaning uzoqligi turlicha bo‘ladi.

FSL quyidagi formula bo‘yicha hisoblanadi:

$$FSL = Y_{dB} - SOM$$

bu yerda SOM (System Operating Margin) – radioaloqa energetikasidagi zahira, dB. Aloqaning uzoqligiga salbiy ta’sir qiladigan bo‘lishi mumkin omillarni hisobga oladi. Ularga quyidagilar kiradi:

- qabullagich sezgirligi va uzatkichning chiqish quvvatining harorat dreyfi;
- atmosferahodisalari: tuman, qor, yomg‘ir;
- qabullagich, uzatkich antennasining antenna-fider trakti bilan nosozlanishi.

SOM parametr odatda 10 dB ga teng olinadi. Kuchaytirish bo‘yicha 10-desibelli zahira muhandislik hisobi uchun yetarli hisoblanadi.

Kanalning F markaziy chastotasi 16.2-jadvaldan olinadi.

16.2-jadval.

Markaziy chastotani hisoblash

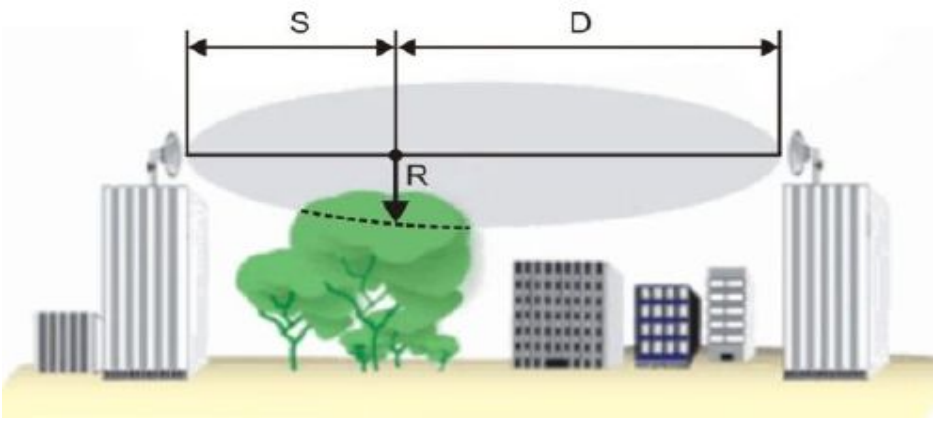
Kanal	Markaziy chastota, MGs	Kanal	Markaziy chastota, MGs
1	2412	8	2447
2	2417	9	2452
3	2422	10	2457
4	2427	11	2462
5	2432	12	2467
6	2437	13	2472
7	2442	14	2484

Yakunda aloqa masofasi uzoqligi formulasini olamiz:

$$D=10^{[(FSL/20)-(33/20)-lgF]}$$

Frenel zonasini hisoblash

Radioto‘lqin fazoda tarqalishi jarayonida oralig‘ida maksimal radiusli ellipsoid ko‘rinishida aylanadigan hajmni egallaydi (16.1–rasm). Bu fazoga tushib qolgan tabiy (yer, balandliklar, daraxtlar) va sun’iy (binolar, tayanchlar) signalni kuchsizlantiradi.



16.1–rasm. Frenel zonasi

Ko‘zda tutilgan to‘siq ustidagi Frenel birinchi zonasining radiusi quyidagi formula yordamida hisoblanishi mumkin.

$$R = 17{,}3\sqrt{\frac{1}{f}\frac{SD}{S+D}},$$

bu yerda R-Frenel zonasining radiusi, m; S, D-antennalardan ko‘zda tutiladigan to‘siqning eng yuqori nuqtasigacha bo‘lgan masofa, km; f-chastota, GGs.

Eslatma:

- odatda, Frenel zonasining 20 % blokirovkalanishini kanaldagi sezilarsiz so‘nish kiritadi. 40 % danortiq blokirovkalanishda signalning so‘nishi endi sezilarli bo‘lib qoladi, tarqalish zonasiga to‘siqlarning tushib qolishidan qochish kerak bo‘ladi.
- bu hisoblash yer tekis deb olinganda amalga oshirilgan. U yer sirtining egriligini hisobga olmaydi. Uzoq masofali kanallar uchun joyning relefini va tarqalish yo‘lidagi tabiy to‘siqlarni hisobga oladigan kompleks hisoblashni o‘tkazish kerak bo‘ladi. Antennalar orasidagi katta masofalarda yer sirtining egriligini hisobga olib antennalarning osilishi balandligini oshirishga harakat qilish kerak bo‘ladi.

Tashqi antennalarli antenna-fider traktlari va radiotizimlarni qo‘rish

Simsiz qurilmalarga qo‘shimcha antennalarni ulash, uzatkichning quvvatni kuchaytirishi, tizimgaqo‘shimcha filtrlarning ulanishi bo‘yicha masalalar simsiz tarmoqlarni qurish amaliyotida yetarlicha tez-tez uchraydi. Va bu mavzu bo‘yicha ko‘pmasalalar yuzaga keladi, ulardan eng keng tarqalgani ishlatiladigan qurilmalarda va qo‘shimcha kabellarda raz’emlarning muvofiqligi masalalari, shuningdek olingan tizimlarni hisoblash bo‘yicha masalalar hisoblanadi.

Shuni ta’kidlash kerakki, antennani ko‘tarish yaxshi emas, chunki bunda vujudga keladigan kabelli birikmalardagi signalning so‘nishi va parazit shovqinlar darajasining ortishi kabi salbiy omillar dastlabki radiotizimning xarakteristikalarini sezilardi yomonlashtiradi. Shu bilan birga antennaning ulanishi (ayniqsa, katta

kuchaytirish koeffisientili) ko‘p jihatdan bu salbiy omillarni kompensatsiyalaydi, lekin bunga qaramasdan loyihalashtirishda baribir ulanish nuqtalari aktiv qurilmalari portidan ko‘tarilgan antennagacha bo‘lgan masofani maksimala qisqartirishga va iloji boricha antennani ulanish nuqtasiga to‘g‘ridan-to‘g‘ri ulashga harakat qilinadi.

Bino ichida qamrab olish zonasini oshirish zarur bo‘ladigan hollar juda tez-tez bo‘ladi, buning uchun ichki bajarilishli antennalar (*indoor*) ishlatiladi. Uylar yoki tumanlar orasidagi aloqa uchun tashqi bajarilishdagi (*outdoor*) qimmatroq qurilmalar ishlatiladi.

Nazorat savollari

1. Sezgirlikni ma’lumotlarni uzatish tezligi nimaga bog’liq?
2. . Frenel zonasini tushuntiring
3. Frenel zonasini hisoblashini tushuntiring
4. Tashqi antennalarli antenna-fider traktlari va radiotizimlarni qo‘rishini tushuntiring

Foydalanilgan adabiyotlar:

Asosiy adabiyotlar

1. Proletarskiy A.V., Baskakov I.V., Chirkov D.N., Fedotov R.A., Bobkov A.V., Platonov V.A. Besprovodnie seti Wi-Fi. BINOM. Laboratoriya znaniy, Internet-universitet informatsionnix texnologiy - INTUIT.ru, 2007.

2. Semenov YU.A. Algoritmi telekommunikatsionnix setey. Chast 1. Algoritmi i protokoli kanalov i setey peredachi dannix. BINOM. Laboratoriya znaniy, Internet-universitet informatsionnix texnologiy - INTUIT.ru, 2007.

3. Novikov YU.V., Kondratenko S.V. Osnovi lokalnix setey. Internet-universitet informatsionnых texnologiy - INTUIT.ru, 2005.

4. A.X. Abdukadыrov, D.A. Davronbekov. Mobilnie sistemы svyazi pokoleniya 4G. - Tashkent. 2011. – 317 s.

5. V. Vishnevskiy, S. Portnoy, I. Shaxnovich. Ensiklopediya WiMAX. Put k 4G. M: Texnosfera, 2009. – 472s.

6. V.Yu. Babkov, M.A. Voznyuk, P.A. Mixaylov. Seti mobilnoy svyazi. Chastotno-territorrialnoe planirovanie/SPbGUT. – SPb, 2000.

Qo’shimcha adabiyotlar

1. Vishnevskiy V., Lyaxov A., Portnoy S, Shaxnovich I. Shirokopolosnie besprovodnie setiperedachi informatsii M.: Eко-Trendz, 2005, 592 s.

2. Grigorev V.A, Lagutenko O.I., Raspaev Yu.A. Seti i sistemi radiodostupa M.: Eко-Trendz, 2005, 384 s.

Internet saytlar:

1. www.gov.uz – O’zbekiston Respublikasi xukumat portali.

2. www.lex.uz – O’zbekiston Respublikasi qonun xujjatlari Қонун ҳужжатлари ma’lumotlari milliy bazasi.

3. www.tuit.uz

MUNDARIJA

“Simsiz keng polosali texnologiyalar”

fanidan ma’ruza ma’tinlari

Mobil aloqa texnologiyalari kafedrasi majlisida muhokama etildi

(19-majlis bayoni , 24.01.2017 y.) va cgop etishga tavsiya qilindi

Telekommunikatsiya texnologiyalari fakulteti ilmiy-uslubiy kengashida muhokama etildi va chop etishga tavsiya qilindi

(____sonli bayonnoma, 2017 yil «___»____).

Muxammad al-Xorazimiy nomidagi TATU ilmiy-uslubiy kengashi tomonidan chop etishga tavsiya qilindi

(____sonli bayonnoma, 2017 yil «___»____).

Tuzuvchi :

катta o’qituvchi M.O.Sultonova

mas’ul muharrir: dots. D.A. Davronbekov

Bosishga ruxsat etildi_____

Bichimi 60x84 1/16. bosma tabog‘i

Adadi Buyurtma №

Muxammad al-Xorazimiy nomidagi

Toshkent axborot texnologiyalari universiteti

“Nashr-matbaa” bo‘limida chop etildi.

Toshkent shahar, A.Temur ko‘chasi, 108-uy.