



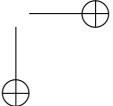
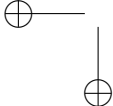
Secure and Reliable Wireless and Ad Hoc Communications

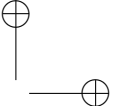
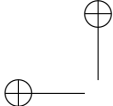
by
Son Thanh Nguyen

Thesis submitted in fulfillment of
the requirements for the degree of
PHILOSOPHIAE DOCTOR
(PhD)



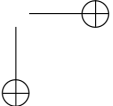
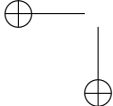
University of Stavanger
Faculty of Science and Technology
2009

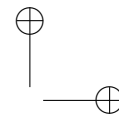
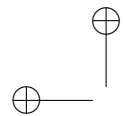




University of Stavanger
N-4036 Stavanger
NORWAY
www.uis.no

ISBN 978-82-7644-390-5
ISSN 1890-1387
©2009 Son Thanh Nguyen





Preface

This thesis is submitted in partial fulfillment for the degree of Philosophy Doctor at the Department of Electrical Engineering and Computer Science, University of Stavanger. The work has been carried out at University of Stavanger during a period from December 2006 to November 2009 under the supervision of Professor Chunming Rong.

This PhD study is funded by the NFR project “Secure and Reliable Wireless and Ad Hoc Communications” (SWACOM) where the author works as a PhD research fellow.

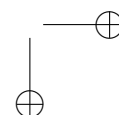
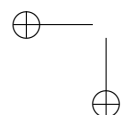
Acknowledgments

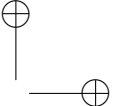

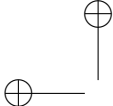
I would like to express my sincere acknowledgment to my advisor, Professor Chunming Rong, for his advices and constant supports through out my research. I do appreciate our stimulating discussions and his insightful advices during my work.

I am indebted to Professor Erdal Cayirci for his guidance and invaluable discussions to complete parts of my PhD work. He has helped me in selecting the research topic and also work together with me in some parts of my PhD work.

My thanks are to Liang Yan, a PhD student at University of Stavanger, for his co-operation during my works. Thanks are also due to Tran Quang Vinh, a PhD student at Shibaura Institute of Technology, for his stimulating discussions. I would also want to thank anonymous reviewers, who have reviewed and given me contributive comments to make my papers better.



I wish to thank University of Stavanger and the Research Council of Norway for their financial supports. I am also grateful to my colleagues at University of Stavanger for making my life and work here fruitful and memorable.

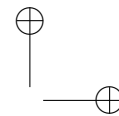
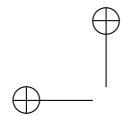




Finally, special thanks to my family and friends for their belief and encouragement during my PhD work.

Son Thanh Nguyen
Stavanger, November 02, 2009.





Executive Summary

Wireless and ad hoc communication systems create additional challenges for the implementation of security and reliability services when compared to fixed networks. On the one hand, the inherent characteristics of wireless environment contribute serious system vulnerabilities if the security requirements are not met. On the other hand, the mobility pattern as well as resource constraints of ad hoc devices make security design more difficult.

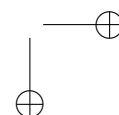
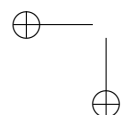
The principal objective of SWACOM project (Secure and Reliable Wireless and Ad Hoc Communications) is to analyze vulnerabilities and develop mechanisms to provide security and reliability in wireless communication networks. A particular focus is on large scale distributed ad hoc networks, which are used in many civilian and military applications.

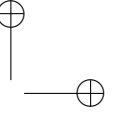
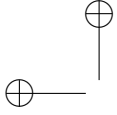
The work contained in this PhD thesis aims to investigate and develop solutions for providing secure and reliable wireless and ad hoc communications. The research goals of this PhD work are:

- **Goal 1:** To collect knowledge that forms a foundation for security and reliability in wireless communications, especially communication in ad hoc networks.
- **Goal 2:** To create solutions for securing and providing reliable wireless communication services, especially for ad hoc network applications.

This PhD project contains a number of distinct, but related works tied to SWACOM project research theme. The main contributions of this thesis are:

- **Contribution 1:** Propose an alternative approach to secure wireless and ad hoc communications by using identity-based cryptography. Paper [A](#) introduces a new application of identity-based cryptography to replace





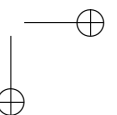
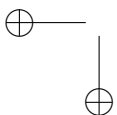
current ZigBee security solution, while Paper [B](#) proposes an application of identity-based cryptography to secure a distributed electronic payment scheme using mobile phones.

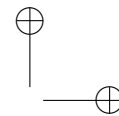
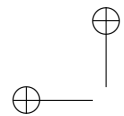
- **Contribution 2:** Propose a routing algorithm to provide reliable communications for underwater sensor networks. Sensor devices running our algorithm can actively move out of shadow zones areas, which causes network disconnection, to keep themselves connected. The solution helps to increase the availability and reliability of underwater sensor network operations. This contribution is presented in Paper [C](#).
- **Contribution 3:** Propose a new secure multicast routing algorithm to increase energy efficiency in actuator and sensor networks. We use existing security building blocks for providing security services while introducing a new solution for reducing energy consumption for multicast communication in sensor and actuator networks. Paper [D](#) presents this work.

The thesis is divided into two parts. The first part is an introduction that contains two chapters while the second part is a collection of papers, which consists of four papers.

Chapter [1](#) presents the background and motivation for this PhD research. In this chapter, we briefly review the security for wireless and ad hoc networks, as well as the use of identity-based cryptography to simplify security implementations. We also discuss security and reliability issues in sensor networks, including underwater sensors with different characteristics. Chapter [2](#) summarizes paper contents and presents contributions of our papers. This chapter ends with conclusions and discussion of open problems.

Four papers in Part [II](#) are grouped into two categories. Paper [A](#) and [B](#) are the applications of identity-based cryptography for securing wireless and ad hoc applications. Paper [C](#) and [D](#) are solutions for secure and reliable communications in wireless sensor networks.



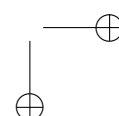
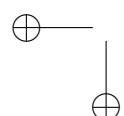


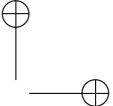
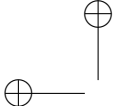
Papers

The author has published five papers and has the other two papers under review. Below is the list of papers completed during the author's PhD study.

Published Papers

1. Son T. Nguyen, Erdal Cayirci, Liang Yan, Chunming Rong. “*A Shadow Zone Aware Routing Protocol for Tactical Acoustic Undersea Surveillance Networks*”. In Proceedings of Milcom 2009, Oct 18–21, 2009, Boston, USA.
2. Erdal Cayirci, Son T. Nguyen, Chunming Rong. “*Secure Many to Many Routing for Wireless Sensor and Actuator Networks*”. Invited paper in the 2nd International Conference on Security of Information and Networks (SIN 2009), Oct 6–10, 2009, North Cyprus.
3. Son T. Nguyen, Erdal Cayirci, Liang Yan, Chunming Rong. “*A Shadow Zone Aware Routing Protocol for Acoustic Underwater Sensor Networks*”. IEEE Communications Letters, Vol.13, Issue 5, pages 366–368, May 2009.
4. Son Thanh Nguyen, Chunming Rong. “*ZigBee Security Using Identity-Based Cryptography*”. In Proceedings of the 4th International Conference on Autonomous and Trusted Computing (ATC'07), Jul 11–13, 2007; LNCS 4610 pages 3–12, Hong Kong, PRC.
5. Son Thanh Nguyen, Chunming Rong. “*Electronic Payment Scheme Using Identity-Based Cryptography*”. In Proceedings of the 4th European PKI Workshop: Theory and Practice (EuroPKI'07) Jun 28–30, 2007; LNCS 4582 pages 330–337, Mallorca, Spain.

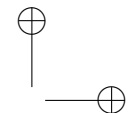
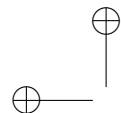




Papers Under Review

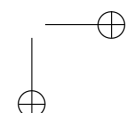
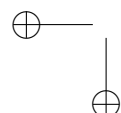
6. Son T. Nguyen, Erdal Cayirci, Liang Yan, Chunming Rong. “*A Shadow Zone Aware Routing Protocol for Underwater Sensor Nodes with Power Controlled and Movable Transducer*”. Submitted to IEEE/ACM Transactions on Networking.
7. Son T. Nguyen, Erdal Cayirci, Chunming Rong. “*Secure Many to Many Routing for Wireless Sensor and Actuator Networks*”. Submitted to ACM Wireless Networks.

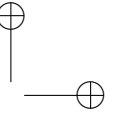
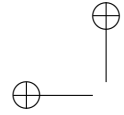
Paper 4, 5, 6 and 7 have been added to constitute Part II of this thesis and are named Paper A, B, C and D respectively. Paper C is an extension of Paper 1 and 3 while Paper D is an extension of Paper 2. The included papers have been re-formatted to comply with the thesis layout.



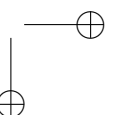
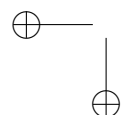
Contents

Preface	iii
Acknowledgments	iii
Executive Summary	v
Papers	vii
Contents	ix
List of Figures	xiii
List of Tables	xv
I Introduction	1
1 Introduction	3
1.1 Background	4
1.1.1 Wireless Network Vulnerabilities	4
1.1.2 Identity-Based Cryptography	8
1.1.3 Secure Routing for Wireless Sensor Networks	13
1.2 Research Objectives	19
1.3 Research Methodology	19
2 Research Results	21
2.1 Research Contributions	21
2.1.1 Security in Wireless and Ad hoc Communications	21
2.1.2 Security and Reliability in Sensor Networks	24
2.2 Open Problems	25
2.3 Conclusion	26
II Paper Collection	29
A ZigBee Security Using Identity-Based Cryptography	31
A.1 Introduction	31



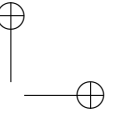
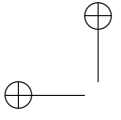


A.2	Security in ZigBee Network	32
A.3	Identity-Based Cryptography	34
A.4	IBC for Security in ZigBee Network	35
A.5	Critical Analysis	39
A.5.1	IBC vs. Current ZigBee Security	39
A.5.2	IBC vs. Public-key Cryptography	39
A.6	Conclusion	40
	References	40
B	Electronic Payment Scheme Using IBC	43
B.1	Introduction	44
B.2	Previous Works	44
B.2.1	Existing Proposals for E-wallet	44
B.2.2	Identity-Based Encryption	47
B.3	An Identity-Based Encryption for Online E-Wallet System	48
B.3.1	Security and Performance Analysis	50
B.4	Conclusion	51
	References	51
C	A Shadow Zone Aware Routing Protocol for UASN	53
C.1	Introduction	53
C.2	Shadow Zone Phenomenon	55
C.3	Related Works	57
C.4	Shadow Zone and Delay Aware Routing	59
C.4.1	System Architecture	59
C.4.2	Self Organization and Data Forwarding	60
C.5	Performance Evaluation	65
C.5.1	Step-length Δ_l Calculation	65
C.5.2	Network Connectivity	67
C.5.3	Event Delivery Ratio	67
C.6	Results and Analysis	68
C.7	Conclusion	71
	References	72
D	A Secure Many to Many Routing Protocol	75
D.1	Introduction	76
D.2	Related Works	77
D.3	Secure Many-to-Many Routing for WSN	78
D.3.1	Network Model and Problem Formulation	78
D.3.2	SMMR Protocol	80
D.3.3	Power Controlled SMMR Protocol	87
D.4	Performance Evaluation	89
D.4.1	Simulation Parameters	89
D.4.2	Radio Model	90
D.4.3	Simulation Results	90
D.5	Conclusion	93
	References	93



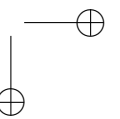
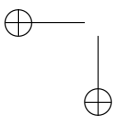
Bibliography

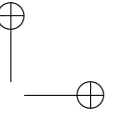
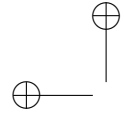
95



—

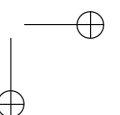
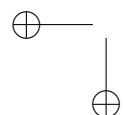
—

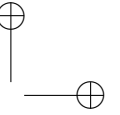
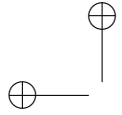




List of Figures

1.1	Model for network security.	8
1.2	Model for conventional cryptosystem.	9
1.3	Model for public-key cryptosystem.	11
1.4	Identity-based encryption and signature scheme.	13
1.5	Fixed underwater sensor network	17
1.6	Mobile underwater sensor network	17
A.1	Keys in residential and commercial mode	33
A.2	Identity-based encryption and signature scheme	35
A.3	Membership approval with hierarchical management	37
A.4	Home automation example	38
B.1	The online wallet general architecture	45
B.2	The transactions of payment system using an online e-wallet	46
B.3	Identity-based encryption and signature schemes	47
B.4	Transactions in mobile payment scenario	48
C.1	Comparison of CMSS and WUSN	54
C.2	Fixed WUSN	55
C.3	Mobile WUSN	55
C.4	Speed of acoustic signal undersea	56
C.5	Shadow zone	56
C.6	A sensor node with separate sensor cluster and transducer	59
C.7	getConnected procedure run by the sending node	61
C.8	<i>HELLO</i> message	61
C.9	<i>routeReply</i> message	61
C.10	Routing table	61
C.11	Power control	63
C.12	Transducer re-location	64
C.13	<i>Data</i> packet	65
C.14	<i>HELLOtoNeighbor</i> message	65

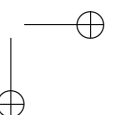
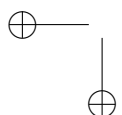


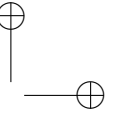
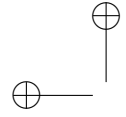


C.15 Optimal moving step Δ_l	68
C.16 $\overline{\Delta E}$ in relation to μ_{E_c}	69
C.17 Connectivity comparison	70
C.18 Event delivery ratio	70
C.19 Packet delay comparison for different Δ_l	71
C.20 Packet delay comparison for different t_w	71
D.1 Packet types in SMMR	80
D.2 Task dissemination in SMMR	81
D.3 The total power used from node X to Y	88
D.4 Number of living nodes against the number of successful events for 500-node configuration.	91
D.5 Average node's residual energy against the number of successful events for 500-node configuration.	91
D.6 Residual energy of 100 randomly selected nodes after 2000 successful events.	92
D.7 Number of successful events against node density.	92
D.8 Number of successful events against the number of actuators	93

—

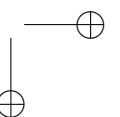
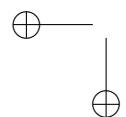
—

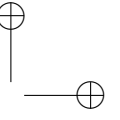
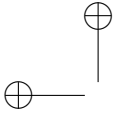




List of Tables

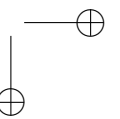
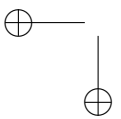
1.1	RSA algorithm	10
2.1	Focus areas of papers in Part II.	22
A.1	Comparison of different schemes used for ZigBee security	40
C.1	Simulation parameters	68
D.1	Notations	79
D.2	Registration table of Node c in Figure D.2 for SMMR	82
D.3	Routing table of Node c in Figure D.2	83
D.4	Registration table of Node c in Figure D.2 for PCSMMR	88
D.5	Simulation parameters	89

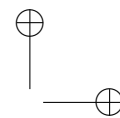
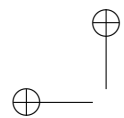




—

—





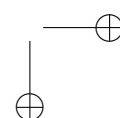
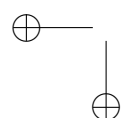
|

Part I

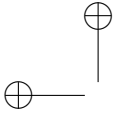
Introduction

—

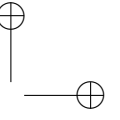
—



|

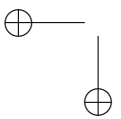


|

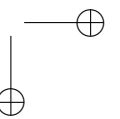


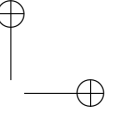
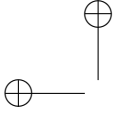
—

—



|





CHAPTER 1

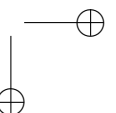
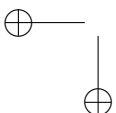
Introduction

—

Wireless communications has played an important role in daily life since its introduction. It can be used in cellular networks, short-range communication networks, e.g. Bluetooth, WiFi, remote control systems, security systems for home and office buildings etc. Among the applications of wireless communication technology, cellular telephony is the most popular. With the advantages of mobility and flexibility, it offers us communications on-the-go. More over, as the mobile devices are getting smarter and more powerful, which can be used for communication, entertainment and business tools, they quickly become integral part of our daily life.

Another application domain of wireless communication is wireless ad hoc networking, which can be used to set up temporary and flexible networks. Wireless ad hoc networking can be useful in monitoring and control applications, disaster relief operations, or military area surveillance etc. A wireless sensor network is an application that uses wireless ad hoc networking technology where a large number of small sensor nodes are deployed closed to the phenomenon to be observed. Those sensor nodes work in ad hoc manner with additional and more stringent constraints. With many advantages that it provides, the use of wireless ad hoc networking has become pervasive.

The use of wireless communication technology introduces more challenges compared to that of fixed networks. The wireless medium is not only easier to eavesdrop on than guided media, it is also susceptible to jamming and other kinds of Denial of Service (DoS) attacks. These problems raise serious security challenges. Moreover, nodes in wireless networks are often mobile, which also introduces availability and reliability challenges as the nodes may be out of network coverage.



In ad hoc networks, there are even more challenges because these networks are infrastructureless and follow a multihop communication pattern, which is harder to manage and to provide security services. Ad hoc and especially sensor devices also suffer from limited resource constraints. These limitations make deploying security and reliability solutions in ad hoc networks even more difficult.

There are many security solutions used for existing wireless networks. For example, the cellular networks have a set of standards, which includes security specifications and implementations that provide the underlying security. Ad hoc networks, despite of their immaturity, also have security features to provide security and reliability services.

Even though security services are widely used in cellular networks and also exist in some ad hoc network applications, there is still a significant requirement for security and reliability research. The use of new technologies or a combination of existing technologies may offer better and/or convenient services to current wireless network users. In the case of ad hoc networks, current security and reliability solutions are often application-specific and there are still unexplored areas.

The main objectives of this PhD thesis is to investigate security and reliability issues in wireless and ad hoc communications and aims at providing solutions to contribute to different aspects of secure and reliable wireless and ad hoc communications. Our particular focuses are in two sub domains: identity-based cryptography for securing wireless network security; and routing algorithms for secure and reliable sensor network communications.

The following section presents some background about the fields that related to our research.

1.1 Background

1.1.1 Wireless Network Vulnerabilities

Conventional wireless networks are primarily used for personal communications. In these systems, end-devices are used by human beings to communicate with other human beings or with service providers. The network architecture is centralized where end-devices connect to service providers' infrastructures and trust the service operators. There is no direct communication among end-devices. Examples of current wireless networks are WiFi, Bluetooth, and GSM/UMTS cellular networks.

These wireless networks are different from fixed networks in the way communication takes place. Thus they suffer from additional security and reliability problems compared to wired networks.

The first difference in wireless networks is that communication between nodes takes place using a wireless channel. That channel suffers from a number of vulnerabilities [10]. The following list shows typical vulnerabilities of a wireless

channel. Though these vulnerabilities also exist in a fixed communication line, they are more severe in a wireless channel:

- **Eavesdropping:** information that the victim transmits or receives can be overheard by placing a receiver in proximity or by using a high sensitivity receiver from a distance. Eavesdropping is often used to collect information for later use.
- **Integrity violation:** the content of messages exchanged between communication parties can be captured and modified.
- **Impersonation:** an attacker can impersonate a legitimate user. Though this vulnerability also exists in wired networks, it is even easier for the attacker to use this kind of attack in wireless environments.
- **Jamming:** an attacker can jam the radio channel for a Denial of Service (DoS) attack. For example, the attacker can transmit at the same time the victim transmits or receives data to create collisions. This can even be done from a long distance with high power transmitters.

The second difference of wireless networks that may affect to security and reliability is that the devices are small and usually mobile, which introduces several challenges compared to fixed networks.

- **Privacy:** when users move, their devices' locations can be used to trace their whereabouts and disclose their privacy. This means that the specific location at specific point of time of the users can be revealed.
- **Availability:** wireless environments might change as users move. This may cause service disruption when users move from a place where service is available to a place without service.
- **Resource constraint:** mobile devices are often small and have limited storage, computing power, and energy. Energy limitation is the most significant among these constraints. Conserving energy by reducing the number of operations performed by the devices can however result in worse security protocols.

Besides conventional wireless networks, which have centralized architecture, there are also ad hoc networks with decentralized architecture. A special kind of ad hoc networks is sensor network where a large number of small sensors are used for monitoring, surveillance and control applications. Those devices are limited in the capability and resources.

The use of ad hoc networks introduces new decentralized and even self-organized architectures where roles of service providers are limited or eliminated. The network consists of peer nodes relaying traffic for one another. Thus, it forms a multi-hop communication pattern. Also, devices in sensor networks have very

limited resources and provide limited computing and communication capabilities. Thus, ad hoc networks introduce new security challenges compared to conventional wireless networks.

The following features make ad hoc and sensor networks more vulnerable than traditional networks [20]:

- **Infrastructureless:** in a general ad hoc network, there is normally no trusted central point where network devices can connect to. In sensor networks, there exists base stations and/or sinks, which can be considered central points. However, the communication among sensor nodes is performed in a multi-hop manner where security of one node may affect that of others. This means that designing a security solution for ad hoc and sensor networks is more difficult since it should rely on a distributed scheme instead of a centralized scheme as in conventional wireless networks.
- **More vulnerable wireless link:** link layer protocols in ad hoc networks rely on trusted and cooperative behaviors of neighbor nodes which might be suffer from selfish behaviors or abuses.
- **Multi-hop communication:** data packets follow multihop routes and pass through different network nodes before arriving at their destinations. Due to the possible untrustworthy behaviors of relaying nodes, this feature presents a serious vulnerability because security of one node may affect security of other nodes.
- **Mobile node:** though nodes in conventional wireless networks also move, node mobility in ad hoc networks introduces more severe effects. As a node might behave as a relay node to pass its neighbor's traffic to the sink, its mobility creates a connection problem when its neighbor cannot find an uplink node to send data to the sink.
- **Topology change:** node mobility, unstable wireless connectivity, and power constraint can be different sources that affect node and link availability. Therefore, network topology might change frequently.
- **Resource constraint:** Ad hoc network devices are small with limited resources. This limitation causes vulnerabilities where attackers may deplete a node's energy to create network partitioning. Also, security solutions that require high computational complexity are difficult to be implemented with the above resource constraints. This is especially true in the case of sensor networks.
- **Physical vulnerability:** ad hoc and sensor nodes are small and portable. Thus, they can be stolen and reverse engineered to get secret information. This information can later be used to compromise other nodes.

Security Requirements

Basic security requirements, including those for existing wired and wireless networks, that a security provider need to provide are:

Confidentiality This might be the most important aspect in network security. Encryption is the common practice to provide confidentiality service.

Integrity While confidentiality protects data from being disclosed, it does not protect data from being changed by the attackers. This change of data may harm the system if not prevented or detected. Data integrity ensures that data has not been altered in transit.

Authentication An attacker might not just alter the content of data packets. He can also inject additional packets for malicious purposes. Authentication guarantees that the received data comes from a legitimate source and the party at the other side of the communication channel is the one he claims to be.

Access control This service protects the infrastructure from unauthorized access. For example, the use of firewalls to protect internal networks from the outside accesses.

Non-repudiation This service prevents a communication party from denying that he has actually involved in the transactions. Non-repudiation service is often associated with public-key cryptography.

Beside general security requirements, ad hoc and especially sensor networks also add additional requirements [67]. Those requirements also exist in traditional security models. However, we mention them here under ad hoc network security requirements as we consider they are crucial for the operation of those networks.

Self-organization Every node need to be self-organizing and self-healing according to different situations because there is no fixed infrastructure available for network management. This feature introduces a challenge to security in ad hoc networks. For instance, when a sensor node is dead due to energy depletion, other nodes must still be able to operate normally.

Clock synchronization Most of sensor network applications rely on some form of clock synchronization. The precise clock is needed for many operations, for example, to decide when the sensor node is going to sleep and when it will awake. The clock can also be used to calculate end-to-end delay when transmitting packets between nodes. Thus, clock synchronization plays an important role for the correct and efficient operations.

Secure and reliable localization A node in ad hoc networks needs to know the location of its neighbors, or at least, who its neighbors are, in order to route packets. If this information is not correct, network operation might be malfunctioned or network security might be violated.

In summary, wireless networks in general and ad hoc networks in particular suffer from more security and reliability problems than fixed networks. This is due to the wireless medium environment, the communication pattern and the characteristics of wireless devices.

1.1.2 Identity-Based Cryptography

This section presents a brief introduction about identity-based cryptography, which is used as a building block for our proposals to secure wireless and ad hoc communications in Paper A and B. In this section, we first briefly present symmetric and public-cryptography, and then introduce identity-based cryptography and its applications.

Symmetric and Public-key Cryptography

A general model for communication security contains a sender, who sends messages, a recipient, who receives the transmitted messages, and an opponent, who tries to attack and violates the confidentiality, authenticity etc., of the transaction by manipulating the transmitted messages. Figure 1.1 [60] presents such a model.

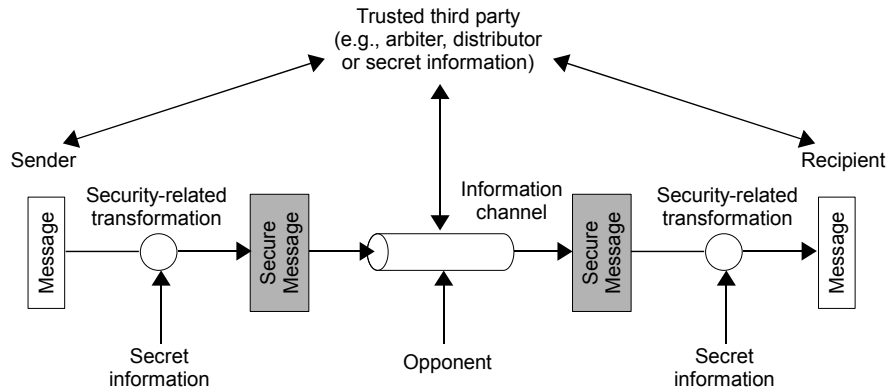


Figure 1.1: Model for network security.

To protect transactions from being compromised by the opponent, the two communication parties have to establish a set of security techniques to secure their communication. As described in [60], all techniques for providing security have two components:

- **A security-related transformation:** this will be applied to the messages to be sent. Examples of the transformation are encryption algorithms used to scramble messages to make them unreadable before sending and thus, prevent the opponent from observing the exact content. At the other side, appropriate decryption algorithms are used to de-scramble the received messages to make them readable to the recipient. A possible authentication code can be added to verify the identity of the sender.
- **A shared secret information:** this information should be shared, by some ways between the two communication parties and be kept secret from the opponent. An example is a secret key shared between parties in

a symmetric encryption scheme. There might be a trusted third party to work as the distributor of the secret information.

Cryptography¹ is probably the most important aspect of communication security. It can be divided into symmetric-key and asymmetric-key cryptography, or secret-key and public-key cryptography. Symmetric-key cryptography was invented thousands of years ago and was the only form of cryptography until 1976, when public-key cryptography was first introduced [19].

Symmetric cryptography is a form of cryptosystems where the encryption and decryption are performed with the same secret key. The key is distributed between two parties securely, i.e. from the opponent perspective, by direct communications or with the help of a trusted third party. Symmetric cryptography is again divided into block cipher and stream cipher. Figure 1.2 presents a model for a symmetric cryptosystem, which is adapted from [60].

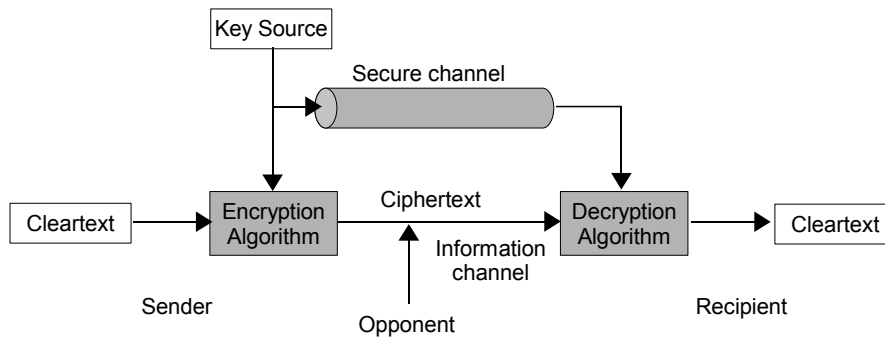


Figure 1.2: Model for conventional cryptosystem.

The main advantage of symmetric cipher is its speed and performance over a later introduced public-key cryptography. However, one of its main disadvantages is key management process, which relates to secret key distribution. This may create a number of problems:

- **Requirement for a secure channel:** to establish a shared secret key between two parties, there must exist secure channels between them. If secure channels do not exist between two parties or between each party and a trusted third party, secure key delivery is impossible.
- **Requirement for a number of keys:** for two parties to communicate securely, there need to have at least one secret key shared between them. However, if the communication involves a number of parties, the number of secret keys required for them to communicate secretly increase as the square of the number of parties, unless a trusted third party is involved.

¹For simplicity, we might use the words cryptography, cipher and encryption/decryption interchangeably. In the situations where clarification is needed, we will mention each concept clearly.

- **Requirement for a trusted third party:** to increase the feasibility of the symmetric cryptography for a network with large number of parties, a trusted third party is introduced. This party shares secret key with each of the other parties. The trusted third party will help establishing a secure channel when other two parties want to communicate but there is no shared key between them. This approach reduce the number of shared secret keys needed. However, this trusted third party might be a bottleneck in the network.

In 1976, Diffie and Hellman [19] presented a seminal paper introducing a notion of public-key cryptography (PKC). The phrase public-key means that two communication parties can share “secret information” without using a pre-established secure channel.

The phrase “secret information” mentioned here does not mean a real common secret key shared by the two parties as in symmetric cryptography case. Each communication party, in fact, holds its own secret piece of information as its private key², which might be different from the other’s. The two parties then commonly agree to an encryption key, i.e. a public key, to encrypt the transmitted messages that both parties can use their own private key to decrypt. This is obtained based on a very nice mathematical feature that makes public-key cryptography the most significant advance in 3000 years history of cryptography [60]. An example of public-key cryptography, a RSA algorithm [54], is presented in Table 1.1.

Public Key: a pair n and e where
n : product of two primes, p and q (p and q must remain secret)
e : relatively prime to $(p-1)(q-1)$
Private Key: d where
$d = e^{-1} \text{ mod } ((p-1)(q-1))$
Encryption:
$c = m^e \text{ mod } n$ where m is the plaintext to encrypt, c is the ciphertext
Decryption:
$m = c^d \text{ mod } n$

Table 1.1: RSA algorithm

The security of public-key cryptosystem is based on the computational complexity of hard problems, for example, the integer factorization problem of the RSA algorithm, or the discrete logarithm problem of Diffie-Hellman algorithm, or number theoretic problem involving elliptic curves in elliptic curve cryptography.

In addition to encryption/decryption, PKC also provides digital signature feature. A digital signature is unique and attached to the party that generates it, easy to produce and difficult to forge. It is also tied to the message that the

²For clarity purpose, the word “secret key” is understood as a shared secret key between parties in symmetric key cryptography while the word “private key” is understood as own secret decryption key kept by each party in public-key cryptography.

sending party signs. Digital signature helps to solve the problem of authenticity, i.e. to prove that a communication party is an entity it claims to be, and non-repudiation, i.e. to prevent a party from denying that it has performed the transactions. Digital signature is a crucial part of public key infrastructure operations as well as many other network security schemes.

Figure 1.3 [60] presents a model of public-key cryptosystem where both secrecy, i.e. encryption/decryption, and authentication are performed. The sender A first signs his message by his private key, and then encrypts it with the recipient B's public key before sending. When the recipient B receives the message, he first decrypts it using his private key and then verify the message by the public key of the sender A.

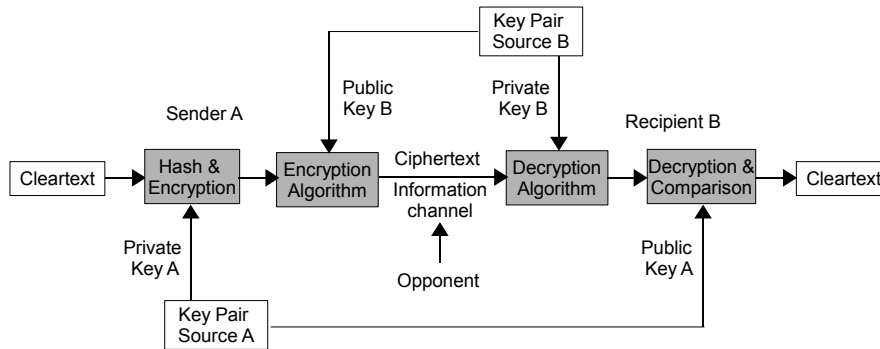


Figure 1.3: Model for public-key cryptosystem.

Though PKC have many nice features over symmetric cryptography, its operations are more computationally expensive than those used in symmetric cryptography. As a consequence, PKC and symmetric cryptography often co-exist in a hybrid system and work together to achieve final security goals. For example, the message is encrypted using symmetric algorithm, while the message encryption/decryption key is encrypted using the public-key algorithm and sent together with the message.

Identity-Based Cryptography

Identity-based cryptography (IBC), invented by Adi Shamir in 1984 [58], is a special form of PKC where a communication party can use its unique identity together with global parameters to form its public key. An identity-based cryptosystem consists of a key generation center, i.e. private key generator or PKG, which is in charge of setting up global parameters and issuing private key associated with specific identity. Users can then use global parameters and an identity to generate a public key for that identity. The exchange of public key is simply the exchange of the unique identity.

IBC makes the use of PKC more convenient as it might eliminate the use of cer-

tificates in PKC because the party's identity can be easily verified. For example, one can use the other party's email address or mobile phone number (suppose that they are unique and authentic) to generate the public-key and use that key to encrypt messages sent to the other party.

The advantages of IBC over PKC are:

- There is no need to maintain a public-key directory, as the public keys are based on identity information widely known by other parties.
- Secure communications can be done even before the recipients obtain private keys from PKG. In this case, the recipient, having received the encrypted messages, will contact the PKG to get a private key associated with its identity information to decrypt the message.

IBC also has inherent problems, for example key revocation, which can be described as follow. When a communication party uses its unique identity to form its public key and has a private key associated with that information, a serious problem appears if the private key is compromised. The common behavior is to replace public/private key pairs. However, the public key is associated with that party's identity which is hard to change. The public key is also influenced by the service provider's public parameters while those parameters are also hard to change as they will affect other users. A simple solution to overcome this problem is to use a private key with attached expiration time, which will become invalid after certain time.

The working principles of identity-based encryption and signature schemes are presented in Figure 1.4 which resembles the figures in our Paper A and B.

Identity-Based Cryptography Applications

IBC is particularly useful when the communication parties are human beings. In this case, instead of exchanging public keys, which are often a long string of ASCII characters, they only need to exchange email addresses or phone numbers to generate public keys. This is also easier to verify the authenticity of these identities.

There are some existing solutions to offer IBC services. Voltage Security [66] has developed an IBC solution for securing emails in which they use email addresses to form public key to encrypt emails. There is also a prototype of securing SMS messages using IBC, as described in [33] and [34], where SMS sent are encrypted by using the recipient's mobile number to form a public key. As mobile phones become an indispensable part of our daily life, the use of IBC for mobile phones is a promising application in the future.

Identity management, which is another research topic under SWACOM project, can also be used together with IBC to provide more convenient and secure solutions.

However, in order for IBC to be integrated and used efficiently in small, resource-constrained devices, there is a need for improvements on the efficiency of IBC.

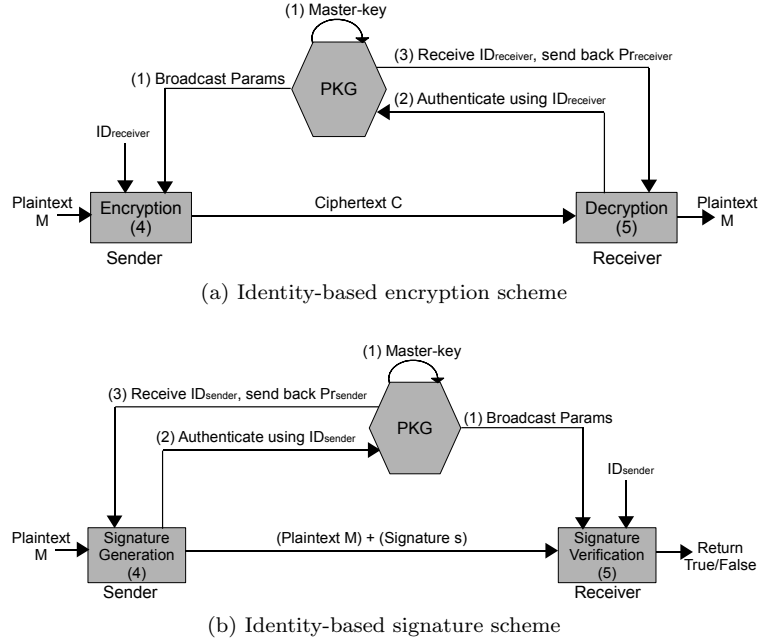


Figure 1.4: Identity-based encryption and signature scheme.

Current IBC solutions based on weil pairings [8] is believed to be too computationally expensive for small devices.

Paper A and B present our works related to IBC. Paper A proposes an ideas to apply IBC for securing ZigBee communication, which can be use in smart home applications. Paper B is a proposal of IBC application to secure mobile payment using mobile phones as the end devices.

1.1.3 Secure Routing for Wireless Sensor Networks

Sensor networks are used in civilian and military applications. They can be used for animal tracking, environment monitoring or disaster relief. They can also be used for military applications like monitoring and surveillance. Security and reliability is therefore very important for them.

Sensor network devices, however, suffer from many constraints, including low computation capability, limited memory and energy supply, susceptibility to physical capture. They also use insecure wireless channels as a form of communication. These constraints make designing security and reliability solutions for sensor networks a big challenge.

Part of this PhD work aims at develop secure and reliable routing solutions for sensor networks. We work on both conventional sensor networks³, which use

³The phrase “sensor network” in general is to represent both conventional sensor network using radio frequency and underwater sensor network using acoustic signals for communication.

radio frequency, and underwater sensor networks, which use acoustic signals for communication. This section aims to provide an overview of related fields used as the foundation for our work presented in Paper C and D. We first presents the obstacles that make designing sensor network security difficult. We then discuss the conventional secure routing problems in sensor networks. After that, we give a brief review of some issues that distinguishes underwater sensor networks from conventional sensor networks.

Sensor Network Security Obstacles

As mentioned above, sensor devices are limited in resources which makes designing security solutions for them difficult. The two main obstacles in providing security for sensor networks are presented as follow:

- **Very limited resources:** security operations require a certain amount of resources for the implementation, for example, memory space, processing power and energy. However, these resources are very limited in a wireless sensor device.
- **Unreliable communication:** security of the network relies heavily on a network protocol, which in turn depends on communication. However, the communication in sensor network is not reliable. Some characteristics that contribute to the unreliable operations of sensor networks are wireless channel unreliability, collisions, multihop communication pattern, network latency and congestion, and lost of clock synchronization. These characteristics are even more severe in underwater sensor networks, which uses acoustic signals for communication.

Secure Routing in Wireless Sensor Networks

An overview of secure routing for conventional wireless sensor networks can be found in [36]. Other sources of references include [13], [20], and [67].

Attacks on Sensor Network Routing Protocols As discussed in [36], routing protocols for sensor network are quite simple and are susceptible to attacks. Below are different kinds of attacks on sensor network routing protocols.

- **Spoofed, altered, or replayed routing information:** in this kind of attack, the attackers target at routing information exchanged between network nodes. By manipulating this routing information, the attackers can create routing loops, disable a legitimate route, generate false alarm messages or partition the whole network.

However, in most cases we use this phrase to mention conventional sensor network without confusions. In case clarification is needed, we will use the prefixes, “conventional” for RF sensor networks, and “acoustic” for underwater sensor networks

- **Selective forwarding:** this attack can be launched by an attacker controlling a malicious node. This node selectively forwards or drops packets passing through it. This kind of attack targets specific nodes, degrades or creates false perception about network quality.
- **Sinkhole attack:** this attack has a goal to attract surrounding traffic to a malicious node. The attacker does this by instructing the node to broadcast good routing information, for example, to let other nodes know that it has low delay and hop count to the sink and thus provides a better route. The traffic destined to the malicious node is subsequently dropped or processed by the attacker with a much more powerful device attached to that node.
- **Sybil attack:** in Sybil attack, a single malicious node may represent multiple identities in the network. Those identities then “cooperate” to provide false information about the network state, thus, assisting the attacker in luring authentic sensor nodes. Sybil attack increases the influence of malicious nodes in the network.
- **Wormhole attack:** in wormhole attack, the attacker creates a tunnel to route traffic from one part of the network to the other. Normally, two malicious nodes located at two ends of the tunnel will attract traffic from the surrounding areas and route through the tunnel, which is under the attacker’s control. The attacker can process the collected traffic for malicious purposes or just simply drop traffic to disrupt network operation.
- **HELLO flood attack:** the attacker in HELLO flood attack simply uses a high power transmitter to broadcast a HELLO message contain information about high-quality route to every node in the network. The faraway nodes cannot send the data packets to the attacker due to their limited transmission power. They, however, are also confused about routing information as their neighbors, who are also receivers of HELLO flood messages, perceive the same information.
- **Acknowledgment spoofing attack:** in this attack, the attacker generate an acknowledgment even if the previous transaction is not successful. The goal of acknowledgment spoofing is to provide wrong information to the victim, e.g. a link quality is higher than it actually is or a dead node is alive.

Attack Countermeasures There have been many researches working on solutions for tackling the above attacks. One approach to provide a countermeasure against selective forwarding attack is to use multipath routing [42] in which a message is forwarded through a number of disjoint paths. In order to launch selective forwarding, the attacker need to control at least one node on each disjoint path. This approach is a very good solution against selective forwarding with the trade-off of high communication overhead. The countermeasure to Sybil attack is to prevent the attacker from using the identities of non-compromised nodes. This prevention can be done by identity verification with the assistance from

the base station⁴. A pair of nodes, after verifying each other, establish a shared key. In the mean time, the base station can limit the number of neighbors, and shared keys, that a node can have. Thus, the compromised node can only communicate with its neighbors. Work in [32] presents a technique for detecting wormhole attacks in ad hoc network routing. This approach, however, requires strict clock synchronization between network nodes. Another approach that help tackles sinkhole and wormhole attacks is geographic routing protocol in which the locations of nodes are known and used to detect such attacks. A simple way to prevent from HELLO flood attacks is to verify the communication channel bidirectionally before accepting a link as legitimate. This approach is, however, not always practical if the attacker has both a powerful transmitter and a high sensitivity receiver. Another approach to overcome this problem is to request neighbor nodes to authenticate each other similar to the case of sinkhole and wormhole attack prevention.

There are also other countermeasures for securing sensor network routing. Each has its own advantages and disadvantages and is used based on specific requirements. As sensor devices are highly resource-limited, it is very hard to design a general purpose security solution that satisfies all the requirements.

Our work in Paper D introduces a solution to secure multicast routing in sensor networks. We use existing key pre-distribution schemes to provide confidentiality among nodes and use authenticated broadcast presented in [53] for authenticated interest dissemination. Thus, it helps preventing malicious nodes from injecting erroneous and incorrect routing information.

Secure and Reliable Routing in Underwater Sensor Networks

The above section presents attacks and countermeasures for secure routing in sensor networks, which is typically true for conventional sensor networks. There is, however, another application domain of sensor networks, i.e. underwater monitoring and surveillance, with additional and different properties. Thus, underwater sensor networking introduces new research challenges though similar aspects in conventional sensor networks have been well-addressed.

Underwater Sensor Networks Similar to conventional sensor networks, underwater sensor networks [2] are used for monitoring and surveillance operations in underwater environment. For examples, the underwater sensor networks can be used to monitor sea floor, fishing farms or to protect harbors. They can be used to assist environment protection, disaster prevention, undersea exploration as well as support military applications. They can be either fixed or mobile. Figure 1.5 represents a fixed underwater sensor network while Figure 1.6 represents two mobile underwater sensor networks, one uses radio frequency and the

⁴In security perspective, a base station is the central point of a sensor network that all nodes can trust. In the mean time, a sink is a node that receives and processes the sensing information from sensor nodes. A base station and a sink differ in their functionality in the sensor network, though they can exist in the same physical device.

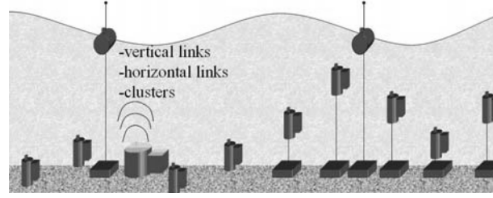


Figure 1.5: Fixed underwater sensor network

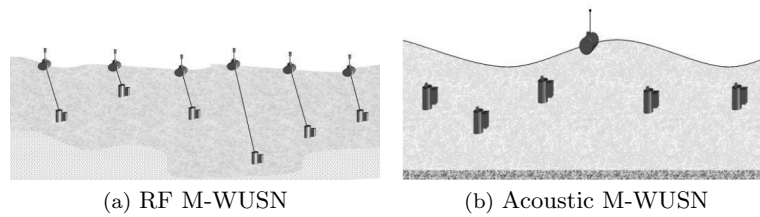


Figure 1.6: Mobile underwater sensor network

other use acoustic signal for communication. The figures have been taken from our Paper C.

The communication in underwater sensor networks can be done in different ways. In the first approach, the sensing devices are underwater that conduct the sensing tasks. Those devices are connected with a buoy floating on the sea surface. The sensed data is transmitted via wired connection from the sensing module to the communication module placed in the buoy. The buoys then communicate with each other using radio frequency similar to conventional sensor networks. This approach however, is not always applicable as it needs to deploy a large numbers of buoys on the sea surface. There might also a communication problem that affect reliability as the buoys are not always within the line-of-sight of others due to the influences of sea waves.

In the second approach, both the sensing and communication modules of a sensor node are underwater. Sensor nodes communicate with one another by acoustic signal, as radio frequency signal cannot transmit far in underwater environment. This second approach is a preferred choice for deploying a *wireless* underwater sensor networks. When mentioning a underwater sensor network, we mean wireless underwater sensor network using acoustic signal as a form of communication.

The differences between conventional and underwater sensor networks that form the major challenges of underwater sensor network communication are as follow:

Limited bandwidth As a underwater sensor uses acoustic signal, the available bandwidth is narrower than that of a conventional RF-based sensor. Thus, it reduces the data rate that can be sent. It may also affect the techniques that can be used to avoid link layer collisions, e.g. bandwidth partitioning.

Low quality channel Underwater channels has much lower quality compare to those of a conventional wireless channel. This low quality is due to the inherent characteristics of the underwater environment as well as other external influences, e.g. fish, tide etc., which leads to higher bit error rate (BER).

Low signal speed The acoustic signal speed is 10^5 times slower than that of radio frequency. Thus, the propagation delay in underwater sensor network is considerably higher than in conventional sensor network. This not only affects the overall delay but also affects the MAC performance in underwater networking as it may generate higher frequency of collisions.

Device failure Underwater devices are prone to failure and hard to replace. Thus, the cost for underwater sensors are higher than that for conventional sensor networks. The maintenance tasks are also more difficult.

Due to the differences in the working environment, underwater sensor networking introduces new research challenges even though some similar aspects in conventional sensor networks have been well-addressed.

Security and Reliability in Underwater Sensor Networks Underwater sensor networks suffer from the same security and reliability problem as conventional sensor networks. Moreover, due to the differences in the working environment as mentioned above, underwater sensor networking is exposed to additional challenges.

1. The first set of new security and reliability problems in underwater networks is due to the changes in the environment, i.e. low channel quality and high propagation delay. While the former requires designing of more reliable networking protocols, the latter introduces higher link layer collisions as well as making it more difficult to achieve clock synchronization. Those differences require a new protocol design or at least, re-design existing protocols to work efficiently with underwater sensor networks.
2. The second problem relates to the difference between *2-dimensional* (2-D) and *3-dimensional* (3-D) communications in underwater networks. While the working environment in conventional sensor networks, i.e. the air, is almost homogeneous, that of underwater environment changes with the depth. Temperature and atmosphere change with depth when going deeper from the sea surface, which affect the acoustic signal speed. The change of signal speed as a signal travels through different depths bend the signal, according to Snell's law. Thus, the communication for underwater environment does not always follow line-of-sight model as in conventional sensor networks. In 2-D underwater sensor networks, when all sensor nodes are almost in the same depth, e.g. in the seabed, the communication among sensor nodes follows in 2-D pattern with little effect due to Snell's law. However, when sensor nodes are placed at different depths, the communication becomes a 3-D pattern which suffers from Snell's law. Designing a

robust underwater sensor networks also need to take these considerations into account.

3. The third set of problems is due to the influences of the surrounding environment. As communication in the underwater environment is affected by more factors than in conventional sensor networks, security and reliability design for underwater networks also need to consider those problems.

Our Paper C is to solve reliability problems in underwater sensor networks. We are dealing with a 3-D underwater sensor network that is affected by shadow zones [43], which are either caused by the second or third problem mentioned above.

1.2 Research Objectives

The principal objective of SWACOM project [62] is to analyze vulnerabilities and develop mechanisms to provide secure and reliable services for wireless communication networks. A particular focus is on securing dynamic and large scale distributed ad hoc networks which have significant usage in both civilian and military applications.

The project goal is to strengthen the ability of individuals and companies to protect their information over the open air transmission. It is also to contribute to the foundation of current research in ad hoc network technology. The project is an interaction between issues in security, privacy protection, vulnerability and reliability in infrastructure and communication technology.

As part of the SWACOM project, this PhD work provides contribution to meet the project goal. More specifically, the main objectives of this PhD work are:

- Collect knowledge that forms a foundation for security and reliability in wireless communications in general and ad hoc network communications in particular.
- Develop solutions for providing security for wireless and ad hoc communications.
- Develop solutions for providing reliable services for wireless and ad hoc communications.

1.3 Research Methodology

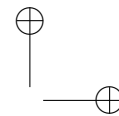
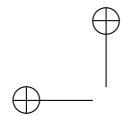
The research approach of this PhD thesis is based on literature review of related works, discussions and guidance from the academic supervisor, discussions and co-operations with colleagues, submission and review of papers, and conference/seminar participations and presentations.

The approach to complete each paper follows conventional research methodology with the number of steps varying depend on paper content, including hypothesis proposal, hypothesis testing and result analysis.

Hypothesis proposal : each paper presents a contribution to the research topic in form of a hypothesis proposal, i.e. introduce a new idea or the new application of existing research ideas. This hypothesis is derived from a review of related works and is backed up by hypothesis testing and/or analysis.

Hypothesis testing : some papers contain hypothesis testing section in which we construct test cases to evaluate our proposed hypothesis. In Paper [C](#) and Paper [D](#), we use simulation to evaluate the proposed hypothesis. The specific tools are OMNET++ for simulations and Matlab for simple calculations and drawing figures.

Result analysis : the proposed hypotheses are compared with similar approaches. In Paper [A](#) and [B](#), comparisons are performed by analyzing the working principle. In other papers, Paper [C](#) and [D](#), comparisons are done by using the simulation results.



CHAPTER 2

Research Results

— This chapter presents the results obtained during this PhD work. The chapter starts with research contributions, where summaries and contributions of papers in Part II are presented. Section 2.2 then provides discussions for open problems related to the research topics, which is useful for future work beyond this PhD thesis. Finally, Section 2.3 draws some concluding remarks after this PhD work. —

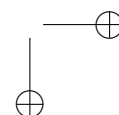
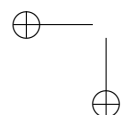
2.1 Research Contributions

Research results of this PhD work are in form of paper publications in scientific conferences and journals. Part II includes representative papers that are the outcome of this PhD. This section presents main contributions of the included papers, which are grouped in the same research areas. Table 2.1 represents the focus area of each paper.

2.1.1 Secure in Wireless and Ad hoc Communications Using Identity-Based Cryptography

Paper A and B propose new applications of identity-based cryptography for securing wireless and ad hoc communications. Though there have been various solutions for securing such communications, the proposals in our works are among the first that use identity-based cryptography.

As the identity of each entity is unique and can be used exclusively to differentiate that entity from others, it can be used to form an encryption key to secure communication for that entity because it inherently attaches to that entity. For



	Cellular Networks	Ad hoc and Sensor Networks
Security Issues	Paper B	Paper A Paper D
Reliability Issues	-	Paper C

Paper A: Propose a solution for securing ZigBee network communication using identity-based cryptography.

Paper B: Propose a solution for securing a distributed mobile payment scheme in cellular networks using identity-based cryptography.

Paper C: Design a shadow zone aware routing algorithm to provide reliable communications for underwater sensor networks.

Paper D: Design an energy-efficient secure multicast routing algorithm for wireless sensor and actuator networks.

Table 2.1: Focus areas of papers in Part II.

example, a human being has many unique identities such that a social security number, an employee number, email addresses, mobile numbers or his name in combination with his address etc., For privacy reasons, not all identities of a person can be exposed to the public and be used for identity-based encryption. However, some unique identities can be used for that purpose, which makes it a very convenient way for securing communication among entities in the community.

Paper A extends the use of identity-based cryptography to secure ZigBee network communication. An example application of a ZigBee network is in smart home environments, where home devices communicate with each other for control and monitoring home environments. Secure communication among devices is implemented by using identity-based cryptography which uses the unique ID of each device to form the public key for it. This is an alternative approach for the current ZigBee security solution and may be of potential use when smart home solutions become widely used and when the capability of devices is getting better over time.

Paper B proposes a solution to use mobile phone number as its owner's identity to secure his communication. With the fact that mobile phones are becoming indispensable devices in human daily life as well as they are getting smarter and more powerful, we believe the use of mobile phones and mobile numbers for secure important daily life transactions is a promising idea and potential application domains in the future.

The following two sections summarize the content of Paper A and B.

Paper A: ZigBee Security Using Identity-Based Cryptography

This paper presents an idea for securing communications between ZigBee network devices by using identity-based cryptography with an example of smart home environment. In this proposal, secure communication is established among network nodes and uses node IDs as part of the encryption keys. This approach

simplifies key management process in current ZigBee networks, reduces overhead, resource requirements and complexity of the system by reducing the number of keys needed, while still keeping the network secure.

Compared to current ZigBee security solution, which use a symmetric security scheme, our approach provides the advantages of public-key cryptography with digital signature capability and session key distribution without the intervention of the key distribution center. This distribution center only needs to exist at network setup phase. In case of node compromise, only nodes that under the attacker's control are affected while other nodes still function normally and securely.

A challenging task for this solution to be practical is the capability of a ZigBee node to work efficiently with an identity-based cryptography solution, meaning that it has enough processing power to implement the security algorithms. Some arguments mention that the use of weil pairings in current identity-based encryption is a burden for resource-constrained devices like ZigBee equipments. We, however, believe that the device capability will be better over time very quickly that make this solution applicable.

Paper B: Electronic Payment Scheme Using Identity-Based Cryptography

Our paper extends the work presented in [47] for online e-wallet system. We introduce a simplified yet secure solution for such system by using identity-based cryptography. Our proposal is not only the alternative solution for secure transactions in that e-wallet system, it can also be used together with other solutions, e.g. identity management, to provide a more convenient security management framework to enhance human daily life.

The online e-wallet with decentralized credential keepers presented in [47] is an architecture that allows a user to leave most of the content of his electronic wallet at the security of his electronic keeper while travelling with his mobile phone. For example, the user leaves his credit cards at home or at some secure locations and access them through mobile phone when necessary. This will relieve the user from remembering information such as PIN codes and prevents the cards from being stolen. When the user needs to make a payment, he uses his mobile phone to connect to his electronic keeper's gateway and access his credentials, e.g. credit cards, then makes the payment. The transactions are secured with existing underlying security technology.

The model proposed in [47] has four secure links: (i) between the buyer and seller; (ii) between the buyer and his secure server where his credentials are kept; (iii) between the buyer secure server and the appropriate credit card issuers/banks; (iv) between the seller and his banks. Security solutions for the last two links are well-established and are not discussed in the paper. Security for the first two links used public-key cryptography, as mentioned in [47].

Our work propose a solution to replace the use of public-key cryptography between the buyer and the seller by using identity-based cryptography. As we

discussed earlier, this approach simplifies the key exchange process, especially when communication parties are human beings. For example, the buyer can easily verify the seller identity information, which is also his key, if this information is the seller's registered number appeared on the payment counter.

This security solution can be extended to work with the buyer's multiple credential keepers, each of which can hold information for some of the buyer's payment credentials. Secure communications between the buyer and those keepers can be done using identity-based cryptography via GPRS link of his mobile phone or even with SMS. The credential keepers can also be service providers instead of the home gateway as proposed in the paper.

2.1.2 Security and Reliability in Sensor Networks

Security and reliability issues in sensor networks are addressed in our Paper C and D. We focus on routing problems in sensor networks. Paper C proposes a novel solution to tackle the shadow zone phenomenon that is inherent in underwater environments. The proposed solution improved reliability and availability in underwater sensor network communication. Paper D introduces a new solution for secure multicast routing in wireless sensor and actuator networks. It helps to reduce energy consumption while keeping the communication among the network nodes secure.

The following two sections summarize the content of Paper C and D.

Paper C: A Shadow Zone Aware Routing Protocol for Undersea Acoustic Sensor Nodes with Power Controlled and Movable Transducer

This paper presents a novel solution to tackle shadow zone problems to increase reliability and availability in underwater sensor network communications. Due to the characteristics of underwater environments, signals transmitted between different depths are bended as the consequence of changing velocity. This bending of signals when travelling might create shadow zones. A shadow zone in respect to one signal source is the area where signals from that source cannot reach due to signal bending, even though that area is within line-of-sight and coverage of that signal source. Another reason that creates shadow zones is the presence water masses with different temperatures, which sometimes appear in the underwater environment. Those water masses also cause signal transmission changed or disrupted. The presence of shadow zones makes communication in a underwater sensor network disrupted and thus, affects the performance of the network.

Our work presented in Paper C addresses this shadow zone problem by proposing a scheme in which disconnected sensor nodes in a shadow zone can actively move out of that shadow zone to re-establish connection and thus, keeping network connections going through them alive. To guarantee that a sensing task is still performed in that shadow zone area, we introduce a new design of sensor nodes, in which the sensing module and communication module are separated. In the

case that movement is needed, a sensor node only moves its communication module out of a shadow zone.

Simulations have been done to evaluate the performance of our scheme. Since our proposal is the first one that tackles the shadow zone phenomenon, no similar scheme is available to compare. We, therefore, compare our scheme with an existing one that is not shadow zone aware. The performance evaluation shows that our scheme provides higher network connectivity, higher event delivery ratio and smaller packet delay compared to the other one.

Paper D: A Secure Many to Many Routing Protocol for Wireless Sensor and Actuator Networks

This paper proposes a solution for secure multicast routing in sensor and actuator networks. The work uses authenticated broadcast to prevent malicious nodes from injecting incorrect routing information. Our work particularly focuses on optimizing energy consumption of network nodes and prolonging nodes life time. This work is among the first that address secure multicast routing in sensor networks and is possibly the first proposal for secure multicast routing in sensor and actuator networks.

In our work, the network model is represented by a base station, a number of event sources, actuators and sensor nodes. There are also a number of events and each actuator is interested in more than one events. Each actuator broadcasts its interested events and network nodes form registration and routing tables based on the messages received from actuators. Nodes send interested events to the registered actuators using secure multicast communications, thus reduce the energy consumption per event. The security of our protocol relies on existing security solutions. For example, the authenticated broadcast presented in [53] is used for interest disseminations and key pre-distribution schemes presented in [14], [21], [41] or [53] are used to secure pair-wise communications between nodes.

2.2 Open Problems

The works presented in this thesis are not fully complete and still open for further research. The following parts show open areas where further research can be done. The first two problems relate to our work in identity-based cryptography while the last two relate to our work in underwater sensor networks.

Complete Identity-based Cryptography Solution The works in our Paper A and B are not complete. Possible extensions of those works can be developments of complete solutions for those ideas. A prototype for mobile payment application, for example, can be develop with the support from PDAs and WLANs. A real prototype based one real working conditions is also a possible future research.

Identity-based Cryptography and Identity Management Identity management is a broad area related to provide, manage and control the identity of entities, e.g. human beings. The goal of identity management is to provide appropriate services/resources to appropriate entities. Beside social aspects, identity management, in security perspective, is a lot more related to access control. Thus, the combination of identity management and identity-based cryptography can be an ideal candidate to provide a good secure identity management solution.

Modeling of Shadow Zone in Underwater Environment Shadow zones can be the results of signal bending when they travel through different depths. A ray tracing model [43] can be used to calculate shadow zones in this case. However, there is currently no tool for modeling shadow zones caused by thermal zones, i.e. the water masses with different temperature compare to the surrounding environment. There is not much information in the literature to model the second kind of shadow zones, which has more influences in underwater sensor network applications. Finding a good model or a good estimation of that model will greatly improve our current solution, which uses simply model to represent shadow zones.

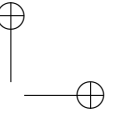
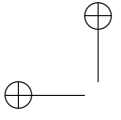
Cooperative Solution to Avoid Shadow Zone In our current solution, network nodes react independently to avoid shadow zone. Though this approach increase network reliability and availability, this approach is not the optimal way. For example, there might be a case when two nodes in each other communication range lost connections and start moving at the same time to different directions. While one node may re-establish connection, the other node might not. In this case, there might be a better solution if only one node moves and the other remains unchanged provided that they are still in the communication range of each other. Another example is network partitioning. In this case, not all the nodes in the disconnected partition need to move to re-establish the connections. Cooperation between nodes for finding the optimal solution to avoid shadow zones is still a challenging problem.

2.3 Conclusion

This PhD work is part of “Secure and Reliable Wireless and Ad hoc Communications” (SWACOM) project under VERDIKT program. The main research focus of this thesis are on two different domains yet relate to the research theme of the project.

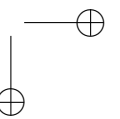
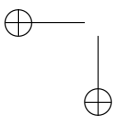
Our work in identity-based cryptography proposes two applications of identity-based cryptography to secure network communications. The first proposal is a solution for securing communications among ZigBee used for control and monitoring applications. The second one is a proposal to secure distributed mobile payment scheme, which provide both security and convenience for the end users.

The research in this thesis is also working toward securing and providing reliable communications for sensor networks, including underwater sensors. We also have two contributions in this working domain. Our work proposes a new routing scheme that tackles shadow zone phenomenon in underwater sensor networks. This scheme improves reliability and availability for underwater sensor applications. Beside the research on underwater sensor networks, we also propose a new solution for energy-efficient secure multicast communication in actuator and sensor networks. This proposal aims at reducing energy consumption while still maintains network security.



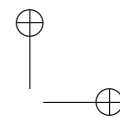
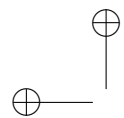
—

—



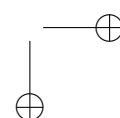
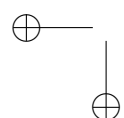
|

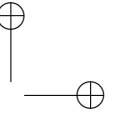
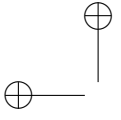
|



Part II

Paper Collection





—

—

