UNIVERSITI PUTRA MALAYSIA

IMPROVED MESSAGE AUTHENTICATION TECHNIQUE ON IEEE 802.15.4 WIRELESS SENSOR NETWORK USING MULTIPLE KEY PROTOCOL

SAIF M. KH. AL-ALAK

FSKTM 2014 7

IMPROVED MESSAGE AUTHENTICATION TECHNIQUE ON IEEE 802.15.4 WIRELESS SENSOR NETWORK USING MULTIPLE KEY PROTOCOL

By

SAIF M. KH. AL-ALAK

Thesis submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Doctor of Philosophy

July 2014

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirements for the degree of Doctor of Philosophy

IMPROVED MESSAGE AUTHENTICATION TECHNIQUE ON IEEE 802.15.4 WIRELESS SENSOR NETWORK USING MULTIPLE KEY PROTOCOL

By

SAIF M. KH. AL-ALAK

July 2014

Chairman: Zuriati Ahmad Zukarnain, PhD

Faculty: Computer Science and Information Technology

Wireless communication is utilized for transferring data over nodes. The Wireless Sensor Network (WSN) is defined to connect the sensors by using a set of protocols. The IEEE 802.15.4 standard includes the required protocols to construct a WSN. The security protocols of the IEEE 802.15.4 support the protection for the WSN; however, the implement of security protocols degrades the performance of the WSN. Also, the encryption system limits the size of the transferred message, since it adopts a single secret key for message ciphering that leads to the possibility of key attack. The authentication algorithm of IEEE 802.15.4 has constraints on a multi processor system, since it can work only in sequential fashion. The aim of the study is to reduce the delay of the authentication operation in WSN and to reduce the possibility of general attack on the ciphertext message in WSN. In this study, the pretest-posttest design is implemented along with the research tests. The implementation of the MKP in the IEEE 802.15.4 WSN increases the flexibility of the cipher transferred message according to the number of secret keys, where each secret key may be used to encrypt 2^{61} blocks (each block is 16-octet) that leads to the increase in the flexibility of the message size.

Meanwhile, the complexity of the secret key is increased, since the number of a mathematical operations to break the secret key is duplicated according to the number of secret keys. Also, the MKP increases the randomness of the ciphertext message, since the message is encrypted with distinct secret keys. Furthermore, the MKP increases the resistance of the ciphertext message against attacks. The DMAC algorithm increases the system utilization for the IEEE 802.15.4 WSN. The DMAC authenticates the messages' block in parallel fashion by utilizing the available processing units. The time of message authentication operation in the IEEE 802.15.4 WSN is decreased by DMAC. The study shows that the developed algorithms MKP-AES and DMAC increase the performance of the WSN and improve the system resistance to attacks on the WSN. The increase of system performance of the WSN improves the efficiency of the WSN. The improvement of the security system of the WSN makes it more trustworthy.

Abstrak tesis yang dikemukakan kepada SenatUniversiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENAMBAHBAIKAN TEKNIK PENGESAHAN MESEJ PADA RANGKAIAN PENGESAN TANPA WAYAR IEEE 802.15.4 MENGGUNAKAN PROTOKOL KUNCI PELBAGAI

Oleh

SAIF M. KH. AL-ALAK

Julai 2014

Pengerusi: ZuriatiAhmadZukarnain, PhD

Fakulti: Sains Komputer danTeknologi Maklumat

Komunikasi tanpa wayar digunakan untuk memindahkan data melalui nod. Rangkaian Pengesan Tanpa Wayar *Wireless Sensor Network* (WSN) digunakan untuk menyambungkan pengesan dengan menggunakan satu set protocol. Piawaian IEEE 802.15.4 termasuk sebagai salah satu protokol bagi membina WSN. Protokol keselamatan IEEE 802.15.4 menyokong perlindungan untuk WSN;walau bagaimanapun, pelaksanaan protokol keselamatan ini telah merendahkan prestasi WSN. Sistem enkripsi juga menghadkan saiz mesej dihantar, memandangkan ianya mengguna pakai kunci rahsia persendirian untuk merahsiakan mesej, ianya terdedah kepada kemungkinan serangan kunci. Algoritma pengesahan IEEE 803.15.4 mempunyai kekangan terhadap sistem pemprosesan yang banyak kerana ia hanya boleh dilaksanakan dalam keadaan berjujukan. Tujuan kajian ini adalah untuk mengurangkan operasi pengesahan dalam WSN dan juga mengurangkan kemungkinan serangan umum terhadap mesej rahsia dalam WSN. Reka bentuk pra dan pasca ujian diguna pakai untuk melaksanakan ujian penyelidikan. Pelaksanaan MKP dengan IEEE 802.15.4 WSN telah meningkatkan fleksibiti terhap kerahsiaan mesej yang dihantar dengan merujuk kepada bilangan kunci rahsia, dimana setiap kunci rahsia digunakan untuk enkrip 2^{61} blok (setiap blok 16-oktet) membolehkan ianya meningkatkan tahap fleksibiliti saiz mesej.

Sementara itu, kerumitan terhadap kunci rahsia meningkat, kerana jumlah operasi matematik untuk memecah kunci rahsia diulang mengikut kepada jumlah kunci rahsia. MKP juga meningkatkan kadar rawak terhadap tulisan rahsia yang terkandung dalam mesej tersebut, kerana mesej di enkrip menggunakan kunci yang berbeza. Tambahan lagi, MKP juga meningkatkan tahap rintangan mesej tulisan rahsia terhadap serangan. Algoritma DMAC meningkatkan tahap penggunaan sistem untuk IEEE 802.15.4 WSN. DMAC mengesahkan blok mesej dalam keadaan selari dengan menggunakan unit pemprosesan yang ada. Masa operasi pengesahan mesej didalam IEEE 802.15.4 WSN dikurangkan oleh DMAC. Kajian ini menunjukkan pembangunan algoritma MPK-AES dan DMAC dapat meningkatkan prestasi WSN dan menambah baik ketahanan sistem terhadap serangan ke atas WSN. Peningkatan sistem prestasi WSN juga meningkatkan tahap kecekapan WSN. Dengan peningkatan sistem keselamatan terhadap WSN, ini membuatkan ianya lebih dipercayai.

ACKNOWLEDGEMENT

In the name of ALLAH, the most gracious and merciful.

I thank ALLAH who gave me the patience and strength during this period of study.

After that, I would like to give my thanks to my supervisor, Associate Professor Dr. Zuriati Ahmad Zukarnain, for providing assistance and guidance to me to complete this research. As well as I would like to thank the members of supervisory committee, Associate Professor Dr. Shamala Subramaniam and Dr. Azizol Abdullah, for giving me their precious time to help me and make this research as better. I would like to give great thanks for my wife (Farah) for her help and support; as well, I thank my parents for their aid during my research.

SAIF M. KH. AL-ALAK

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory committee were as follows:

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Shamala Subramaniam, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Azizol Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Saif M. Kh. Alalak, GS27832

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Associate Prof. Zuriati Ahmad Zukarnain

Signature: _____
Name of Member of Supervisory Committee: Associate Prof. Shamala Subramaniam

Signature: _____
Name of Member of Supervisory Committee: Dr. Azizol Abdullah

Signature: _____
Name of Member of Supervisory Committee:

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

LIST OF ABBREVATIONS

AES	Advanced Encryption Standard
AFH	Adaptive Frequency Hopping
AODV	Ad Hoc On Demand Distance Vector
AWMA	Alternating Wireless Medium Access
BAN	Body Area Network
BO	Beacon Order
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining Message Authentication Code
CBR	Constant Bit Rate
CCM	CTR CBC-MAC
CSMA-CA	Carrier Sense Multiple Access With Collision Avoidance
CTR	Counter
DES	Data Encryption Standard
DMAC	Distributed Message Authentication Code
DoS	Denial of Service
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptosystem
ED	Energy Detection
FFD	Fully Function Device
FPGA	Field Programmable Gate Array
GF	Galois Field
GPU	Graphic Processing Unit
GTS	Guaranteed Time Slot
IDEA	International Data Encryption Algorithm
IEEE	Institute Of Electrical And Electronics Engineers
IV	Initial Vector
KS-test	Kolmogorov-Smirnov test
LEAP	Local Encryption And Authentication Protocol
LK	Link Key
LLC	Logical Link Control
LQI	Link Quality Indication
LR-WPAN	Low Rate Wireless Personal Area Network
MAC	Media Access Control
MK	Master Key
MKP	Multiple Key Protocol
MLME	Mac Layer Management Entity
MPDU	Mac Protocol Data Unit
MDS	Maximum Distance Separable
NIST	National Institute of Standard and Technology
NK	Network Key
NS2	Network Simulator version 2
OCB	Offset Code Book
OSI	Open Systems Interconnection
parfor	Parallel For-Loops
PHY	Physical
PLME	Physical Layer Management Entity
PPDU	Protocol Data Unit
RF	Radio Frequency

RFD	Reduces Function Device
SAP	Service Access Point
SO	Super Frame Order
spmd	Single Program Multiple Data
SSCS	Service-Specific Convergence Sublayer
SUN	Smart Utility Networks
TC	Trust Center
Tesla	Timed Efficient Stream Loss-Tolerant Authentication
UDP	User Datagram Protocol
UWB	Ultra Wide Band
VLC	Visible Light Communication
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
WSNS	Wireless Sensor Network Security

CHAPTER 1

INTRODUCTION

1.1 Background and Motivation

Wireless Sensor Network (WSN) is convenient to be used in various types of applications because it is easy to install, control, and for network access. WSN needs little human interaction, and supports system mobility. Nowadays, most airports, fields of chemical and radiation experiments, and disaster areas prefer to adopt the WSN for communication since human accessibility to these places is difficult.

A WSN consists of a set of connected sensors. The sensor is an electronic or electrical device that is deployed in many fields for information collecting in different environments, and its output is a reflection of the external environment. The sensor is considered an essential unit to construct a WSN, which may consist of thousands of simple and multiple function nodes. Each node collects data from its environment, processes them, and then transfers them over an ad-hoc network to the sink. Furthermore, the WSN has desirable properties such as power saving, nodes mobility, network scalability, convenience, nodes heterogeneity, and ability to cope with node failures. The WSN facilitates those features to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, and motion or pollutants. The WSN has been utilized in many different fields such as industry (for process monitoring and control, as well as health monitoring) and military (for battlefield surveillance).

The WSN as a technology utilizes other communication standards such as IEEE 802.15.4 Wireless Personal Area Network (WPAN) for transferring the data. The IEEE 802.15.4 WPAN standard is considered the basis for many types of WSN applications, for example, ZigBee technology, 6LoWPAN, and WirelessHART. The WSN works with low data rate that consumes reasonable power. Meanwhile, the WSN can be used for collecting data from a hostile environment with a long-life time network.

The IEEE 802.15 is a standard for WPAN that is created by seven kinds of task groups. Each task group is responsible for developing a standard to support one kind of WPAN. The WPAN includes Bluetooth, Coexistence, Ultra Wide Band, ZigBee, Mesh Networking, Body Area Network, and Visible Light Communication. Each kind of WPAN communication belongs to different standards that is developed by one of the task groups as illustrated in Figure 1.1.

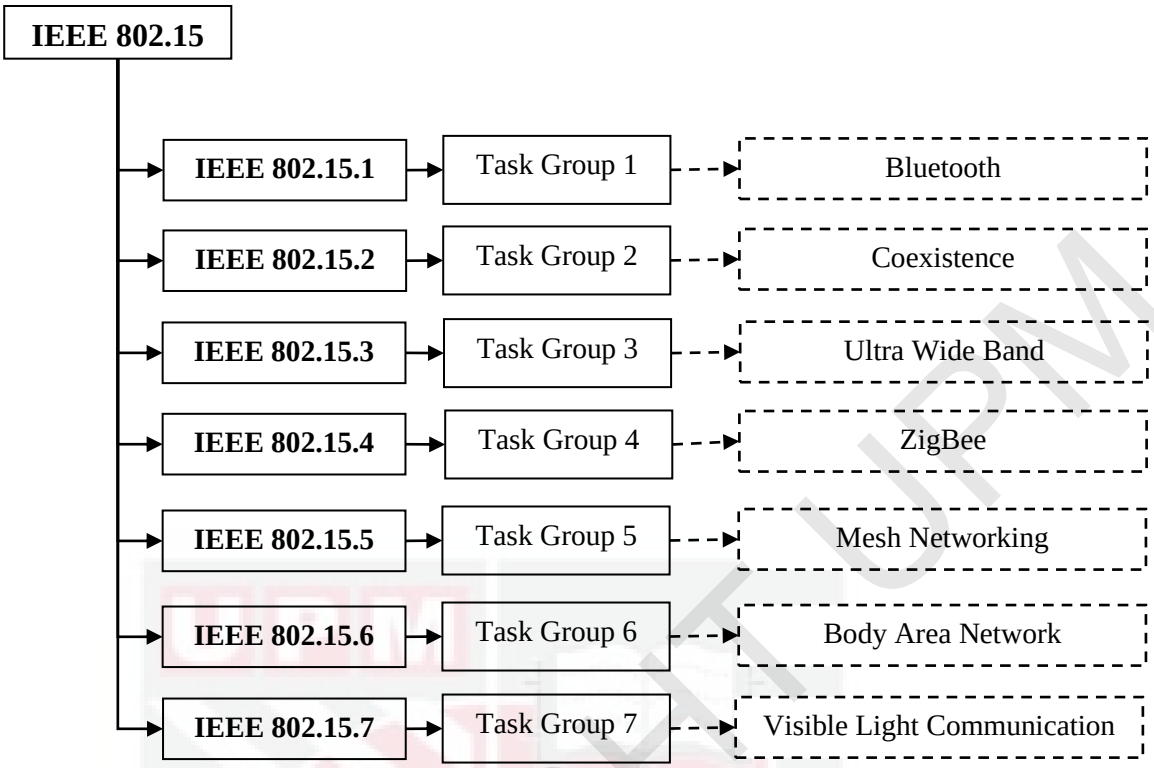

Figure 1.1. Types of WPAN

However, governments and business institutes that adopt the WSN in their projects are very excited to secure the data inside the network. Since the sensitive nature of WSN's data and the environment where the sensors are deployed are unsecured, the companies have been competing to produce a secure WSN. Many security protocols are built to support the security in WSN. The IEEE 802.15.4 standard adopts the AES algorithm in CCM mode to provide message confidentiality and message authentication.

Also, the sensor architecture gives an opportunity to the network attackers to access the network, because it has many constrains like computational capabilities, memory, communication bandwidth, and battery power. A sensor's constraints lead to the limitation of its flexibility to utilize the more sophisticated algorithms and protocols to protect the WSN. Hence, running and utilizing cryptographic protocols to provide security services for WSN are challenges as attackers may replay the message and this is sent over a WSN network.

On the other hand, many security schemes have been developed to reduce the influence of an attack on the WSN. There are two types of security algorithms, which are block cipher (symmetric key) and public key cipher (asymmetric key). The security algorithms are utilized to provide protection for the WSN network. The block cipher algorithm uses a secret key to encrypt and decrypt the blocks of data, and the key must be exchanged securely between the data sender and receiver. The public key algorithms are more complicated than block cipher algorithms. Many arithmetic and logical operations are used to calculate the ciphertext from plaintext. Each public key algorithm has two keys, which are public key and private key. On

the sender side, the public key is used for the data encryption. On the receiver side, the private key is used for the data decryption. Normally, the public and private keys are related mathematically to each other.

Most of the network standards employ one of the block cipher algorithms for data confidentiality because the block cipher algorithm is faster than the stream cipher algorithm for encrypting and decrypting operations (Aladdin, 2000). The block cipher algorithm breaks the message into blocks of data, and then encrypts the blocks by a secret key, which must be shared among the entities of the network. There are many block cipher algorithms that have been developed to improve the data confidentiality; for example, Data Encryption Standard (DES) (Standard, 1999), International Data Encryption Algorithm (IDEA), RC5 (Rivest, 1995), Blowfish, and AES (FIPS, 2001).

The Low Rate Wireless Personal Area Network (LR-WPAN) adopts the IEEE 802.15.4 WSN (LAN/MAN, 2006) to transfer data over short distances. The IEEE 802.15.4 WSN provides a set of security protocols to protect the information inside the network. Furthermore, the security protocols are implemented in MAC sub layer of the IEEE 802.15.4 standard to provide data confidentiality, data authentication, and protection against replay attacks. The designers of the IEEE 802.15.4 WSN used a set of security algorithms to execute the security protocols.

Moreover, the IEEE 802.15.4 WPAN standard has protocols to provide the confidentiality, authentication, and replay protection requirements to keep the message safe. The IEEE 802.15.4 WPAN utilizes the Advanced Encryption Standard (AES) symmetric key algorithm, with 128-bit key and 16-octet block size, to secure the transferred messages over the WSN network. For authenticating the messages over the network, the IEEE 802.15.4 WPAN adopts Cipher Block Chaining Message Authentication (CBC-MAC) algorithm with an AES algorithm. To explain further, the IEEE 802.15.4 WPAN runs the security protocols in Counter (CTR) with CBC-MAC (CCM*) mode, which enables it to compute the message confidentiality, message authentication, or both . The nonce is used in the IEEE 802.15.4 WPAN network to check that the received message is not replayed.

The LR-WPAN adopts the IEEE 802.15.4 WSN because it is lower in cost and lower power compared to other networks. The importance of cost and power saving for the system pushed the designers of the standard to utilize an efficient security algorithm such as AES. The IEEE 802.15.4 implements the AES under CTR mode to cipher the sensitive data, which means the count value for block encryption would be duplicated many times. However, the frequent use of the same count value in blocks weakens the system security. The secret key is refreshed to reset the count value to zero. (Qianqian & Kejin, 2009) The entity under IEEE 802.15.4 WSN utilizes the secret key for only 2^{61} variants count.

The embedded security protocols in the IEEE 802.15.4 WPAN standard increase the robustness of the WSN against security threats. However, the application of security operations to the message will delay the message inside the node and slow down the network performance. Moreover, the network security protocols degrade the network performance and network lifetime.

The IEEE 802.15.4 WSN security protocol uses the CCM security mode for message encryption and authentication. The CCM security mode adopts the CTR mode for message encryption and CBC-MAC mode for message authentication. In IEEE 802.15.4 WSN, both of CTR and CBC-MAC modes are using the AES algorithm for message encryption and authentication respectively as illustrated in Figure 1.2. The AES can uses single or multiple secret key to encrypt the blocks of the message.

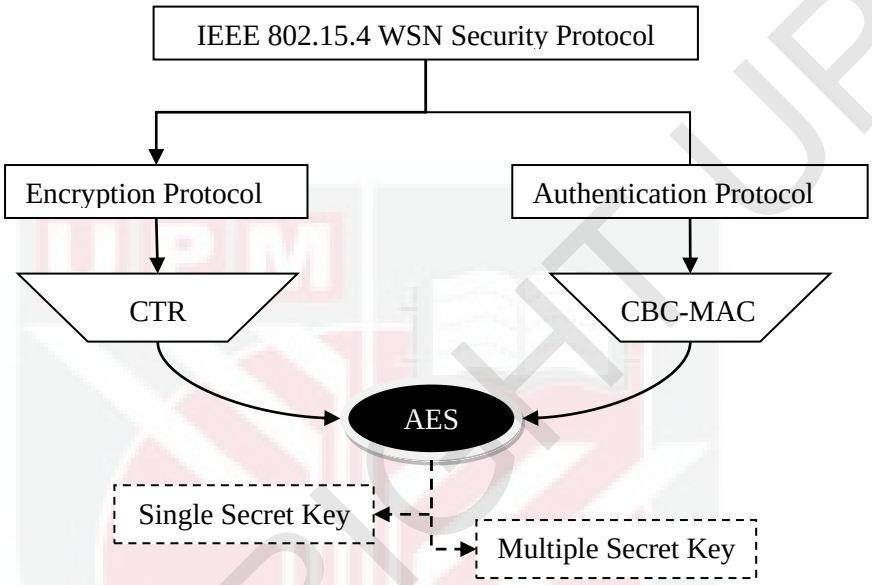

Figure 1.2. IEEE 802.15.4 WSN Security Protocol

1.2 Problem Statement

In the era of Julius Caesar, the eldest crypto-system was invented, and used by the Emperor to cipher the messages to the military leaders. The ciphering methods were developed to diffuse the information and make it incomprehensible for unauthorized people. Nowadays, most of the sensitive information is exchanged over the network, and all types of wire and wireless networks have a security defense system against different types of attack. The network defenses are the security protocols that prevent data from being exposed and intruder access to the sensitive information.

The National Institute of Standards and Technology (NIST) announced that the Rijndael (Daemen & Rijmen, 1999) algorithm is the Advanced Encryption Standard (AES). The AES algorithm consists of a set of transformations. The previous studies focused on developing the transformations of the AES algorithm to increase the security of the AES algorithm. Abuelyman and Alsehibani in (2008), Janadi and Tarah in (2008), Sinha and Arya in (2012), and Hussain et al. in (2010) developed the S-Box transformation. Kamali et al. in (2010) developed a ShiftRows transformation. Ahmed et al. in (2009) developed a MixColumns transformation. Mohan and Reddy in (2012) developed aAddRoundKey transformation. May et al. in

(2002), and Muda et al. in (2010) developed a key transformations. However, none of the previous studies develop a protocol that is able to provide multiple secret keys to increase the security of the AES algorithm.

The CBC-MAC authentication algorithm works in sequential fashion. It adopts the AES algorithm to cipher the blocks of data. Moreover, the AES algorithm can be implemented in a parallel fashion when multiple computing devices are available (Soliman & Abozaid, 2010). However, the AES under CBC-MAC authentication mode in the IEEE 802.15.4 WSN is unable to work in parallel fashion (LAN/MAN, 2006) because each ciphertext block is the input for the next block ciphering operation (Rogaway, 2011).

The IEEE 802.15.4 WSN adopts the CCM to provide security operations such as message encryption and message authentication. The CCM mode has an important parameter L (L $\in$ {2, 3, 4, 5, 6, 7, 8}) that indicates the message size must be less than 2^{8*L} block (LAN/MAN, 2006). However, the use of CCM mode in IEEE 802.15.4 WSN limits the maximum size of the transferred ciphertext message. The CCM mode in IEEE 802.15.4 WSN assigns a single secret key (128-bit) to cipher the sequences of CTR mode. The single secret key can be used to encrypt 2^{61} blocks of a message (the block is 16 byte).The IEEE 802.15.4 WSN must refresh the secret key for ciphering any 2^{61} blocks of a message that leads to reduce the network performance. The IEEE 802.15.4 WSN needs to exchange more than one secret key with the other nodes (sender/receiver) to transfer a big ciphertext message.

The security algorithms are designed to be secure; however, the intruders are trying to attack the weak points of the security algorithms. For AES algorithm in the IEEE 802.15.4 WSN, the complexity of 128-bit key is O($log_2 64$).The attacker needs 2^{64} operations to expose the single secret key of the AES algorithm by the traditional way (Whiting et al. , 2003). The secret key strength of encryption operation in the IEEE 802.15.4 WSN is low that leads to the possibility of attack on the key.

The AES algorithm is considered as the best algorithm in terms of both security and efficiency. The AES (Rijndael) algorithm passed the randomness test by NIST (Soto & Bassham, 2000), where the randomness test represents a measurement for the robustness of the security algorithm. However, there are many types of attack on the AES algorithm, which detects the weak points of the AES algorithm. Brute force attack (Bernstein, 2005) is a traditional way to break the secret key that performs one trial decryption for each key. XSL attack (Cid & Leurent, 2005) is a theoretical attack based on the simple algebraic description for the AES. Related-key attack (Biryukov & Khovratovich, 2009) on the 192-bit and 256-bit versions of AES exploits the simple key schedule. Known-key distinguishing attack (Gilbert & Peyrin, 2010) is a developed version of the start-from-the-middle attack; it works on the 8-round version of AES-128. Chosen-key-relations-in-the-middle (Rijmen, 2009) is one of the attacks on AES. Key-recovery attack (Bogdanov et al., 2011) on full AES is faster than brute force by a factor of about 4. In the IEEE 802.15.4 WSN, the randomness of the ciphertext message from AES encryption algorithm is low, which means the possibility of being attacked.

The AES under CBC-MAC authentication mode is unable to work in a parallel fashion (LAN/MAN, 2006) that means the CBC-MAC algorithm is unable to authenticate the message in parallel. The use of the CBC-MAC algorithm for a message authentication in a multi-processing system leads to lack in system utilization. Codabux-Rossan and Doomun in (Codabux-Rossan & Doomun, 2010) developed a two-way Interleaving CBC protocol to decrease the authentication time by constructing two streams of messages to be authenticated in parallel; however, two secret keys should be exchanged between the sender and receiver nodes for any two messages. The time performance of CBC-MAC message authentication algorithm of IEEE 802.15.4 WSN under multiprocessing system is low.

The security implementation gives some impact on the network performance, and causes the performance degradation. The previous studies showed the impact of security protocols (encryption, authentication) and key exchange protocol on the performance of IEEE 802.15.4 WSN. Daidone et al. in (Daidone et al., 2011) referred to that the security services degrade the performance of IEEE 802.15.4 WSN. Nyamasvisva and Hasbullah in (Nyamasvisva & Hasbullah, 2010) explained that the use of long secret key in the security protocol degrades the performance of IEEE 802.15.4 WSN. Khan et al. in (Khan et al., 2006) showed how the key exchange protocol can reduce the IEEE 802.15.4 system performance. Since the CBC-MAC algorithm in IEEE 802.15.4 WSN authenticates the blocks of a transferred message sequentially, the network performance of IEEE 802.15.4 WSN is reduced due to message authentication implementation.

The problem of the study includes low system performance and low security of IEEE 802.15.4 WSN. The IEEE 802.15.4 WSN has low system performance because it needs to exchange a lot of secret keys to transfer a big ciphertext message, the authentication algorithm is unable to utilize available processing units to parallelize the authentication operation, and the implementation of security protocol delays the message transferring. The IEEE 802.15.4 WSN has low security because it adopts a single 128-bit secret key for message ciphering which is attackable, and the ciphertext message has low randomness.

1.3 Research Objectives

The objective of this study is to develop a Multiple Key Protocol (MKP) and Distributed Message Authentication Code (DMAC) that improve the security of the IEEE 802.15.4 WSN and increases the network performance by reducing the time of message authentication operation, which leads to increase the network throughput and data packet delivery ratio. To achieve the main objective of this study, the following processes are developed:

1. To improve the performance of IEEE 802.15.4 WSN by reducing the number of exchanged secret keys for message encryption and authentication by expanding the maximum size of the encrypted and the authenticated message. The using of the developed protocol (MKP) in the IEEE 802.15.4 WSN provides more than one secret key for message encryption and authentication. The MKP enables the IEEE 802.15.4 WSN to avoid exchanging extra secret keys for encrypting and authenticating a big message.

2. To improve the secret key attack resistance by increasing the strength of the secret key of the encryption and authentication algorithm of IEEE 802.15.4 WSN through using the MKP.

3. To reduce the possibility of attack on the ciphertext message by increasing the randomness of the ciphertext message in the IEEE 802.15.4 WSN through developing the MKP.

4. To improve the system utilization by exploiting the available processing units in parallel message authentication to reduce the time of the message authentication operation in the IEEE 802.15.4 WSN. The DMAC algorithm is used to implement the message authentication in a parallel fashion, where it authenticates the blocks of messages in parallel.

5. To improve the network performance of the IEEE 802.15.4 WSN by using the DMAC algorithm that decreases the impact of message authentication operation on the performance of the WSN. The use of DMAC algorithm for message authentication in IEEE 802.15.4 WSN improves the network performance through increasing the network throughput and delivery ratio of data packet.

1.4 Research Scope

This study focuses on developing a Multiple Key Protocol (MKP) for AES algorithm and testing its impact on the security of the IEEE 802.15.4 WSN. Also, the study develops a Distributed Message Authentication Code (DMAC) algorithm for message authentication and tests the impact of DMAC algorithm on the performance of IEEE 802.15.4 WSN.

The network security system includes data confidentiality, data authentication, and replay attack prevention. The ciphertext randomness is tested and key strength is analyzed. The message authentication time is tested over multi core CPU device and its influence on the performance of the IEEE 802.15.4 WSN environment is computed. The tested performance metrics for WSN environment include throughput time and data packet delivery ratio.

The length of the key of the AES algorithm limits the number of rounds for each plaintext block during ciphering operation. In this study, the researcher considers the AES algorithm with key length of 128-bit and 16-octet block size. The reason behind the choosing of the AES with 128-bit key is that it has proven its efficiency and secrecy through the tests done by NIST competition.

The diehard is used to test the ciphertext randomness, since it is the best statistical test for data randomness measurement. The MATLAB is utilized to measure the authentication time over multi core CPU system, since it supports multiprocessing and multiprogramming. The NS2 is used to test the IEEE 802.15.4 WSN performance, since NS2 is a popular network simulator for network performance measurement.

1.5 Research Contributions

The contributions of this study include security and performance improvement for IEEE 802.15.4 WSN. Thus, the features of the proposed algorithms MKP-AES and DMAC in this study are the following:

1. **Maximum size of the ciphertext message for CCM mode is expanded**: The maximum size of the secured transferred message over IEEE 802.15.4 WSN is limited for single secret key to ensure security. It is increased when the MKP is used for message ciphering in CCM mode.
2. **Attack resistance of secret key of AES algorithm is strengthened**: The key strength refers to the number of mathematical operations that are needed to expose the key of the security algorithm. The use of the MKP improves the key complexity of the cryptography system.
3. **Randomness of the ciphertext of AES algorithm is increased**: The randomness is the measurement of the robustness for the security algorithm. Normally, the AES algorithm utilizes a single secret key to cipher the plaintext. The proposed MKP uses multiple secret keys to generate the ciphertext and the secret keys are computed by using a public key cryptosystem.
4. **Time of message authentication operation in CCM mode is reduced**: The reduction of the authentication time influences the network cost. The message authentication is implemented in a parallel fashion. The DMAC algorithm distributes the message authentication computations among the available computing elements, since the MKP protocol provides multiple secret keys.
5. **WSN network performance is improved:** The performance improvement of the network has some criteria like throughput and data packet delivery ratio. The network throughput is the measurement for transferred data in a unit of time in the network. The data packet delivery ratio is the percentage ratio of the transferred data packet to the received packet in the network. The use of the MKP-AES algorithm and DMAC algorithm in IEEE 802.15.4 WSN improves the network throughput and data packet delivery ratio.

1.6 Organization of the Thesis

This thesis is divided into seven chapters, according to the second writing style in UPM thesis preparation guide (year 2010). The contents of each chapter are described as follows:

Chapter 1 introduces the WSN communication and briefly defines its structure. The motivation and applications for WSN are mentioned. The security protocol and algorithms that are utilized by the WSN are defined. The IEEE 802.15.4 standard security protocols are introduced and the algorithms that are used to provide security of IEEE 802.15.4 standard are presented.

Chapter 2 reviews the wireless personal area network standards and explains the IEEE 802.15.4 standard briefly. The characteristics, topology, structure, types and security protocols that belong to IEEE 802.15.4 standard are mentioned. The performance studies for IEEE 802.15.4 WSN are surveyed. The studies related to the impact of security protocol over IEEE 802.15.4 WSN system performance are

mentioned. The network security algorithm is reviewed and the types of security algorithm and security mode of operations are discussed. The AES algorithm as the best block cipher algorithm is explained in detail and the other works that are related to AES algorithm are mentioned as well. The ECC algorithm is briefly explained and its features are mentioned with its related works.

Chapter 3 gives an account of how the research is designed and describes the research instruments, procedure, implementation, and analysis. It shows the parameters for the three tests (Randomness test, Authentication Time test, and Network Performance test).

Chapter 4 describes the MKP-AES algorithm, and explains how it works. The key generation and ciphering operations are explained. It proves that the use of MKP protocol increases the randomness of AES algorithm, which is one of the research contributions. It shows the results of two experiments. It also describes the research instrument used to conduct the experiments, which is the diehard software, and explains the implementation details of the experiments. The data analysis part is explained at the end of the chapter.

Chapter 5 describes the DMAC algorithm. It explains how authentication operation is done by DMAC algorithm and how the messages are distributed over the available processing units. It proves that the DMAC algorithm reduces the time of message authentication operation in CCM mode on multiple processing units system by utilizing the available processing units to implement the message authentication operation in parallel, which is one of the research contributions. It shows the results of four experiments. It also describes the research instrument used to conduct the experiments, which is the multiprocessing tools of MATLAB software, and explains the implementation details of the experiments. The data is analyzed at the end of the chapter.

Chapter 6 proves that the use of DMAC algorithm for message authentication of IEEE 802.15.4 WSN improves the performance of WSN by reducing the message delay during message authentication operation, which is another research contribution. It examines two performance metrics, which are network throughput and data packet delivery ratio. It shows the results of two experiments and also describes the research instrument used to conduct the experiments, which is the NS2 software, and explains the implementation details of the experiments. At the end of the chapter, the data is analyzed.

Chapter 7 reviews the overall significance of the study, and concludes the findings of the study according to the objective set. It also acknowledges the limitations of the study, and suggests recommendations for future research.

REFERENCES

Abuelyman, E. S., & Alsehibani, A. A. S. (2008). An Optimized Implementation of The S-Box using Residue of Prime Numbers. *International Journal of Computer Science and Network Security, 8*(4), 304-309.

Ahmed, A. S. (2009). An Evaluation of Security Protocols on Wireless Sensor Network. *internet] available at URL:<http://www. cse. tkk. fi/en/publications/B/5/papers/ahmed_final1. pdf>,[accessed on 8th November 2009]*.

Ahmed, E., Shaaban, E., & Hashem, M. (2009). *Lightweight Mix Columns Implementation For AES*. Paper presented at the Proceedings of the nineth WSEAS International Conference on Applied Informatics and Communications (AIC '09), Moscow, Russia, August 20-22, 2009

Akdemir, K., Dixon, M., Feghali, W., Fay, P., Gopal, V., Guilford, J., Zohar, R. (2010). Breakthrough AES Performance with Intel AES New Instructions,*internet] available at URL:<https://communities.intel.com/docs/DOC-5003>, [accessed on 1stSeptember 2013]*.

Aladdin, K. S. L. (2000). The Enduring Value of Symmetric Encryption.*internet] available at URL:<http://etoken.mikrobeta.com.tr/PDF/WP-SymmetricEncryption.pdf>, [accessed on 1stSeptember 2013]*.

Alani, M. M. (2010). Testing Randomness in Ciphertext of Block-Ciphers using DieHard Tests. *International Journal of Computer Science and Network Security, 10*, 53-57.

Barkan, E., & Biham, E. (2002). In How Many Ways Can You Write Rijndael? *Advances in Cryptology—ASIACRYPT 2002*, 160-175.

Bernstein, D. J. (2005).*Understanding Brute Force*.Paper presented at the Symmetric Key Encryption Workshop in Aarhus, Denmark.

Biryukov, A., & Khovratovich, D. (2009). Related-key Cryptanalysis of the Full AES-192 and AES-256. *Advances in Cryptology–ASIACRYPT 2009*, 1-18.

Bloom, B. H. (1970). Space/Time Trade-Offs In Hash Coding With Allowable Errors. *Communications of the ACM, 13*(7), 422-426.

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique Cryptanalysis of the Full AES. *Advances in Cryptology–ASIACRYPT 2011*, 344-371.

Bougard, B., Catthoor, F., Daly, D. C., Chandrakasan, A., & Dehaene, W. (2005). *Energy Efficiency of the IEEE 802.15.4 Standard In Dense Wireless Microsensor Networks: Modeling And Improvement Perspectives.* Paper presented at the International Conference on Design, Automation and Test in Europe, Munich, Germany.

Brown, R. G., Eddelbuettel, D., & Bauer, D. (2012). Dieharder: A Random Number Test Suite Retrieved 20 Sept., 2012, from http://www.phy.duke.edu/~rgb/General/dieharder.php

Buratti, C., Conti, A., Dardari, D., & Verdone, R. (2009). An Overview on Wireless Sensor Networks Technology and Evolution. *Sensors, 2009*(9), 6869-6896. doi: 10.3390/s90906869

Caltagirone, C., & Anantha, K. (2003). *High Throughput, Parallelized 128-Bit AES Encryption in A Resource-Limited FPGA*. Paper presented at the Proceedings of the Fifteenth Annual ACM symposium on Parallel algorithms and architectures, San Diego, California, USA.

Cid, C., & Leurent, G. (2005). An Analysis of the XSL Algorithm. *Advances in Cryptology-ASIACRYPT 2005*, 333-352.

Codabux-Rossan, Z., & Doomun, M. R. (2010). Performance of Interleaved Cipher Block Chaining in CCMP. *Novel Algorithms and Techniques in Telecommunications and Networking*, 53-58.

Daemen, J., & Rijmen, V. (1999). AES Proposal: Rijndael. *First Advanced Encryption Standard (AES) Conference*, from *http://ftp.csci.csusb.edu/ykarant/courses/w2005/csci531/papers/Rijndael.pdf*

Daidone, R., Dini, G., & Tiloca, M. (2011). *On Experimentally Evaluating the Impact of Security on IEEE 802.15.4 Networks*. Paper presented at the International Conference on Distributed Computing in Sensor Systems and Workshops, Barcelona.

Di Francesco, M., Anastasi, G., Conti, M., Das, S. K., & Neri, V. (2011). Reliability and Energy-Efficiency in IEEE 802.15.4/ZigBee Sensor Networks: An Adaptive and Cross-Layer Approach. *Selected Areas in Communications, IEEE Journal on, 29*(8), 1508-1524.

Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *Information Theory, IEEE Transactions on, 22*(6), 644-654.

Dworkin, M. (2001). Recommendation for Block Cipher Modes of Operation. Methods and Techniques: DTIC Document.

Dworkin, M. (2004). 800-38C, Recommendation for Block Cipher Modes of Operation-The CCM Mode for Authentication and Confidentiality *NIST Special Publication*.

Edoh, K. D. (2004). *Elliptic Curve Cryptography: Java Implementation*. Paper presented at Proceedings of the 1st annual conference on Information security curriculum development (InfoSecCD '04). New York, USA.

Ehrsam, W. F., Meyer, C. H. W., Smith, J. L., & Tuchman, W. L. (1978). Message Verification and Transmission Error Detection By Block Chaining, 4074066. US Patent.

ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.*Information Theory, IEEE Transactions on, 31*(4).

FDK, C. (2003). The Evaluation of Randomness of RPG100 by Using NIST and Diehard Tests. Retrieved from http://www.fdk.co.jp/cyber-e/pdf/HM-RAE104.pdf

FIPS, N. (2001). 197: Announcing the Advanced Encryption Standard (AES). *Information Technology Laboratory, National Institute of Standards and Technology*.

FIPS, P. (2000). 186-2. Digital Signature Standard (DSS). *National Institute for Standards and Technology*.

Gao, A., Wei, W., & Xiao, X. (2010). Multiple Hash Sub-Chains: Authentication for the Hierarchical Sensor Networks. *Information. Technoogy Journal*, *9*, 740-748.

Gilbert, H., & Peyrin, T. (2010). *Super-Sbox Cryptanalysis: Improved Attacks for* AES-Like Permutations. Paper presented at proceedings of the 17th international conference on Fast software encryption(FSE'10), Seokhie Hong and Tetsu Iwata (Eds.). Springer-Verlag, Berlin, Heidelberg, 365-383.

Gupta, R., karan Singh, J., & Tiwari, M. (2012). Simulation of AES Encryption and Decryption Algorithm with Parallel Data Execution. *International Journal of Electronics Communication and Computer Engineering , 3*(3), 254-258.

Hussain, I., Shah, T., & Mahmood, H. (2010). A New Algorithm To Construct Secure Keys For AES. *International Journal of Contemporary Mathematical Sciences, 5*(26), 1263-1270.

IEEE. (2003a). *IEEE 802.15.3 Working Group– Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications For High Rate Wireless Personal Area Networks (WPAN) IEEE Draft Standard*. USA: IEEE Inc.

IEEE. (2003b). *IEEE Recommended Practice for Information Technology-Telecommunications And Information Exchange Between Systems-Local And Metropolitan Area Networks-Specific Requirements Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands*. USA: IEEE Inc.

IEEE. (2005). *IEEE Standard for Information Technology-Telecommunications And Information Exchange Between Systems-Local And Metropolitan Area Networks-Specific Requirements Part 15.1: Wireless Medium Access Control (MAC) And Physical Layer (PHY) Specifications For Wireless Personal Area Networks (WPANs)*. USA: IEEE Inc.

IEEE. (2009). *IEEE Recommended Practice For Information Technology-Telecommunications and Information Exchange Between Systems-Local And Metropolitan Area Networks-Specific Requirements Part 15.5: Mesh*

Topology Capability in Wireless Personal Area Networks (WPANs). USA: IEEE Inc.

IEEE. (2011). *IEEE Standard for Local and Metropolitan Area Networks-Part 15.7: Short-Range Wireless Optical Communication Using Visible Light*, USA: IEEE Inc.

IEEE. (2012). *IEEE Standard for Local and Metropolitan Area Networks-Part 15.6: Wireless Body Area Networks*, USA: IEEE Inc.

Innovative-Logic. (2012). AES CCM Encryption and Decryption, 2013, from http://www.inno-logic.com/resources/17.php

Issariyakul, T., & Hossain, E. (2011). *Introduction to Network Simulator NS2*: Springer.

Janadi, A., & Anas Tarah, D. (2008, April 7-11). *AES Immunity Enhancement Against Algebraic Attacks by using Dynamic S-Boxes*. Paper presented at proceeding of ICTTA 2008 3rd International Conference on Information and Communication Technologies: From theory to Applications in Damascus, Syria.

Jorstad, N., & Landgrave, T. (1997). *Cryptographic Algorithm Metrics*.Institute for Defense AnalysesScience and Technology Division, From *<http://csrc.nist.gov/nissc/1997/proceedings/128.pdf>*

Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. (2010, August 1-3). *A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption*. Paper presented at International Conference on Electronics and Information Engineering (ICEIE) in Kyoto, Japan.

Karlof, C., Sastry, N., & Wagner, D. (2004, November 3-5). *TinySec: a Link Layer Security Architecture For Wireless Sensor Networks.* Paper presented at the Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems in Baltimore, Maryland, USA.

Khan, M., Amini, F., Misic, J., & Misic, V. B. (2006, October). *The Cost of Security: Performance of Zigbee Key Exchange Mechanism in an 802.15.4 Beacon Enabled Cluster.* Paper presented at the IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Vancouver, British Columbia, Canada.

Kim, H., Kim, C. H., & Chung, J. M. (2012). A Novel Elliptical Curve ID Cryptography Protocol For Multi-Hop Zigbee Sensor Networks. *Wireless Communications and Mobile Computing, 12*(2), 145-157.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation, 48*(177), 203-209.

Kohvakka, M., Kuorilehto, M., Hännikäinen, M., & Hämäläinen, T. D. (2006, October 2-6). *Performance analysis of IEEE 802.15. 4 and ZigBee for large-scale wireless sensor network applications.* Paper presented at the 3rd ACM

International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous networks-PE, Torremolinos, Malaga, Spain.

Kumar kaushal, P., Sobti, R., & G Geetha, D. (2012). Random Key Chaining (RKC): AES Mode of Operation. *International Journal of Applied Information Systems, 1*, 39-45.

LAN/MAN, S. C. (2006). IEEE Standard for Information Technology-Telecommunications And Information Exchange Between Systems-Local And Metropolitan Area Networks-Specific Requirements--Part 15.4: Wireless MAC and PHY Specifications for Low-Rate WPANs. *Control, 2006*(September), 1-203.

Lee, J. S. (2006). Performance evaluation of IEEE 802.15.4 for Low-Rate Wireless Personal Area Networks. *Consumer Electronics, IEEE Transactions on, 52*(3), 742-749.

Lenstra, A. K., & Verheul, E. R. (2001). Selecting Cryptographic Key Sizes. *Journal of cryptology, 14*(4), 255-293.

Li, Z. R., Zhuang, Y. Q., Zhang, C., & Jin, G. (2009). Low-Power and Area-Optimized VLSI Implementation of AES Coprocessor for Zigbee System.*The Journal of China Universities of Posts and Telecommunications, 16*(3), 89-94.

Lopez, J., & Dahab, R. (2000). An Overview of Elliptic Curve Cryptography. [internet] available at URL:<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.37.2771&rep=rep1&type=pdf>,[accessed on 1st September 2013].

Luk, M., Mezzour, G., Perrig, A., & Gligor, V. (2007, April 25 - 27). *MiniSec: A Secure Sensor Network Communication Architecture*. Paper presented at the Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on.Cambridge, Massachusetts, USA.

Lupu, T. G., Rudas, I., & Mastorakis, N. (2009). *Main types of Attacks in Wireless Sensor Networks.* Paper presented at the Proceedings of the 9th WSEAS International Conference on Signal, Speech and Image Processing, and 9th WSEAS International Conference on Multimedia, Internet and Video Technologies, Budapest, Hungary.

Marandin, D. Retrieved October 10, 2012, from http://www.ifn.et.tu-dresden.de/~marandin/ZigBee/ZigBeeSimulationEnvironment.html#simulation-7

MathWorks. (2012). Parallel Computing Toolbox TM User ' s Guide Retrieved 1 January 2012, 2012, from http://www.mathworks.com/help/pdf_doc/distcomp/distcomp.pdf

May, L., Henricksen, M., Millan, W., Carter, G., & Dawson, E. (2002). *Strengthening the Key Schedule of the AES*.In L. Batten & J Seberry (Eds.),

Information Security and Privacy (Vol. 2384, pp. 226-240): Springer Berlin Heidelberg

Mišić, J., & Mišić, V. B. (2008). *Wireless Personal Area Networks: Performance, Interconnections And Security with IEEE 802.15.4* (Vol. 3): John Wiley & Sons Inc.

Mohan, H., & Reddy, A. R. (2012). Revised AES and Its Modes of Operation. *International Journal of Information Technology, 5*(1), 31-36.

Muda, Z., Mahmod, R., & Sulong, M. (2010). Key Transformation Approach for Rijndael Security. *Information Technology Journal, 9*(2), 290-297.

Murphy, S., & Robshaw, M. (2002). Essential Algebraic Structure Within the AES. *Advances in Cryptology—CRYPTO 2002*, 1-16.

Nyamasvisva, T., & Hasbullah, H. (2010, June 15-17). *Multi-level security Algorithm for Random ZigBee Wireless Sensor Networks.* Paper presented at the International Symposium in Information Technology (ITSim), Kuala Lumpur, Malaysia.

Perrig, A., Canetti, R., Tygar, J. D., & Song, D. (2002). The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes, 5*(2), 2-13.

Perrig, A., Szewczyk, R., Tygar, J., Wen, V., & Culler, D. E. (2002). SPINS: Security Protocols for Sensor Networks. *Wireless networks, 8*(5), 521-534.

Qianqian, M., & Kejin, B. (2009). *Security Analysis for Wireless Networks Based on ZigBee*. Paper presented at the Information Technology and Applications, 2009. IFITA'09. International Forum on.

Rabah, K. (2005). Theory and Implementation of Elliptic Curve Cryptography. *Journal of Applied Sciences(Pakistan), 5*(4), 604-633.

Rijmen, V. (2009, December 6-10). *Practical-Titled Attack on AES-128 Using Chosen-Text Relations.* Paper presented at the ASIACRYPT, Tokyo.

Rivest, R. (1995). The RC5 Encryption Algorithm. In B. Preneel (Ed.), *Fast Software Encryption* (Vol. 1008, pp. 86-96): Springer Berlin Heidelberg.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Rogaway, P. (2011). Evaluation of Some Blockcipher Modes of Operation: Technical report, Cryptography Research and Evaluation Committees (CRYPTREC).

Shao, F., Chang, Z., & Zhang, Y. (2010, February 26-28). *AES Encryption Algorithm Based on the High Performance Computing of GPU.* Paper presented at the Second International Conference on Communication Software and Networks. Singapore.

Sharma, G., & Martin, J. (2009). MATLAB®: A Language for Parallel Computing. *International Journal of Parallel Programming, 37*(1), 3-36.

Sharma, R., Chaba, Y., & Singh, Y. (2010). Analysis of Security Protocols in Wireless Sensor Network. *International Journal of Advanced Networking and Applications, 2*(2), 707-713.

Sinha, S. D., & Arya, C. P. (2012). Algebraic Construction and Cryptographic Properties of Rijndael Substitution Box. *Defence Science Journal, 62*(1), 32-37.

Soliman, M. I., & Abozaid, G. Y. (2010). FastCrypto: Parallel AES Pipelines Extension for General-Purpose Processors. *Neural, Parallel & Scientific Computations, 18*(1), 47-58.

Soto, J., & Bassham, L. (2000). Randomness Testing of the Advanced Encryption Standard Finalist Candidates: DTIC Document.

Srirenganachiyar, V., & Dhaya, R. (2012, April). *Improved Security in Multi AESTHETIC Processor using AES Architecture*. Paper presented at the IJCA Proceedings on International Conference in Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012) ICON3C(5).

Standard, N. (1999). Data Encryption Standard (DES). *Federal Information Processing Standards Publication*.

Timmons, N. F., & Scanlon, W. G. (2004, October4-7). *Analysis of the Performance of IEEE 802.15.4 For Medical Sensor Body Area Networking*. Paper presented at First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks 2004.

Tomoiaga, R., & Stratulat, M. (2010, 22-27 August). *AES Performance Analysis on Several Programming Environments, Operating Systems or Computational Platforms.* Paper presented at the Fifth International Conference on Systems and Networks Communications. Nice, France.

Vanstone, S. A. (2003). Next Generation Security For Wireless: Elliptic Curve Cryptography. *Computers & Security, 22*(5), 412-415.

Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005, March8-12).*Energy analysis of public-key cryptography for wireless sensor networks*. Paper presented at Third IEEE International Conference on PerCom 2005 Pervasive Computing and Communications.

Wang, M. Y., Su, C. P., Horng, C. L., Wu, C. W., & Huang, C. T. (2010). Single-and Multi-Core Configurable AES Architectures for Flexible Security. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, 18*(4), 541-552.

Whiting, D., Housley, R., & Ferguson, N. (2003). Counter With CBC-MAC (CCM) AES Mode of Operation.Submitted to NIST, from

<http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf>.

Xiao, Y., Chen, H. H., Sun, B., Wang, R., & Sethi, S. (2006). MAC Security and Security Overhead Analysis in the IEEE 802.15. 4 Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking, 2006*(2), 81-81.

Yeh, H. L., Chen, T. H., Liu, P. C., Kim, T. H., & Wei, H. W. (2011). A Secured Authentication Protocol for Wireless Sensor Networks using Elliptic Curves Cryptography. *Sensors, 11*(5), 4767-4779.

Yüksel, E., Nielson, H. R., & Nielson, F. (2008). *Zigbee-2007 Security Essentials.* Paper presented at the Proc. 13th Nordic Workshop on Secure IT-systems.

Zaidan, A., Zaidan, B., Al-Frajat, A. K., & Jalab, H. A. (2010). An Overview: Theoretical and Mathematical Perspectives for Advance Encryption Standard/Rijndael. *J. Appl. Sci, 10*(18), 2161-2167.

Zhang, F., Dojen, R., & Coffey, T. (2011). Comparative Performance and Energy Consumption Analysis of Different AES Implementations On a Wireless Sensor Network Node. *International Journal of Sensor Networks, 10*(4), 192-201.

Zheng, J., & Lee, M. J. (2004). A Comprehensive Performance Study of IEEE 802.15.4. *Sensor network operations*, 218-237.

Zhu, S., Setia, S., & Jajodia, S. (2003). *LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks*. Paper presented at the Proceedings of the 10th ACM conference on Computer and communications security, Washington D.C., USA.