Security and Data Reliability in Cooperative Wireless Networks

Emad Hassan

CRC Press
Taylor & Francis Group

Security and Data Reliability in Cooperative Wireless Networks

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Security and Data Reliability in Cooperative Wireless Networks

Emad S. Hassan

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper

International Standard Book Number-13: 978-1-138-09279-2 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Preface

Broadcast nature is one of the main characteristics of the wireless medium with a double-edged arm; the first is beneficial while the other is harmful. With respect to its beneficial side, it allows applying what is called cooperative communications in wireless systems. Cooperative communication is a mechanism that aims to achieve transmission diversity performance enhancements in terms of increased capacity and improved transmission reliability in a new and interesting way. It enables many wireless devices in a multi-user environment, which are limited by size or hardware complexity to one antenna, to share their antennas for forwarding their messages to the destination together.

On the other hand, the harmful side of the wireless medium broadcast nature lies in its negative effect on the system security. Due to the broadcast nature of wireless communication networks, the adversarial "eavesdropper" nodes in their coverage area can intercept transmissions and try to recover parts of the transmitted message. Therefore, a resurgence of interest has been given recently for studying the security of data transmission in wireless systems from a physical layer point of view. The main objective behind physical layer security is to enable the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers, without relying on higher-layer encryption.

This book provides new solutions for these problems, and its main objective is to enhance the security and data reliability in cooperative wireless networks.

A major attraction of the book is the presentation of MATLAB® simulations and the inclusion of MATLAB codes to help readers understand the topic under discussion and to be able to carry out extensive simulations. The book is structured into ten chapters and broadly covers two important parts as follows:

Part one: Security in cooperative wireless networks
Part two: Security and data reliability in wireless sensor networks (WSNs)

- In the first part, we first give a detailed overview about both cooperative communications and the physical layer security, the two main topics on which our book relies. We firstly introduce cooperative communications,

the innovative approach which exploits wireless medium broadcast nature to achieve multiple-input–multiple-output (MIMO) gains in a distributed manner in order to be suitable for application in small wireless devices. Different cooperative protocols concerned with the processing of the signal received from the source node at the relay node are discussed. Furthermore, different relay selection metrics concerned with selecting the best relay among the available N relays with an indication to the entity which evaluates these metrics and selects the relay are also given. Finally, we end this point by presenting cooperative communication applications and the pros and cons.

- In addition to the foregoing, an overview for physical layer security is also given in this first part of the thesis. The main objective behind physical layer security is to improve the secrecy rate of a given transmitter–receiver pair in the presence of unauthorized eavesdroppers. This can be accomplished by using some relay nodes as jamming nodes to transmit artificial interference and confuse the eavesdroppers. Firstly, we give an overview about both key-based and keyless security. This is followed by discussing such cooperating approaches that help in achieving secrecy at the physical layer of a multi-user system through introducing the cooperative jamming concept. Then, the idea of employing cooperative jammers in a multiple relay network in order to improve security is adopted. Finally, the interactions arising between cooperation and secrecy in the channel models with untrusted relays are studied.
- Then, different relay and jammer selection schemes are proposed in order to achieve security in one-way cooperative networks. It should be obvious that selecting the best relay is necessary for applying the cooperative communication idea through its assistance to the source in forwarding its message to the corresponding destination besides its own message. Moreover, selecting jammers is necessary for achieving physical layer security through their intentional interference at the eavesdroppers' nodes. The selection schemes without jamming, the selection schemes with conventional jamming, the selection schemes with controlled jamming, and the hybrid switching schemes are the four different proposed selection schemes presented through this part. The numerical results shown at the end of this part illustrate the effectiveness of the different proposed schemes in improving both ergodic secrecy capacity and secrecy outage probability performance metrics. The proposed selection schemes with jamming outperform the corresponding nonjamming selection schemes, and the hybrid schemes which switch between jamming and nonjamming selection schemes further improve both performance metrics.
- Because of two-way relay channel bandwidth efficiency and potential application to cellular networks and peer-to-peer networks, different relay and jammer selection schemes are proposed to improve physical layer security in two-way cooperative networks. The obtained results show that the selection schemes with jamming cannot outperform the schemes without jamming in

all cases. Therefore, a hybrid scheme which switches between both jamming and nonjamming selection schemes is introduced as an efficient solution in such cases. In addition to the foregoing, the obtained results show the ongoing effectiveness of our proposed selection schemes in improving both the secrecy rate and the secrecy outage probability of the two-way cooperative networks despite the presence of multiple cooperating eavesdroppers. At the end of this part, a comparison between relay and jammer selection schemes in both one-way and two-way cooperative networks is given in terms of both secrecy metrics.

- The second part of this book focuses on data security and reliability in unattended wireless sensor networks (UWSNs) in the presence of a mobile adversary. In this part, we explore the different challenges of UWSNs, such as compromising probability, probability of BSe to be compromised, and data reliability. During this part, several self-healing algorithms are developed to provide data security and reliability in UWSNs. In the second part of this book, we cover the following points:
  - Overview of WSNs followed by an overview of UWSNs.
  - A proposal called the cooperative hybrid self-healing randomized distributed (CHSFRD) scheme is introduced to provide self-healing in UWSNs. Self-healing algorithms are developed to increase the likelihood for data reliability and data security in homogeneous UWSNs, without implementing cryptography. In addition, the UWSN model is defined in a way that encompasses all common WSN assumptions and characterizes the unattended operation mode that involves periodic visits by an itinerant sink. Also, we define a new adversarial model geared for UWSNs, delineating its capabilities and identifying many adversary subtypes based on its specific goals. The proposed scheme is based mainly on the hybrid cooperation principal between healthy and compromised (sick) sensors and that sensor collaboration is necessary to mislead an adversary. The proposed scheme proves its ability to enhance the UWSN security by improving the data reliability and compromising probability and probability of backward secrecy.
  - A proposal called self-healing controlled mobility within a cluster (SH-CMC) scheme is developed for self-healing enhancement in UWSNs, in which the clustering and mobility of some sensors were used beside the hybrid cooperation. Both of them can enhance the self-healing capability of UWSNs. In addition, different mobility models available for wireless networks are discussed in detail. The proposed scheme proves that using the mobility within a cluster of sick sensors is the best and complementary solution for the problem of the leakage of healthy sponsors. The proposed scheme proves that the use of mobility beside the hybrid cooperation can enhance the self-healing capability over the scheme that does not consider mobility.

  - A proposal called self-healing single flow cluster controlled mobility (SH-SFCCM) scheme is introduced for self-healing enhancement considering energy consumption due to mobility. The trade-off between energy consumption in both mobility and communication is estimated. The energy consumption cost functions for both communication and mobility are estimated. In addition, the influence of sensor mobility on self-healing capability and other network aspects is studied.
- Finally, MATLAB codes for all simulation experiments are included in Appendices A-E at the end of the book.

List of Abbreviations

AF	Amplify-and-forward
AWGN	Additive white Gaussian noise
BPCU	Bits per channel use
CF	Compress-and-forward
CRC	Cyclic redundancy check
CS	Conventional selection
CJ	Cooperative jamming
CRBC	Cooperative relay broadcast channel
CSI	Channel state information
DF	Decode-and-forward
ECC	Error control coding
EGC	Equal gain combiner
GSM	Global system for mobile communications
GWT	Gaussian wiretap channel
ISI	Intersymbol interference
i.i.d	Independent and identically distributed
MIMO	Multiple-input–multiple-output
MISO	Multiple-input–single-output
MRC	Maximal ratio combiner
MAC-GF	Multiple access channel with generalized feedback
NE	Nash equilibrium
NF	Noise forwarding
OR	Opportunistic relaying
OS	Optimal selection
OSJ	Optimal selection with jamming
OW	Optimal switching
OSCJ	Optimal selection with controlled jamming
OS-MMISR	Optimal selection with max–min instantaneous secrecy rate
OSJ-MMISR	Optimal selection with jamming with max–min instantaneous secrecy rate
PL	Path loss
PU	Primary user

PHY	Physical layer
QoS	Quality of service
SC	Selection combiner
SNR	Signal-to-noise ratio
SU	Secondary user
SIMO	Single-input–multiple-output
SS	Suboptimal selection
SSJ	Suboptimal selection with jamming
SW	Suboptimal switching
s.d.o.f.	Secure degrees of freedom
SINR	Signal to interference-plus-noise ratios
SS-MMISR	Suboptimal selection with max–min instantaneous secrecy rate
SSJ-MMISR	Suboptimal selection with jamming with max–min instantaneous secrecy rate
VAA	Virtual antenna array
WSN	Wireless sensor network
WANET	Wireless ad hoc network
ZF	Zero-forcing

List of Symbols

A	Best passive helpers
B_d	Doppler-frequency spread
B_c	Channel coherence bandwidth
B_s	Transmitted signal bandwidth
$b(\cdot)$	Function depends on the processing strategy implemented at the relay node
c	Speed of propagation of the electromagnetic field in the medium
C	Cryptogram
C_S	Secrecy capacity
C_B	Channel capacity of the legitimate link
C_E	Channel capacity of the eavesdropping link
C_d	Decoding set
d_0	Reference distance
$d_{a,b}$	Euclidean distance between node a and node b
D	Destination
d	Distance between the transmitter and the receiver
E	Eavesdropper
$\mathrm{E}[.]$	Expectation operator
$\mathrm{E}\left[R_S^{\lvert C_d \rvert}(R, J_1, J_2) \right]$	Ergodic secrecy rate
F	Number of subcarriers
f_o	Transmitted frequency
f_d	Doppler shift
g	Channel gains vector to the eavesdropper
G_d	Diversity gain
$h_{s,d}$	Channel fades between the source and destination
$h_{s,r}$	Channel fades between the source and the relay
$h_l(t)$	Attenuation of the l-th path at time t
$h_{R_i,D}$	Channel gain between the i-th relay node and the destination node
h_{S,R_i}	Channel gain between the source node and the i-th relay node

h	Channel gains vector to the intended receiver
$h_{a,b}$	Channel coefficient for each channel $a \rightarrow b$
$H(.)$	Entropy
$I(.\ ;.)$	Mutual information
$I_{S,Ri}$	Source–relay channel mutual information
J_1	First phase jammer
J_2	Second phase jammer
J_1^*	First selected jammer
J_2^*	Second selected jammer
K	Number of helpers
$\mathcal{K}$	Secret key
L	Number of resolvable paths at the receiver
L'	Ratio between the relay power to the jammer power
m	Eavesdropper number
M	Number of eavesdroppers
m_g	Multiplexing gain
N_t	Number of transmitting antennas
N_r	Number of receiving antennas
$n_{\mathrm{s,d}}$	Additive noise at the destination
$n_{\mathrm{s,r}}$	Additive noise at the relay
$\check{N}$	Noise variance
N_p	Noise power spectral density
N	Number of intermediate nodes (relays)
n	Relay number
$PL_{(dB)}$	Path loss measured in dB
P_{SER}	Probability of symbol error
P	Source and relay nodes equal transmitted power
P_l	Transmitted power of the legitimate transmitter
P_{out}	Secrecy outage probability
$P^{(S)}$	Transmitted power of the source node
$P^{(R)}$	Transmitted power of the relay node
$P^{(J)}$	Transmitted power of the jamming nodes
Q	Covariance matrix
R^*	Best relay
R_T	Target secrecy rate
R_0	Transmission spectral efficiency/required transmission rate
R	Conventional relay
$R_{S_i}^{\lvert C_d \rvert}(R, J_1, J_2)$	The instantaneous secrecy rate with the decoding set C_d for source S_i
S_{eves}	Eavesdroppers set
S_1	First source
S_2	Second source
S	Source

S_{relay}	Intermediate node set
T_m	Channel delay spread
T_s	Duration of the symbols
T_c	Channel coherence time
$\mathcal{T}$	Number of transmission hops
v	Speed of the vehicle
V	Message carrying signal
W	Confidential message
x	Jamming signals vector emitted by the helpers
X	Legitimate transmitter information signal
$x(t)$	Transmitted signal
$y(t)$	Received signal
$y_{\mathrm{s,d}}$	Received signal at the destination in the first phase
$y_{\mathrm{s,r}}$	Received signal at the relay
$\mathrm{y}_{\mathrm{r,d}}$	Received signal at the destination in the first phase
Y	Intended receiver observed signal
Z	Unauthorized eavesdropper received signal
β	Path-loss exponent
ω	Shadow loss
Γ_i	Signal to interference-plus-noise ratio of link $S_j \rightarrow S_i$
Γ_{E_j}	Signal to interference-plus-noise ratio of link $S_j \rightarrow E$
δ	Constant related to the antenna gain and the average channel attenuation
$\sigma^2_{a,b}$	Channel variance
$(.)^T$	Transpose
$\tau_l(t)$	Corresponding path delay
θ	Angle between the direction of propagation of the electromagnetic wave and the direction of motion
α	Coding length
$\gamma_{a,b}$	Instantaneous signal-to-noise ratio for the link $a \rightarrow b$
γ	Signal-to-noise ratio
σ^2_B	Power of ambient Gaussian noise at the intended receiver
σ^2_E	Power of ambient Gaussian noise at the unauthorized eavesdropper
ψ_0	Global instantaneous knowledge for all the links
ψ_1	Average channel knowledge for the eavesdropper links

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

About the Author

Dr. Emad S. Hassan received his BSc (Honors), MSc, and PhD from the Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2003, 2006, and 2010, respectively. In 2008, he joined the Communications Research Group at Liverpool University, Liverpool, UK, as a visitor researcher to finish his PhD research. He is Associate Professor at the Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menoufia University, Egypt.

Dr. Hassan was a full-time demonstrator (2003–2006) and Assistant Lecturer (2007–2010) at the Faculty of Electronic Engineering, Menoufia University. He has been a visitor researcher at Liverpool University, Liverpool, UK, (2008–2009); a teaching assistant at the University of Liverpool, UK (2008–2009); Assistant Professor (2010–2015) and Associate Professor (2015–present) at the Faculty of Electronic Engineering, Menoufia University; and a part-time lecturer at many respectable private engineering universities in Egypt (2010–2011). He co-supervises many MSc and PhD students, (2010–present). Currently, he is Associate Professor at the Faculty of Engineering, Jazan University, Saudi Arabia.

Dr. Hassan is a reviewer for many international journals and conferences. He was a Technical Program Committee (TPC) member for many international conferences. He has published more than 66 scientific papers in national and international conference proceedings and journals and three books under CRC Press, Taylor & Francis. His current research areas of interest include image processing, digital communications, cooperative communication, cognitive radio networks, OFDM, SC-FDE, MIMO, WSNs, and CPM-based systems.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Acknowledgments

First and foremost, I am thankful to *God*, the most gracious most merciful, for helping me finish this work.

I wish to express my sincere thanks to *Prof. Fathi E. Abd El-Samie*, *Prof. Moawad Dessouky*, and *Prof. Sami El-Dolil*. I am deeply indebted to them for their valuable comments, continuous encouragement, useful suggestions, and active help during the course of this work.

Many thanks are extended to the authors of all journals and conference papers, articles, and books that have been consulted in writing this book. I would also like to extend my gratitude to all my past and current MSc and PhD students for their immense contributions to knowledge in the area of security and data reliability in cooperative wireless networks. Their contributions have undoubtedly enriched the content of this book.

Also, I greatly appreciate the support received through the collaborative work undertaken with the *Engineering College, Jazan University, KSA*.

Finally, I remain extremely grateful to my family who has continued to be supportive and provide the needed encouragement. In particular, my very special thanks go to my wife, *Samah A. Ghorab*, for her continuous patience and unconditional support that have enabled me to finally complete this challenging task. Her support has been fantastic. Also, my three wonderful children, Mahmoud, Omar and Joury, who provide unending inspiration.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 1

Introduction

1.1 Cooperative Wireless Networks

Future generations of cellular communications require higher data rates and a more reliable transmission link with the growth of multimedia services, while keeping satisfactory quality of service. Multiple-input–multiple-output (MIMO) antenna systems have been considered as an efficient approach to address these demands by offering significant multiplexing and diversity gains over single-antenna systems without increasing bandwidth and power. Although MIMO systems can unfold their huge benefit in cellular base stations, they may face limitations when it comes to their deployment in mobile handsets. To overcome this drawback, an innovative approach known as cooperative communication has been suggested to exploit MIMO's benefit in a distributed manner. Such a technique is also called a virtual MIMO, since it allows single-antenna mobile terminals in a multi-user environment to share their antennas and therefore reap some of the benefits of MIMO systems.

Because of the inherent openness of the wireless transmission medium, wireless communication systems are particularly vulnerable to security attacks. It is therefore necessary to focus on guaranteeing confidentiality against eavesdropping attacks where an unauthorized entity aims to intercept an ongoing wireless communication. From a physical layer point of view, the transmission secrecy can be achieved by exploiting the inherent randomness of noise and communication channels to limit the amount of information that can be extracted at the 'bit' level by an unauthorized receiver. Adopting this point of view, in a multi-user network, focusing on a specific transmitter–receiver pair, other (independent) transmitters can act as helpers that can improve the individual secrecy rate of this specific pair by cooperatively jamming the eavesdropper.

1.1.1 Cooperative Communications Idea

The increasing number of users demanding service has encouraged intensive research in wireless communications. However, the problem with wireless communications is the unreliable medium through which the signal has to travel. To mitigate the effects of wireless channel on the transmitted signal, the idea of diversity has been deployed in many wireless systems [1–3]. Space diversity, for example, is a communication technique where the transmitted signal travels through various independent paths, and thus the probability that all the wireless paths are in fade is made negligible. Time diversity, frequency diversity, and space diversity are the three basic techniques for providing diversity to wireless communication systems.

Multiple-input–multiple-output (MIMO) systems, where the transmitters as well as the receivers are equipped with multiple antennas, proved to be a breakthrough in wireless communication systems, which offered a new degree of freedom, in spatial domain, to wireless communications. However, due to size, cost, or hardware limitations of many wireless agents, it became a challenge to support them with multiple transmitting antennas. To address this challenge, the idea of cooperative communications came into existence to implement the idea of MIMO in a distributed manner. This concept says that transmitting users share each others' antennas to forward their messages to the destination and form a virtual MIMO.

1.1.2 Physical Layer Security Idea

Away from the traditional cryptographic techniques for ensuring security in a wireless system, nowadays, most researchers started studying secrecy from a physical layer point of view. The idea of achieving security in a physical layer depends mainly on maximizing the capacity of the main channel, i.e., channel between the legitimate source–destination pair, about that of the wiretap channel, i.e., channel between the source and the eavesdropper. The degradation of the wiretap channel can be achieved by using some jammers to transmit intentional interference on the eavesdroppers and confuse them.

1.2 Wireless Sensor Networks

The goal of a wireless sensor network (WSN) is to provide the end user with a more intelligent understanding of its life and environment. WSN is a class of special wireless ad-hoc networks. An ad hoc network is a group of wireless nodes that interconnect directly over a common wireless channel. There is no extra structure needed for ad hoc networks. A strength of this type of networks is their capability of self-organizing the infrastructure after they are installed. There are many

differences between common ad hoc networks and WSNs; they are outlined below [4–6]:

- Different areas of application.
- The number of sensor nodes in a WSN is several orders higher than that in an ad hoc network.
- Sensor nodes are closely deployed.
- The topology of this network changes frequently.
- WSNs use broadcast while most ad hoc networks use point-to-point communications.
- Sensors are limited in computational capacities, power, and memory.
- Sensors may not take global identification (ID) because this will cause a large overhead communication.

A WSN is formed from distributed autonomous sensor nodes to monitor environmental conditions, such as temperature, pressure, and sound, and cooperatively send their data through the network to a main site. For example, sensors can be deployed underwater to monitor ocean currents or on top of a mountain to monitor pollution at high altitudes, within the foundation of a building to acquire information on vibration, or be attached to animals to supervise migration patterns. WSNs are used in many industrial and civilian applications, such as environment and habitat monitoring, industrial process control, home automation, health care, and traffic regulation.

The typical size of a WSN ranges between tens to thousands of sensors. WSNs are managed through a powerful device, usually referred to as the sink that represents the gateway between the WSN and the external world (e.g., the Internet). The sink is considered to be a trusted, tamper-resistant, online device. It is responsible for providing commands to sensors and collecting data.

In some application, it is required that the sink is not existent all the time. This is due to the fact that the area is too large to be covered by the sink, or it is not required for the sink to exist all the time due to the environment or the measurement. We therefore have what is called an unattended wireless sensor network (UWSN).

1.2.1 Unattended Wireless Sensor Networks

A UWSN [7–10] (Figure 1.1) is a specific type of WSN where the sink is absent most of the time. Data sensed by the sensor nodes is not collected continuously by the data sink. Data has to be stored and secured by every node until the subsequent visit of the mobile data sink. This inability to communicate with the sink might be for reasons such as power constraints, limited transmission ranges, or signal propagation difficulties [11]. The concept of UWSNs with a mobile sink looks realistic if we consider the environments where the sensing under consideration is too far

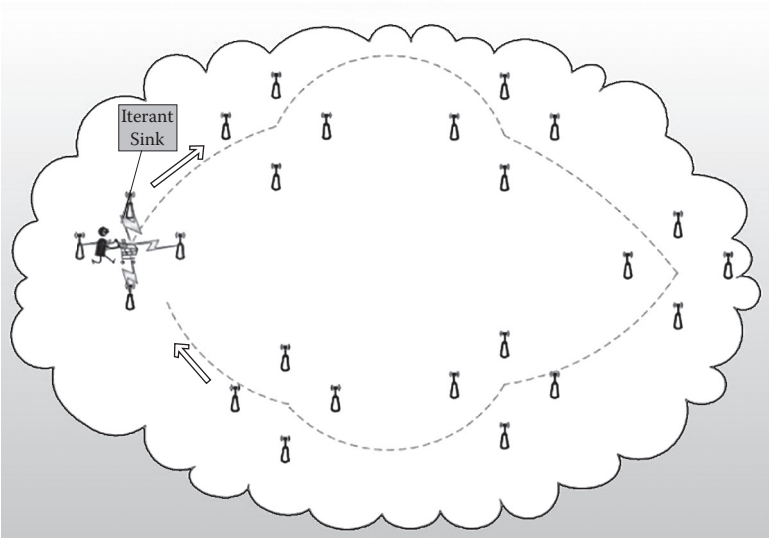

Figure 1.1 Unattended wireless sensor network with mobile sink collecting the data.

from the base station. Sending data through midway nodes may therefore result in a weakening of the network security (e.g., for example the midway nodes may alter the data) or an increase in the energy consumption of the nodes close to the base station. In normal multi-hop WSN, the power of the sensors placed nearby the sink will be exhausted earlier than that of the other sensor nodes.

The reason behind it is that all the sensors have to transmit their data to the data sink through the sensor nodes placed nearby the data sink. Therefore, the UWSN can save the battery of these sensor nodes, and, as a result, an increase in the lifetime of the network can be achieved.

Unattended environments as mentioned in [12,13] include sensor networks for monitoring airborne networks for tracking adversary aircrafts, vibration and sound produced by army troop motion, and LANdroids [14], which retain information until soldiers move close to the network. In addition, it can be used for monitoring nuclear emissions, national parks for firearm discharge and illicit cultivation, and along an international border to record illegal crossings. The scale, in terms of both the number of sensors and the size of the coverage area, might make it too costly to install a multitude of fixed sinks–one per border segment.

The common feature in the above-mentioned examples is that constant physical access to the entire sensor network is impossible, and a periodic visit by an itinerant sink may be more realistic. Consequently, sensors cannot off-load their data in real-time fashion: they have to collect data and wait for an upload signal. Sensors' lack of ability to off-load their data in real time exposes them to a great

risk. Moreover, this rules out all security protocols that rely on the constant presence of the sink.

Another common assumption in prior WSN's security is that an adversary can compromise a set of sensors during the entire operation of the network. In contrast, we envision a powerful UWSN adversary that can compromise up to a certain number of sensors within a specific time interval. This interval can be smaller than the time between two consecutive visits of the data sink. Given more intervals, the adversary can undermine the whole network as it moves from a set of compromised sensors to another set, thus gradually undermining network security.

1.3 Motivation

In many real-world applications, critical data is collected and stored in the unattended nodes in hostile environments. The data must be stored until the next visit of the data sink. The unattended nature of the network and the lack of tamper-resistant hardware increase the susceptibility of attacks over the data collected by the sensors [15].

Since the UWSN scenario is different from that of a traditional WSN, defense solutions from WSN security literature are not suitable for coping with a mobile adversary in UWSNs. Security needs should be taken into account to ensure data protection (also called data reliability) in these sensors at the time of design. Data security and data authentication are a major concern in UWSNs.

Most cryptographic techniques provide data authenticity and integrity but do not ensure data reliability. This implies that if an adversary compromises a sensor and destroys the data contained therein, the data is lost forever. Another drawback of cryptographic schemes is that they are computationally costly, and this is not suitable for resource-constrained sensors. For these reasons, non-cryptographic techniques can be considered over cryptographic ones. In the past few years, techniques for data authentication have been proposed [15,16] as well as cryptographic techniques for data protection [9,13,17–19].

The above-mentioned schemes assume that the sensors are stationary between consecutive visits from the data sink. However, this assumption is not practical in some real applications, so it must be relaxed and allow nodes to move between two visits from the data sink. Another important concern in UWSNs is that a mechanism is needed to ensure that the data received at the sink is authentic.

The main goal of some of the adversaries is to inject fraudulent data into the information collected by the nodes and remain undetected. The mobile adversary can compromise K out of N nodes during each round; also, it can switch to other sets of K nodes during the next rounds. Authentication schemes for UWSN against a mobile adversary presented in [15] and [16] guarantee good security but suffer from high communication cost relative to the level of security achieved. The problems identified above motivates us to find the best possible way for securing the data in UWSNs.

1.4 Problem Statement

Along with the growing popularity of WSN, it continues to be plagued by issues of data security, a situation which has prompted considerable research during the past period. WSNs are vulnerable to many kinds of attacks due to their inherent features, such as being self-organized and lacking tamper resistance [20,21]. Most of the previous research has focused on data security in the presence of a static online sink, which is considered as follows:

- A trusted party (i.e., tamper resistant)
- Can obtain collected data from sensors in real time (or near real time)
- Can take appropriate action instantly to cease the further effects of an adversary if one is detected [22]

However, our focus is on security in UWSNs, which is more challenging than for WSNs because most of the time sensors' activities are left unattended. Sensors are not able to communicate with the sink in a real-time manner and do not off-load data immediately after collecting them. An adversary can easily take advantage of the time between sink visits to roam the network with impunity and thereby learn the network topology and security strategy, compromise sensors, alter or delete the collected data in the sensors' storage, and leave the network without leaving a trace to the collector. In light of such potential overwhelming and pervasive threats, the issue here is how to protect data against an adversary or how to maintain data survival until a collector arrives [23].

1.5 Book Objectives and Contributions

This book addresses the following:

1. **Overview of the wireless channel impairments**. At first, the path loss, shadowing, and fading effects are introduced as the main wireless channel impairments that impede the achievement of future generations' requirements.
2. **Study of MIMO antenna systems**. The basic idea of the spatial-diversity-based MIMO systems is briefly explained. Then, the efficiency of MIMO systems in dealing wireless channel impairments is shown.
3. **Overview of cooperative communication in wireless systems**. The great role of the emerged cooperative communication paradigm in overcoming the difficulties of applying MIMO in mobile handsets is illustrated. In cooperative communication, a virtual MIMO system is formed by sharing antennas of the single-antenna mobiles in the multi-user environment. A hint to the relay channel concept which considers the basis for a cooperative communication working principle is also given.

4. **Study of different cooperation protocols**. Both fixed relaying schemes and adaptive relaying schemes focused on studying the processing strategy implemented on the source information at the relay node are introduced.
5. **Study of different relay selection metrics**. In this work, different relay selection metrics concerned with selecting the best relay among the available N relays are presented. The selected relay helps in applying the cooperative communications concept by assisting the source in forwarding its message to the destination besides its own message.
6. **Overview of the physical layer security in wireless systems**. The side effect of the wireless transmission broadcast nature which led to the application of data security in the wireless systems is firstly illustrated. Then, the main vulnerabilities of many implemented traditional cryptographic schemes which have recently motivated many researchers to study the data security from a physical layer point of view are shown. Physical layer security depends mainly on the inherent randomness of noise and communication channels to limit the amount of information that can be extracted by the eavesdropper.
7. **Study of cooperative secrecy techniques for physical layer**. Various cooperating approaches helping in achieving secrecy at the physical layer of a multi-user system through introducing the cooperative jamming concept are given. All the nodes in the coverage area of the transmission except the legitimate source–destination pair can act as jammers to confuse the eavesdroppers and prevent them from extracting the source information.
8. **Proposal of joint relay and jammer selection schemes for secure one-way cooperative networks**. Different proposed relay and jammer selection schemes focused on selecting one relay and two jamming nodes are introduced for ensuring physical layer security in one-way cooperative networks. In one-way cooperative networks, the signal is transmitted in one direction from the source to the destination. The obtained results showed the effectiveness of the different proposed schemes in improving both ergodic secrecy capacity and secrecy outage probability metrics.
9. **Proposal of joint relay and jammer selection schemes for secure two-way cooperative networks**. Due to the great benefits of the two-way relay channel into which the legitimate transmission pair has the ability to both transmit and receive messages, various relay and jammer selection schemes have been proposed in order to improve physical layer security in this type of networks. Then, through the numerical results, the integration between different categories of the proposed relay and jammer selection schemes is shown, and the ability of each category to improve performance metrics under certain network conditions is illustrated.
10. **Performance comparison of different proposed selection schemes in different network models**. A comparison between the proposed relay and jammer selection schemes in both one-way and two-way cooperative networks is presented in terms of ergodic secrecy capacity and secrecy outage probability.

The obtained results showed that when the relays are distributed dispersedly between the sources and the eavesdropper, all the proposed two-way schemes outperform the proposed one-way schemes, especially when the transmitted power is increased.

11. **Study of the effect of the multiple eavesdroppers' presence on the secrecy of both one-way and two-way network models**. The obtained results showed that even if there are multiple eavesdroppers, the different proposed selection schemes still have the ability to improve the performance metrics.
12. **Overview of WSNs** followed by an overview of UWSNs.
13. **A proposal called the cooperative hybrid self-healing randomized distributed (CHSFRD) scheme** is introduced to provide self-healing in UWSN. Self-healing algorithms is developed to increase the likelihood for data reliability and data security in homogeneous UWSNs, without implementing cryptography. In addition, the UWSN model is defined in a way that encompasses all common WSN assumptions and characterizes the unattended operation mode that involves periodic visits by an itinerant sink. Also, we define a new adversarial model geared for UWSNs, delineating its capabilities and identifying many adversary subtypes based on its specific goals. The proposed scheme is based mainly on the hybrid cooperation principal between healthy and compromised (sick) sensors; sensor collaboration is necessary to mislead an adversary. The proposed scheme proves its ability to enhance the UWSN security by improving the data reliability and compromising probability and probability of backward secrecy.
14. **A proposal called the self-healing controlled mobility within a cluster (SH-CMC) scheme** is developed for self-healing enhancement in UWSNs, in which the clustering and mobility of some sensors were used beside the hybrid cooperation. Both of them can enhance the self-healing capability of UWSNs. In addition, different mobility models available for wireless networks were discussed in detail. The proposed scheme proves that using the mobility within a cluster of sick sensor is the best and complementary solution for the problem of the leakage of health sponsors. The proposed scheme proves that the use of mobility beside the hybrid cooperation can enhance the self-healing capability more than the scheme that does not consider mobility.
15. **A proposal called the self-healing single flow cluster controlled mobility (SH-SFCCM) scheme** is introduced for self-healing enhancement considering energy consumption due to mobility. The trade-off between energy consumption in both mobility and communication is estimated. The energy consumption cost functions for both communication and mobility are estimated. In addition, the influence of sensor mobility on self-healing capability and other network aspects is studied.

1.6 Book Outline

Chapter 2 gives a general overview of the cooperative communications through handling the first five objectives of the book in detail.

Chapter 3 highlights many issues concerned with achieving secrecy in the physical layer through discussing the sixth and seventh objectives of the book in detail.

Chapter 4 focuses on achieving the book's eighth objective by presenting the different proposed relay and jammer selection schemes for ensuring secrecy in one-way cooperative networks. Also, the book's eleventh objective concerned with studying the effect of the presence of multiple eavesdroppers on the network performance metrics is discussed.

Chapter 5 illustrates the efficiency of the proposed relay and jammer selection schemes in improving the physical layer security of two-way cooperative networks, the book's ninth objective. Moreover, a comparison between the different proposed relay and jammer selection schemes in both one-way and two-way cooperative networks (the book's tenth objective) is provided in the presence of one or multiple eavesdroppers.

Chapter 6 presents an overview on the WSN, composition of WSN, types, modes, application, and factors influencing WSN design. This is followed by an overview on the UWSN, as well as security research applied to the field, expounding on the unattended feature of this network, together with the benefits and impacts. An explanation of the network composition, the strong and weak points and application, the mobile adversary, security goals, and challenge, and the possible attacks on nodes is given.

Chapters 7 proposes a novel cooperative hybrid self-healing randomized distributed (CHSFRD) scheme for self-healing in UWSNs. The proposed scheme is based mainly on the hybrid cooperation principal; it proves its ability to enhance the UWSN security by improving data reliability and security in UWSNs.

Chapters 8 presents a novel proposal of a self-healing controlled mobility within a cluster (SH-CMC) scheme. This scheme uses the clustering and mobility beside the hybrid cooperation to enhance the self-healing capability. Different mobility models are discussed. Also, we define a new powerful adversarial model to attack the UWSN.

Chapters 9 proposes a self-healing single flow cluster controlled mobility (SH-SFCCM) scheme; it is a novel scheme for self-healing. The trade-off between energy consumption in both mobility and communication is estimated. The energy cost functions for communication and motion are assessed. The impact of sensor mobility on network aspects is studied.

Chapter 10 presents the concluding remarks and the future work.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

References

3GPP TR 36.814 V1.2.1. “Further advancements for EUTRA: Physical layer aspects”. Technical Specification Group Radio Access n/w. Jun. 2009.

I. P802.16j/D9 . “Draft amendment to IEEE standard for local and metropolitan area network part 16: Air interface for fixed and mobile broadband wireless access systems: Multihop relay specification”. May 2009.

Y. Yang , H. Hu , J. Xu , and G. Mao . “Relay technologies for WiMAX and LTE Advanced mobile systems”. IEEE Comm. Magazine 47(10), 100–105, Oct. 2009.

E. H. Callaway . Wireless Sensor Networks: Architectures and Protocols. CRC Press, 2003.

H. M. Ammari . The Art of Wireless Sensor Networks. Springer, 2014.

I. Stojmenovic , Ed. Handbook of Sensor Networks: Algorithms and Architectures. Vol. 49. John Wiley & Sons, 2005.

T. M. Y. Vo and J. Talim . “Random distribution for data survival in unattended wireless sensor networks”. In: Sensor Technologies and Applications (SENSORCOMM), Fourth International Conference, pp. 468–471, IEEE, 2010.

S. K. V. L. Reddy . Data Security in Unattended Wireless Sensor Networks. PhD Dissertation, University of Ottawa, 2013.

R. Di Pietro , L. V. Mancini , C. Soriente , A. Spognardi , and G. Tsudik . “Catch me (if you can): Data survival in unattended sensor networks”. Proc. of PERCOM ‘08, Washington, DC, USA, IEEE Computer Society, pp. 185–194, 2008.

D. Ma and G. Tsudik . “Extended abstract: Forward-secure sequential aggregate authentication”. Proc. IEEE Symp. on Security and Privacy, Oakland, CA, USA, pp. 86–91, May 2007.

R. D. Pietro , L. V. Mancini , C. Soriente , A. Spognardi , and G. Tsudik . “Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks”. Ad Hoc Networks 7(8), 1463–1475, 2009.

R. D. Pietro , L. V. Mancini , C. Soriente , A. Spognardi , and G. Tsudik . “Data security in unattended wireless sensor networks”. IEEE Transactions on Computers 58(11), 1500–1511, 2009.

R. D. Pietro , L. V. Mancini , C. Soriente , A. Spognardi , and G. Tsudik . “Maximizing data survival in unattended wireless sensor networks against a focused mobile adversary”. IACR Cryptology e-Print Archive, 1–23, 2008.

Information Processing Technology Office (IPTO) Defense Advanced Research Projects v Agency (DARPA) , BAA 07-46 LANdroids Broad Agency Announcement, URL: http://www:darpa:mil = IPTO = solicit = open = BAA—07-46 P IP:pdf, 2007.

T. Dimitriou and A. Sabouri . “Pollination: A data authentication scheme for unattended wireless sensor networks”. In: Proc. IEEE Trust, Security and Privacy in Computing and Communications, pp. 409–416, 2011.

R. D. Pietro , L. V. Mancini , C. Soriente , A. Spognardi , and G. Tsudik . “Collaborative authentication in unattended wireless sensor networks”. Proc. 2nd ACM Conference on Wireless Network Security, Zurich, Switzerland, pp. 237–244, 16–19 Mar. 2009.

R. Di Pietro , D. Ma , C. Soriente , and G. Tsudik . “POSH: Proactive co-operative self-healing in unattended wireless sensor networks”. Proc. IEEE Symp. on Reliable Distributed Systems, Napoli, Italy, pp. 185–194, Oct. 2008.

R. D. Pietro , G. Oligeri , C. Soriente , and G. Tsudik . “Securing mobile unattended WSNs against a mobile adversary”. In: Proc. IEEE Symp. on Reliable Distributed Systems, pp. 11–20, 2010.

M. A. Santos , C. B. Margi , M. A. Jr., G. F. Pereira , and B. T. Oliveira . “Implementation of data survival in unattended wireless sensor networks using cryptography”. Proc. IEEE Local Computer Networks (LCN), Sense App, Denver, Washington USA, IEEE Computer Society, pp. 961–967, 10–14 Oct. 2010.

Y. Wang , G. Attebury , and B. Ramamurthy . “A survey of security issues in wireless sensor networks”. IEEE Commun. Surveys Tutorials 8, 2–23, 2006.

G. Padmavathi and D. Shanmugapriya . “Survey of attacks, security mechanisms and challenges in wireless sensor networks”. International Journal of Computer Science and Information Security (IJCSIS), 4(1&2), 2009.

Z. Ruan , X. Sun , W. Liang , D. Sun , and Z. Xia . “CADS: Co-operative anti-fraud data storage scheme for unattended wireless sensor networks”. Inform. Technol. J. 9, 1361–1368, 2010.

W. Ren , J. Zhao , and Y. Ren . “MSS: A multi-level data placement scheme for data survival in wireless sensor networks”. Fifth International Conference on Wireless Communications, Networking and Mobile Computing, IEEE, 2009.

V. Erceg , L. Greenstein , S. Tjandra , S. Parkoff , A. Gupta , B. Kulic , A. A. Julius , and R. Bianchi . “An empirically based path loss model for wireless channels in suburban environments”. IEEE Journal on Selected Areas in Communications 17(7), 1205–1211, 1999.

A. Goldsmith . Wireless Communications. Cambridge University Press, 2005.

F. Owen and C. Pudney . “Radio propagation for digital cordless telephones at 1700 MHz and 900 MHz”. IEEE Electronics Letters 25(1), 52–53, 1989.

T. Rappaport . Wireless Communications—Principles and Practice, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 2001.

S. Seidel , T. Rappaport , S. Jain , M. Lord , and R. Singh . “Path loss, scattering, and multipath delay statistics in four European cities for digital cellular and microcellular radiotelephone”. IEEE Transactions on Vehicular Technology 40(4), 721–730, 1991.

A. F. De Toledo , and A. M. D. Turkmani . “Propagation into and within buildings at 900, 1800, and 2300 MHz”. In: Proc. on IEEE Vehicular Technology Conference (VTC), 633–636, 1992.

A. F. De Toledo , A. M. D. Turkmani , and J. D. Parsons . “Estimating coverage of radio transmission into and within buildings at 900, 1800, and 2300 MHz”. IEEE Personal Communications Magazine 5(2), 40–47, 1998.

T. S. Rappaport . Wireless Communications. Chaps. 3 and 4. Upper Saddle River, NJ: Prentice-Hall, 1996.

J. Garg , K. Gupta , and P. K. Ghosh . “Performance analysis of MIMO wireless communications over fading channels—A review”. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2(4), Apr. 2013.

J. B. Andersen , T. S. Rappaport , and S. Yoshida . “Propagation measurements and models for wireless communications channels”. IEEE Communications Magazine, 42–49, Jan. 1995.

P. M. Shankar . Introduction to Wireless Systems. John Wiley & Sons, 2002.

A. Sendonan , E. Erkip , and B. Hahang . “User cooperation diversity techniques. Part 1, System description”. IEEE Transactions on Communications, 51(11), 1927–1938, Nov. 2003.

Y. Sitti . “Error performance analysis of cooperative systems with receiver diversity: Effect of shadowing in source–destination link”. Signal Processing and Communications Applications (SIU), 2011 IEEE 19th Conference, pp. 482–485, 20–22 Apr. 2011.

A. Singh . “Cooperative spectrum sensing in multiple antenna based cognitive radio network using an improved energy detector”. IEEE Communications Letters 16(1), 64–67, Jan. 2012.

Y. Nasser . “Effect of mobility on the performance of amplify-and-forward cooperation in SC-FDMA systems”. Computing, Networking and Communications (ICNC), 2012 International Conference, pp. 798–803, Jan. 30 2012–Feb. 2 2012.

L. Zheng and D. N. C. Tse . “Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels”. IEEE Transactions on Information Theory 49(5), 1073–1096, May 2003.

M. Jankiraman . Space–Time Codes and MIMO Systems. Artech House, 2004.

B. Vucetic and J. Yuan . Space–Time Coding. John Wiley, 2003.

D. Gesbert , M. Shafi , D. Shiu , P. J. Smith , and A. Naguib . “From theory to practice: An overview of MIMO space–time coded wireless systems”. IEEE Journal on Selected Areas in Communications. 21(3), 281–301, Apr. 2003.

L. Zheng and D. N. Tse . “Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels”. IEEE Transactions on Information Theory 49(5), 1073–1096, May 2003.

E. C. der Meulen . “Three-terminal communication channels”. Advances in Applied Probability 3(1), 120–154, 1971.

T. M. Cover and A. A. E. Gamal . “Capacity theorems for the relay channel”. IEEE Transactions on Information Theory 25(5), 572–584, Sept. 1979.

K. J. Rayliu , A. K. Sadek , Weifengsu , and Andres Kwasinski . Cooperative Communications and Networking. Cambridge University Press, ISBN- 13 978-0-511-46548-2, 2009.

J. N. Laneman , G. W. Wornell , and D. N. C. Tse . “An efficient protocol for realizing cooperative diversity in wireless networks”. Proc. IEEE ISIT, Washington, DC, p. 294, June 2001.

A. Sendonaris , E. Erkip , and B. Aazhang . “User cooperation diversity part I and part II”. IEEE Transactions on Communications 51(11), 1927–1948, Nov. 2003.

A. Wyner and J. Ziv . “The rate-distortion function for source coding with side information at the decoder”. IEEE Transactions on Information Theory 22(1), 1–10, Jan. 1976.
T. E. Hunter and A. Nosratinia . “Cooperative diversity through coding”. In: Proc. IEEE International Symposium Information Theory (ISIT), Laussane, Switzerland, p. 220, Jul. 2002.
A. Stefanov and E. Erkip . “Cooperative coding for wireless networks”. IEEE Transactions on Communications 52(9), 1470–1476, Sept. 2004.
T. E. Hunter and A. Nosratinia . “Diversity through coded cooperation”. IEEE Transactions on Wireless Communications 5(2), 283–289, Feb. 2006.
W. Su and X. Liu . “On optimum selection relaying protocols in cooperative wireless networks”. IEEE Transactions on Communications 58(1), 52–57, Jan. 2010.
J. N. Laneman , D. N. C. Tse , and G. W. Wornell . “Cooperative diversity in wireless networks: Efficient protocols and outage behavior”. IEEE Transactions on Information Theory 50(12), 3062–3080, 2004.
S. S. Ikki and M. H. Ahmed . “Performance analysis of decode-and-forward incremental relaying cooperative diversity networks over Rayleigh fading channels”. Vehicular Technology Conference, 2009.
S. S. Ikki and M. H. Ahmed . “Performance analysis of incremental-relaying cooperative-diversity networks over Rayleigh fading channels”. IET Communications 5(3), 337–349, Feb. 2011.
A. H. Bastami and A. Olifat . “Optimal incremental relaying in cooperative diversity systems”. IET Communications 7(2), 152–168, Jan. 2013.
Q. Zhou and F. Lau . “Two incremental relaying protocols for cooperative networks”. IET Communications 2(10), 1272–1278, Nov. 2008.
H. Long , K. Zheng , W. Wang , and F. Wang . “Approximate performance analysis of the incremental relaying protocol and modification”. In: Proc. IEEE 70th VTC-Fall, Anchorage, AK, USA, pp. 1–5, Sep. 2009.
J. Kuang , C. Hu , H. Long , K. Zheng , and W. Wang . “Selective fractional incremental relaying protocol in cooperative systems”. International Conference on Communications, Circuits and Systems (ICCCAS), 2010.
M. M. Fareed , M.-S. Alouini , and H.-C. Yang . “Efficient incremental relaying for packet transmission over fading channels”. IEEE Transactions on Wireless Communications 13(7), 3609–3620, Jul. 2014.
E. Beres and R. Adve “Selection cooperation in multi-source cooperative net- works”. IEEE Transactions on Wireless Communications, vol. 7, pp. 118–127, Jan. 2008.
A. Bletsas , A. Khisti , D. Reed , and A. Lippman . “A simple cooperative diversity method based on network path selection”. IEEE Journal on Selected Areas in Communications 24, 659–672, Mar. 2006.
A. Bletsas , A. Khisti , and M. Win . “Cooperative communications with outage-optimal opportunistic relaying”. IEEE Transactions on Wireless Communications 6(9), 3450–3460, Sept. 2007.
A. Adinoyi , Y. Fan , H. Yanikomeroglu , and V. Poor . “On the performance of selective relaying”. In: Proc. IEEE Vehicular Technology Conference (VTC) Fall, Sept. 2008.
A. S. Ibrahim , A. K. Sadek , W. Su , and K. J. Liu . “Cooperative communications with relay selection: When to cooperate and whom to cooperate with”. IEEE Transactions on Wireless Communications 7(7), 2814–2827, Jul. 2008.
E. Beres and R. Adve . “Selection cooperation in multi-source cooperative networks”. IEEE Transactions on Wireless Communications 7, 118–127, Jan. 2008.
C.-K. Toh . Ad Hoc Wireless Networks: Protocols and Systems. Prentice Hall Publishers, 2002.
C. Siva Ram Murthy and B. S. Manoj . Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, May 2004.
H. Ilhan , I. Altunbas , and M. Uysal . “Performance analysis and optimization of relay-assisted vehicleto-vehicle (v2v) cooperative communication”. In: Signal Processing, Communication and Applications Conference, 2008. SIU 2008. IEEE 16th, pp. 1–4, Apr. 20–22, 2008.
J. Santa , A. Moragon , and A. F. Gomez-Skarmeta . “Experimental evaluation of a novel vehicular communication paradigm based on cellular networks”. In: Intelligent Vehicles Symposium, 2008 IEEE, pp. 198–203, Jun. 4–6, 2008.
M. L. Sichitiu and M. Kihl . “Inter-vehicle communication systems: A survey”. IEEE Communications Surveys & Tutorials 10, 88–105, second quarter 2008.

Y. Zou , J. Zhu , B. Zheng , and Y.-D. Yao . “An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks”. IEEE Transactions on Signal Processing 58(10), Oct. 2010.
Y. Zou , B. Zheng , and Y.-D. Yao . “Outage probability analysis of cognitive transmissions: Impact of spectrum sensing overhead”. IEEE Transactions on Wireless Communications 9(8), 2676–2688, June 2010.
E. Peh and Y. C. Liang . “Optimization for co-operative sensing in cognitive radio networks”. IEEE Wireless Communications and Networking Conference, pp. 27–32, Mar. 2007.
A. Nosratinia , T. E. Hunter , and A. Hedayat . “Cooperative communication in wireless networks”. IEEE Communications Magazine 42(10), 74–80, 2004.
M. Dohler , Y. Li . Cooperative Communications Hardware, Channel & Phy. John Wiley & Sons, ISBN 978-0-470-99768-0, 2010.
J. L. Massey . “An introduction to contemporary cryptology”. Proc. IEEE 76(5), 533–549, May 1988.
G. Kapoor and S. Piramithu . “Vulnerabilities in some recently proposed RFID ownership transfer protocols”. IEEE Communications Letters 14(3), 260–262, Mar. 2010.
A. Barenghi , L. Breveglieri , I. Koren , and D. Naccache . “Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures”. Proc. IEEE 100(11), 3056–3076, Nov. 2012.
X. Zhou , L. Song , and Y. Zhang , Eds. Physical Layer Security in Wireless Communications. CRC Press, 2013.
M. Bloch and J. Barros . Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.
E. Jorswieck , A. Wolf , and S. Gerbracht . Secrecy on the Physical Layer in Wireless Networks. In-Tech Publishers, 2010.
R. Liu and W. Trappe . Securing Wireless Communications at the Physical Layer. Norwell, MA: Springer, 2009.
C. E. Shannon . “Communication theory of secrecy systems”. The Bell System Technical Journal 28(4), 656–715, Oct. 1949.
A. D. Wyner . “The wire-tap channel”. The Bell System Technical Journal 54(8), 1355–1387, Jan. 1975.
I. Csiszár and J. Körner . “Broadcast channels with confidential messages”. IEEE Transactions on Information Theory IT-24(3), 339–348, May 1978.
S. K. Leung-Yan-Cheong and M. E. Hellman . “The Gaussian wire-tap channel”. IEEE Transactions on Information Theory IT-24(4), 451–456, Jul. 1978.
E. Tekin and A. Yener . “Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy”. In: Proc. 44th Annu. Allerton Conf. Commun. Contr. Comput. 2006.
E. Tekin and A. Yener . “The multiple access wire-tap channel: Wireless secrecy and cooperative jamming”. In: Proc. Information Theory and Applications Workshop, 2007.
E. Tekin and A. Yener . “The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming”. IEEE Transactions on Information Theory 54(6), 2735–2751, Jun. 2008.
E. Tekin and A. Yener . “The Gaussian multiple access wire-tap channel”. IEEE Transactions on Information Theory 54(12), 5747–5755, Dec. 2008.
L. Lai and H. El Gamal . “The relay-eavesdropper channel: Cooperation form secrecy”. IEEE Transactions on Information Theory 54(9), 4005–4019, Sept. 2008.
R. Bassily and S. Ulukus . “Deaf cooperation and relay selection strategies for secure communication in multiple relay networks”. IEEE Transactions on Signal Processing 61(6), 1544–1554, Mar. 2013.
E. Ekrem and S. Ulukus . “Cooperative secrecy in wireless communications”. In: Securing Wireless Communications at the Physical Layer, W. Trappe and R. Liu , Eds. New York: Springer-Verlag, pp. 143–172, 2009.
X. Tang , R. Liu , P. Spasojevic , and H. V. Poor . “The Gaussian wiretap channel with a helping interferer”. In: Proc. IEEE Int. Symp. Inf. Theory, Toronto, ON, Canada, pp. 389–393, Jul. 2008.
X. He and A. Yener . “Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels”. IEEE Transactions on Information Theory 60(4), 2121–2138, 2014.

X. He and A. Yener . “Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling”. In: Proc. IEEE Global Telecommun. Conf., 2009.

X. He . Cooperation and Information Theoretic Security in Wireless Networks. PhD Dissertation, Dept. Electr. Eng., Pennsylvania State Univ., State College, PA, USA, 2010.

O. O. Koyluoglu , H. E. Gamal , L. Lai , and H. V. Poor . “Interference alignment for secrecy”. IEEE Transactions on Information Theory 57(6), 3323–3332, Jun. 2011.

A. S. Motahari , S. Oveis-Gharan , M. A. Maddah-Ali , and A. K. Khandani . “Real interference alignment: Exploiting the potential of single antenna systems”. IEEE Transactions on Information Theory 60(8), 4799–4810, 2014.

I. Krikidis , J. Thompson , and S. McLaughlin . “Relay selection for secure cooperative networks with jamming”. IEEE Transactions on Wireless Communications 8(10), 5003–5011, Oct. 2009.

D. H. Ibrahim , E. S. Hassan , and S. A. El-Dolil . “A new relay and jammer selection schemes for secure one-way cooperative networks”. Wireless Personal Commu. 72(2), doi: 10.1007/s11277-013-1384-5, 2013.

R. Bassily and S. Ulukus . “Deaf cooperation and relay selection strategies for secure communication in multiple relay networks”. IEEE Transactions on Signal Processing 61(6), 1544–1554, Mar. 2013.

D. H. Ibrahim , E. S. Hassan , and S. A. El-Dolil . “Improving physical layer security in two-way cooperative networks with multiple eavesdroppers”. Proc. of IEEE INFOS, Egypt, 2014.

D. H. Ibrahim , E. S. Hassan , and S. A. El-Dolil . “Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks”. Computers & Security Journal 50, 47–59, 2015.

R. Bassily and S. Ulukus . “Secure communication in multiple relay networks through decode-and-forward strategies”. Journal of Communications and Networks 14(4), 352–363, Aug. 2012.

Y. Oohama . “Coding for relay channels with confidential messages”. In: Proc. IEEE Information Theory Workshop (ITW), Cairns, Australia, pp. 87–89, 2001.

X. He and A. Yener . “Cooperation with an untrusted relay: A secrecy perspective”. IEEE Transactions on Information Theory 56(8), 3807–3827, Aug. 2010.

X. He and A. Yener . “Two-hop secure communication using an untrusted relay”. EURASIP J. Wireless Commun. Network., 2009.

X. He and A. Yener . “Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay”. IEEE Transactions on Information Theory 59(1), 177–192, Jan. 2013.

Y. Liang and H. V. Poor . “Multiple access channels with confidential messages”. IEEE Transactions on Information Theory. 54(3), 976–1002, Mar. 2008.

R. Liu , I. Maric , R. D. Yates , and P. Spasojevic . “The discrete memoryless multiple access channel with confidential messages”. In: Proc. IEEE Int. Symp. Information Theory, 2006.

E. Ekrem and S. Ulukus . “Effects of cooperation on the secrecy of multiple access channels with generalized feedback”. In: Proc. Conf. Information Sciences Systems, 2008.

E. Ekrem and S. Ulukus . “Secrecy in cooperative relay broadcast channels”. IEEE Transactions on Information Theory 57(1), 137–155, Jan. 2011.

E. D. Silva , A. L. D. Santos , L. C. P. Albini , and M. Lima . “Identity-based key management in mobile ad hoc networks: Schemes and applications”. IEEE Wireless Communication 15, 46–52, Oct. 2008.

R. Liu , I. Maric , P. Spasojevic , and R. D. Yates . “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions”. IEEE Transactions on Information Theory 54, 2493–2507, Jun. 2008.

M. Bloch , J. Barros , M. R. D. Rodrigues , and S. W. McLaughlin . “Wireless information-theoretic security”. IEEE Transactions on Information Theory 54, 2515–2534, June 2008.

J. Barros and M. R. D. Rodrigues . “Secrecy capacity of wireless channels”. Proc. IEEE Int. Symp. Inf. Theory, Seattle, USA, pp. 356–360, July 2006.

Y. Liang , H. V. Poor , and L. Ying . “Wireless broadcast networks: Reliability, security, and stability”. Proc. IEEE Inf. Theory Appl. Work, San Diego, CA, USA, pp. 249–255, Feb. 2008.

L. Dong , Z. Han , A. P. Petropulu , and H. V. Poor . “Secure wireless communications via cooperation”. Proc. Allerton Conf. Commun. Cont. Comp., Urbana-Champaign, IL, USA, Sept. 2008.

S. Yang and J.-C. Belfiore . “Towards the optimal amplify-and-forward cooperative diversity scheme”. IEEE Transactions on Information Theory 53, 3114–3126, Sept. 2007.

L. Dong , Z. Han , A. Petropulu , and H. V. Poor . “Improving wireless physical layer security via cooperating relays”. IEEE Transactions on Signal Processing 58, 1875–1888, Mar. 2010.
L. Lai and H. El Gamal . “The relay–eavesdropper channel: Cooperation for secrecy”. IEEE Transactions on Information Theory 54, 4005–4019, Sept. 2008.
I. Krikidis . “Opportunistic relay selection for cooperative networks with secrecy constraints”. IET Communications 4, 1787–1791, 2010.
E. Beres and R. Adve . “Selection cooperation in multi-source cooperative networks”. IEEE Transactions on Wireless Communications 7, 118–127, Jan. 2008.
O. Simeone and P. Popovski . “Secure communications via cooperating base stations”. IEEE Communications Letter 12, 188–190, Mar. 2008.
P. Popovski and O. Simeone . “Wireless secrecy in cellular systems with infrastructure-aided cooperation”. IEEE Transactions on Information Forensics and Security 4, 242–256, Jun. 2009.
T. Wang and G. B. Giannakis . “Mutual information jammer-relay games”. IEEE Transactions on Information Forensics and Security 3, 290–303, Jun. 2008.
E. S. Hassan . “Energy-efficient hybrid opportunistic cooperative protocol for single-carrier frequency division multiple access-based networks”. IET Communications 6(16), 2602–2612, 2012.
A. Y. Al-nahari , I. Krikidis , A. S. Ibrahim , M. I. Dessouky , and F. E. Abd El-Samie . “Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers”. Transactions on Emerging Telecommunications Technologies, doi: 10.1002/ett.2581, Nov. 2012.
Y. Liang , H. V. Poor , and S. Shamai . “Secure communication over fading channels”. IEEE Transactions on Information Theory 54(6), 2470–2492, Jun. 2008.
L. Dong , Z. Han , A. P. Petropulu , and H. V. Poor . “Amplify-and forward based cooperation for secure wireless communications”. In: Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Taipei, Taiwan, Apr. 2009.
B. Rankov and A. Wittneben . “Achievable rate regions for the two-way relay channel”. In: Proc. IEEE Int. Symp. Information Theory, Seattle, WA, Jul. 2006.
B. Rankov and A. Wittneben . “Spectral efficient protocols for half duplex fading relay channels”. IEEE Journal on Selected Areas in Communications 25(2), 379–389, Feb. 2007.
J. Chen , R. Zhang , L. Song , Z. Han , and B. Jiao . “Joint relay and jammer selection for secure decode-and-forward two-way relay networks”. In: Proc. of Communications (ICC), IEEE International Conference, 2011.
N. Zhou , X. Chen , C. Li , and Q. Lai . “Relay selection for physical layer security in decode-and-forward two-way relay networks”. Journal of Information & Computational Science, doi: 10.12733/jics20102372, 5821–5828, Dec. 2013.
J. Chen , R. Zhang , L. Song , Z. Han , and B. Jiao . “Joint relay and jammer selection for secure two-way relay networks”. IEEE Transactions on Information Forensics and Security 7(1), 310–320, Feb. 2012.
I. F. Akyildiz , W. Su , Y. Sankarasubramaniam , and Cayirci, E. “Wireless sensor networks: A survey”. Computer Networks 38(4), 393–422, 2002.
K. Al Agha , M.-H. Bertin , T. Dang , A. Guitton , P. Minet , T. Val , and J.-B. Viollet . “Which wireless technology for industrial wireless sensor networks? The development of OCARI technology”. IEEE Transactions on Industrial Electronics 56(10), 4266–4278, 2009.
M. S. Mahmoud and Y. Xia . Networked Filtering and Fusion in Wireless Sensor Networks. CRC Press, 2014.
J. Yick , B. Mukherjee , and D. Ghosal . “Wireless sensor network survey”. Computer Networks 52, 2292–2330, 2008.
S. Toumpis and T. Tassiulas . “Optimal deployment of large wireless sensor networks”. IEEE Transactions on Information Theory 52, 2935–2953, 2006.
J. Yick , G. Pasternack , B. Mukherjee , and D. Ghosal . “Placement of network services in sensor networks”. Int. J. Wireless and Mobile Computing (IJWMC), Self-Organization Routing and Information, Integration in Wire-less Sensor Networks (Special Issue) 1, 101–112, 2006.
D. Pompili , T. Melodia , and I. F. Akyildiz . “Deployment analysis in underwater acoustic wireless sensor networks”. WUWNet, Los Angeles, CA, 2006.
I. F. Akyildiz and E. P. Stuntebeck . “Wireless underground sensor networks: Research challenges”. Ad-Hoc Networks 4, 669–686, 2006.

M. Li and Y. Liu . “Underground structure monitoring with wireless sensor networks”. Proc. the IPSN, Cambridge, MA, 2007.
I. F. Akyildiz , D. Pompili , and T. Melodia . “Challenges for efficient communication in underwater acoustic sensor networks”. ACM Sigbed Review 1(2), 3–8, 2004.
J. Heidemann , Y. Li , A. Syed , J. Wills , and W. Ye . “Underwater sensor networking: Research challenges and potential applications”. Proc. the Technical Report, USC/Information Sciences Institute, 2005.
I. F. Akyildiz , T. Melodia , and K. R. Chowdhury . “A survey on wireless multi-media sensor networks”. Computer Networks 51, 921–960, 2007.
D. Estrin , R. Govindan , J. Heidemann , and S. Kumar . “Next century challenges: Scalable coordination in sensor networks”. ACM MobiCom’99, Washington, USA, pp. 263–270, 1999.
B. Atwood , B. Warneke , and K. S. J. Pister . “Preliminary circuits for smart dust”. Proc. Southwest Symp. Mixed-Signal Design, pp. 87–92, 2000.
R. Sharma and N. T. S. Kumar . “Review paper on wireless sensor networks”. In: Proc. of the Intl. Conf. on Recent Trends in Computing and Communication Engineering, (RTCCE), pp. 978–981, 2013.
N. Bulusu , D. Estrin , L. Girod , and J. Heidemann . “Scalable coordination for wireless sensor networks: Self-configuring localization systems”. International Symposium on Communication Theory and Applications (ISCTA 2001), Ambleside, UK, Jul. 2001.
J. M. Kahn , R. H. Katz , and K. S. J. Pister . “Next century challenges: Mobile networking for smart dust”. Proc. of the ACM MobiCom’99, Washington, USA, pp. 271–278, 1999.
Y. H. Nam et al. “Development of remote diagnosis system integrating digital telemetry for medicine”. International Conference IEEE-EMBS, Hong Kong, pp. 1170–1173, 1998.
N. Noury , T. Herve , V. Rialle , G. Virone , E. Mercier , G. Morey , A. Moro , and T. Porcheron . “Monitoring behavior in home using a smart fall sensor”. IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology, pp. 607–610, Oct. 2000.
B. Sibbald . “Use computerized systems to cut adverse drug events: Report”. CMAJ: Canadian Medical Association Journal 164(13), 1878–1878, 2001.
E. M. Petriu , N. D. Georganas , D. C. Petriu , D. Makrakis , and V. Z. Groza . “Sensor based information appliances”. IEEE Instrumentation and Measurement Magazine, 31–35, Dec. 2000.
C. Herring and S. Kaplan . “Component-based software systems for smart environments”. IEEE Personal Communications, 60–61, Oct. 2000.
J. M. Rabaey , M. J. Ammer , J. L. da Silva Jr. , D. Patel , and S. Roundy . “Pico radio supports ad hoc ultra-low power wireless networking”. IEEE Computer Magazine, 42–48, 2000.
G. J. Pottie , W. J. Kaiser . “Wireless integrated network sensors”. Communications of the ACM 43(5), 551–558, 2000.
E. Shih , S. Cho , N. Ickes , R. Min , A. Sinha , A. Wang , and A. Chandrakasan . “Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks”. Proc. of ACM MobiCom’01, Rome, Italy, pp. 272–286, Jul. 2001.
G. Hoblos , M. Staroswiecki , and A. Aitouche . “Optimal design of fault tolerant sensor networks”. IEEE International Conference on Control Applications, Anchorage, AK, pp. 467–472, Sept. 2000.
J. Rabaey , J. Ammer , J. L. da Silva Jr. , and D. Patel . “Pico-radio: Ad-hoc wireless networking of ubiquitous low-energy sensor monitor nodes”. Proc. of the IEEE Computer Society Annual Workshop on VLSI (WVLSI’00), Orlando, Florida, pp. 9–12, Apr. 2000.
C. Intanagonwiwat , R. Govindan , and D. Estrin . “Directed diffusion: A scalable and robust communication paradigm for sensor networks”. Proc. of the ACM Mobi-Com’00, Boston, MA, pp. 56–67, 2000.
L. Li and J. Y. Halpern . “Minimum-energy mobile wireless networks revisited”. IEEE International Conference on Communications ICC’01, Helsinki, Finland, Jun. 2001.
A. Savvides , C. Han , and M. Srivastava . “Dynamic fine-grained localization in ad-hoc networks of sensors”. Proc. of ACM MobiCom’01, Rome, Italy, pp. 166–179, Jul. 2001.
W. Du , R. Wang , and P. Ning . “An efficient scheme for authenticating public keys in sensor networks”. Proc. of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM, 2005.
A. S. Wander , N. Gura , H. Eberle , V. Gupta , and S. C. Shantz . “Energy analysis of public-key cryptography for wireless sensor networks”. In: Third IEEE International Conference on Pervasive Computing and Communications, pp. 324–328, Mar. 2005.

K. Ren , W. Lou , K. Zeng , and P. J. Moran . “On broadcast authentication in wireless sensor networks”. IEEE Transactions on Wireless Communications 6(11), 4136–4144, 2007.
K. C. Barr and K. Asanović . “Energy-aware lossless data compression”. ACM Transactions on Computer Systems (TOCS) 24.3, 250–291, 2006.
Texas Instruments Inc ., “Msp430 Family of Ultra-low power 16-bit RISC Processors”, http://www.ti.com. Accessed Nov. 2, 2012.
D. Ma , C. Soriente , and G. Tsudik . “New adversary and new threats: Security in unattended sensor networks”. IEEE Network, Mar. 2009.
D. Ma and G. Tsudik . “Security and privacy in emerging wireless networks”. IEEE Wireless Communications, Special Issue on Security and Privacy in Emerging Wireless Networks, 2010.
R. Ostrovsky and M. Yung . “How to withstand mobile virus attacks”. In: Proc. of the Tenth Annual ACM Symposium on Principles of Distributed Computing, ACM, pp. 51–59, July 1991.
Y. Frankel , P. Gemmell , P. D. MacKenzie , and M. Yung . “Proactive RSA”. In: Annual International Cryptology Conference, Springer Berlin Heidelberg, pp. 440–454, August 1997.
T. Rabin . “A simplified approach to threshold and proactive RSA”. In: Annual International Cryptology Conference, Springer Berlin Heidelberg, pp. 89–104, Aug. 1998.
R. Gennaro , S. Jarecki , H. Krawczyk , and T. Rabin . “Robust and efficient sharing of RSA functions”. In: Proc. Annual Int. Cryptology Conference (CRYPTO), pp. 157–172, 1996.
R. Gennaro , S. Jarecki , H. Krawczyk , and T. Rabin . “Robust threshold DSS signatures”. In: International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 354–371, May 1996.
D. Ma and G. Tsudik . “DISH: Distributed self-healing in unattended sensor networks”, Proc. of SSS ‘08, Detroit, MI, USA, pp. 47–62, Nov. 2008.
S. Basagni , K. Herrin , D. Bruschi , and E. Rosti . “Secure pebblenets”. Proc. of ACM International Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, CA, pp. 156–163, Oct. 2001.
C. Karlof and D. Wagner . “Secure routing in wireless sensor networks: Attacks and countermeasures”. Ad Hoc Networks 1(2), 293–315, 2003.
X. Chen , K. Makki , K. Yen , and N. Pissinou . “Sensor network security: A survey”. IEEE Communications Surveys & Tutorials 11(2), 52–73, 2009.
P. Turaga and Y. A. Ivanov . “Diamond sentry: Integrating sensors and cameras for real-time monitoring of indoor spaces”. IEEE Sensors Journal 11(3), 593–602, Mar. 2011.
W. Jang , W. M. Healy , and M. J. Skibniewski . “Wireless sensor networks as a part of a web-based building environmental monitoring system”. Automation in Construction 17(6), 729–736, Aug. 2008.
Z. Sun , P. Wang , M. C. Vuran , M. A. Al-Rodhaan , A. M. Al-Dhelaan , and I. F. Akyildiz . “Border sense: Border patrol through advanced wireless sensor networks”. Ad Hoc Networks 9, 468–477, 2011.
M. Clure , D. R. Corbett , and D. W. Gage . “The DARPA LANdroids program”. Defense Advanced Research Projects Agency (DARPA). In: Unmanned Systems Technology XI, Orlando, FL. SPIE Proceedings 7332, Apr. 2009.
W. Lou , W. Liu , and Y. Fang . “SPREAD: Enhancing data confidentiality in mobile ad hoc networks”. Proc. IEEE INFOCOM ‘04, Hong Kong, pp. 2404–2413, Mar. 2004.
R. D. Pietro , D. Ma , C. Soriente , and G. Tsudik . “Self-healing in unattended wireless sensor networks”. ACM Transactions on Sensor Network, Article 39, 19 pages, Mar. 2010.
A. Kamra , V. Misra , J. Feldman , and D. Rubenstein . “Growth codes: Maximizing sensor network data persistence”. Proc. of SIGCOMM ‘06, New York: ACM, pp. 255–266, 2006.
V. Gianuzzi . “Data replication effectiveness in mobile ad-hoc networks”. Proc. of PE-WASUN ‘04, New York: ACM, pp. 17–22, 2004.
C. Chen and Y. Tsai . “Location privacy in unattended wireless sensor networks upon the requirement of data survivability”. IEEE Journal on Selected Areas in Communications 29(7), 1480–1490, 2011.
P. Kamat , Y. Zhang , W. Trappe , and C. Ozturk . “Enhancing source location privacy in sensor network routing”. Proc. IEEE ICDCS 2005, Columbus, Ohio, USA, pp. 599–608, Jun. 2005.
K. Mehta , D. Liu , and M. Wright . “Location privacy in sensor networks against a global eavesdropper”. Proc. IEEE ICNP 2007, Beijing, China, pp. 314–323, Oct. 2007.
B. H. Liu , W. C. Ke , C. H. Tsai , and M. J. Tsai . “Constructing a message-pruning tree with minimum cost for tracking moving objects in wireless sensor networks is NB-complete and an

enhanced data aggregation structure". IEEE Transactions on Computers 57(6), 849–863, Jun. 2008.

Y. Ren , V. Oleshchuk , and F. Y. Li . "Optimized secure and reliable distributed data storage scheme and performance evaluation in unattended WSNs". Computer Communications Journal Elsevier (COMCOM), 1–11, Aug. 2012, URL: http://dx.doi.org/10.1016/j.comcom. 2012.08.001.

J. Newsome , E. Shi , D. Song , and A. Perrig . "The sybil attack in sensor networks: Analysis & defenses". Proc. of the 3rd Int. Symposium on Information Processing in Sensor Networks, Berkeley, California, USA, pp. 259–268, 26–27 Apr. 2004.

A. Perrig , J. Stankovic , and D. Wagner . "Security in wireless sensor networks". Magazine Communications of the ACM—Wireless Sensor Networks 47(6), 53–57, 2004.

I. Reed and G. Solomon . "Polynomial codes over certain finite fields". Journal of the Society for Industrial and Applied Mathematics 8(2), 300–304, 1960.

M. Conti , R. D. Pietro , L. V. Mancini , and A. Mei . "Mobility and cooperation to thwart node capture attacks in MANETs". EURASIP Journal on Wireless Communications and Networking, 2009.

A. Becher , E. Becher , Z. Benenson , and M. Dornseif . "Tampering with motes: Real-world physical attacks on wireless sensor networks". In: Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC), pp. 104–118, 2006.

A. S. Elsafrawey , E. S. Hassan , and M. I. Dessouky . "Cooperative hybrid self-healing scheme for secure and data reliability in unattended wireless sensor networks". IET Information Security, doi: 10.1049/iet-ifs.2014.0267, 2015.

A. R. Silva , M. Moghaddam , M. Liu ., "Case study on the reliability of unattended outdoor wireless sensor systems". 9th Annual IEEE International Systems Conference (SysCon), pp. 785–791, 13–16 Apr. 2015.

Y. Ren , V. I. Zadorozhny , V. A. Oleshchuk , and F. Y. Li . "A novel approach to trust management in unattended wireless sensor networks". IEEE Transactions on Mobile Computing 13(7), 1409–1423, 2014.

A. S. Elsafrawey , E. S. Hassan , and M. I. Eldosoki . "A new cooperative hybrid self-healing scheme for secure and data reliability in UWSNs". Proc. of the 30th National Radio Science Conference (30th NRSC), NTI, Cairo, Egypt, 15–16 April 2013.

M. Batalin , M. Rahimi , Y. Yu , D. Liu , A. Kansal , G. Sukhatme , W. Kaiser , M. Hansen , G. J Pottie , M. Srivastava , and D. Estrin . "Call and response: Experiments in sampling the environment". Proc. of 2nd Annual Conference on Sensors and Systems, Baltimore, MD, USA, Nov. 2004.

M. H. Rahimi , H. Shah , G. S. Sukhatme , J. Heidemann , and D. Estrin . "Studying the feasibility of energy harvesting in mobile sensor networks". Proc. of the IEEE International Conference on Robotics and Automation, Taipei, Taiwan, Sept. 2003.

T. Camp , J. Boleng , and V. Davies . "A survey of mobility models for ad hoc network research". Wireless Communications & Mobile Computing (WCMC): Special Issue on Mobile Ad Hoc Networking: Research, Trends and Applications 2(5), 483–502, 2002.

S. Batabyal and P. Bhaumik . "Mobility models, traces and impact of mobility on opportunistic routing algorithms: A survey". IEEE Communications Surveys & Tutorials 17(3), 1679–1707, 2015.

S. Madi and H. Al-Qamzi . "A survey on realistic mobility models for vehicular ad hoc networks (VANETs)". 10th IEEE International Conference on Networking, Sensing and Control (ICNSC), pp. 333–339, 2013.

A. S. Elsafrawey , E. S. Hassan , and M. I. Dessouky . "Improving UWSNs security and data reliability using a cluster controlled mobility scheme". Proc. of IEEE INFOS, Egypt, 2014.

A. S. Elsafrawey , E. S. Hassan , and M. I. Dessouky . "Analytical analysis of a cluster controlled mobility scheme for data security and reliability in UWSNs". Proc. of NRSC, 2015.

A. Howard , M. Mataric , and G. S. Sukhatme . "An incremental self-deployment algorithm for mobile sensor networks". Autonomous Robots-Special Issue on Intelligent Embedded Systems 13(2), 113–126, 2002.

S. Poduri and G. Sukhatme . "Constrained coverage for mobile sensor networks". Proc. of the IEEE International Conference on Robotics and Automation, April 2004.

R. D. Pietro , G. Oligeri , C. Soriente , and G. Tsudik . "United we stand: Intrusion-resilience in mobile unattended WSNs". IEEE Transactions Mobile Computing (TMC) 12(7), 1456–1468, 2013.

R. D. Pietro , G. Oligeri , C. Soriente , and G. Tsudik . “Intrusion-resilience in mobile unattended WSNs”. Proc. of 29th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM’10), pp. 2303–2311, 2010.
T. Iida , K. Emura , A. Miyaji , and K. Omote . “An intrusion and random-number-leakage resilient scheme in mobile unattended WSNs”. Advanced Information Networking and Applications Workshops (WAINA), 26th International Conference on. IEEE, 2012.
B. Liu , P. Brass , O. Dousse , P. Nain , and D. F. Towsley . “Mobility improves coverage of sensor networks”. In: 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc’05), pp. 300–308, 2005.
G. Wang , G. Cao , T. F. L. Porta , and W. Zhang . “Sensor relocation in mobile sensor networks”. In: 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM’05), pp. 2302–2312, 2005.
R. Dutta , Y. D. Wu , and S. Mukhopadhyay . “Constant storage self-healing key distribution with revocation in wireless sensor network”. In: IEEE International Conference on Communications (ICC’07), pp. 1323–1328, 2007.
F. Sivrikaya and B. Yener . “Time synchronization in sensor networks: A survey”. IEEE Network 18(4), 45–50, 2004.
E. Kiesling , C. Strauss , A. Ekelhart , B. Grill , and C. Stummer . “Simulation-based optimization of information security controls: An adversary-centric approach”. Simulation Conference (WSC), pp. 2054–2065, 2013.
W. Z. Khan , M. Y. Aalsalem , and M. N. M. Saad . “Detection of masked replication attack in wireless sensor networks”. 8th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6, 2013.
C. Tang and P. K. McKinley . “Energy optimization under informed mobility”. IEEE Transaction on Parallel and Distributed Systems 17(9), 947–962, 2006.
Z. Pala , K. Bicakci , and M. Turk . “Effects of node mobility on energy balancing in wireless networks”. Computers & Electrical Engineering 41, 314–324, 2015.
Y. Yan and Y. Mostofi . “Utilizing mobility to minimize the total communication and motion energy consumption of a robotic operation”. IFAC Proceedings 45(26), 180–185, 2012.
D. K. Goldenberg et al. “Towards mobility as a network control primitive”. Proc. of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM, pp. 163–174, 2004.
M. Grossglauser and D. N. C. Tse . “Mobility increases the capacity of ad hoc wireless networks”. IEEE/ACM Transactions on Networking 10(4), 477–486, 2002.
S. A. Jafar . “Too much mobility limits the capacity of wireless ad hoc networks”. IEEE Transactions on Information Theory 51(11), 3954–3965, 2005.
M. Schwager , J. McLurkin , J. J. E. Slotine , and D. Rus . “From theory to practice: Distributed coverage control experiments with groups of robots”. Springer Tracts in Advanced Robotics 54, 127–136, Mar. 2009.
Q. Wang , X. Wang , and X. Lin . “Mobility increases the connectivity of k-hop clustered wireless networks”. Proc. of the 15th Annual International Conference on Mobile Computing and Networking, (MOBICOM), pp. 121–131, 2009.
S. Čapkun , J.-P. Hubaux , and L. Buttyán . “Mobility helps security in ad hoc networks”. Proc. of the Fourth ACM International Symposium on Mobile Ad Hoc Networking & Computing, ACM, pp. 46–56, 2003.
A. T. Hoang and M. Motani . “Exploiting wireless broadcast in spatially correlated sensor networks”. IEEE International Conference on Communications (ICC 2005), vol. 4, 2005.
C. C. Ooi and C. Schindelhauer . “Minimal energy path planning for wireless robots”. Mobile Networks and Applications 14(3), 309–321, 2009.
J. Bachrach and C. Taylor . “Localization in sensor networks”. Handbook of Sensor Networks: Algorithms and Architectures, 2005.
K. Römer , P. Blum , and L. Meier . “Time synchronization and calibration in wireless sensor networks”. Handbook of Sensor Networks. pp. 199–237, Chichester: John Wiley and Sons, 2005.
Y. Mei , Y. H. Lu , Y. C. Hu , and C. G. Lee . “A case study of mobile robot’s energy consumption and conservation techniques”. Proc. of the 12th International Conference on Advanced Robotics and Automation (ICAR’05), pp. 492–497, 2005.

P. A. Tipler . Physics for Scientists and Engineers. Third edition. Worth Publishers, 1991.