

CAPITAL UNIVERSITY OF SCIENCE AND  
TECHNOLOGY, ISLAMABAD



**A Signed-Response Based Node  
Authentication and Data  
Securing Scheme for Wireless  
Sensor Networks**

by

**Muhammad Saud Khan**

A thesis submitted in partial fulfillment for the  
degree of Doctor of Philosophy

in the

Faculty of Computing

Department of Computer Science

2019

# A Signed-Response Based Node Authentication and Data Securing Scheme for Wireless Sensor Networks

By

Muhammad Saud Khan  
(PC111009)

Prof. Dr. Feng Xia

School of Software, Dalian University of Technology, China

Associate Prof. Dr. Mohamed Younis

University of Maryland, Baltimore, USA

Supervisor Name

(Prof. Dr. Noor M. Khan)

Dr. Nayyer Masood

(Head, Department of Computer Science)

Dr. Muhammad Abdul Qadir

(Dean, Faculty of Computing)

DEPARTMENT OF COMPUTER SCIENCE  
CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY  
ISLAMABAD

2019

Copyright © 2018 by Muhammad Saud Khan

All rights reserved. No part of this thesis may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, by any information storage and retrieval system without the prior written permission of the author.

Dedicated to my father who didnt live long enough to see my achievements.



# CAPITAL UNIVERSITY OF SCIENCE & TECHNOLOGY ISLAMABAD

Expressway, Kahuta Road, Zone-V, Islamabad  
Phone: +92-51-111-555-666 Fax: +92-51-4486705  
Email: [info@cust.edu.pk](mailto:info@cust.edu.pk) Website: <https://www.cust.edu.pk>

## CERTIFICATE OF APPROVAL

This is to certify that the research work presented in the thesis, entitled “**A Signed-Response Based Node Authentication and Data Securing Scheme for Wireless Sensor Networks**” was conducted under the supervision of **Dr. Noor Muhammad Khan**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **Department of Computer Science, Capital University of Science and Technology** in partial fulfillment of the requirements for the degree of Doctor in Philosophy in the field of **Computer Science**. The open defence of the thesis was conducted on **January 08, 2019**.

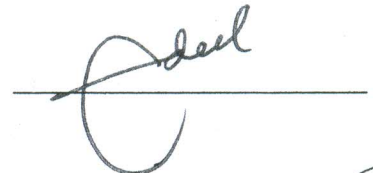
**Student Name :** Mr. Muhammad Saud Khan  
(PC111009)



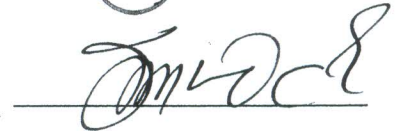
The Examination Committee unanimously agrees to award PhD degree in the mentioned field.

### **Examination Committee :**

(a) External Examiner 1: Dr. Adeel Akram  
Professor  
UET, Taxila



(b) External Examiner 2: Dr. Sajjad A. Madani  
Professor  
COMSATS University, Islamabad



(c) Internal Examiner : Dr. Amir Qayyum  
Professor  
CUST, Islamabad



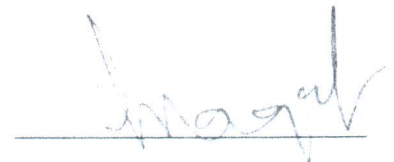
**Supervisor Name :** Dr. Noor Muhammad Khan  
Professor  
CUST, Islamabad



**Name of HoD :** Dr. Nayyer Masood  
Professor  
CUST, Islamabad



**Name of Dean :** Dr. Muhammad Abdul Qadir  
Professor  
CUST, Islamabad



## AUTHOR'S DECLARATION

I, **Mr. Muhammad Saud Khan (Registration No. PC111009)**, hereby state that my PhD thesis titled, '**A Signed-Response Based Node Authentication and Data Securing Scheme for Wireless Sensor Networks**' is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/ world.

At any time, if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my PhD Degree.



**(Mr. Muhammad Saud Khan)**

Dated: *30th* January, 2019

Registration No : PC111009

## PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled “**A Signed-Response Based Node Authentication and Data Securing Scheme for Wireless Sensor Networks**” is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/ cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of PhD Degree, the University reserves the right to withdraw/ revoke my PhD degree and that HEC and the University have the right to publish my name on the HEC/ University Website on which names of students are placed who submitted plagiarized thesis.

Dated: 30<sup>th</sup> January, 2019



---

(**Mr. Muhammad Saud Khan**)  
Registration No. PC111009

## *List of Publications*

It is certified that following publication(s) have been made out of the research work that has been carried out for this thesis:-

1. **M. Saud Khan**, and Noor M. Khan, Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks, *Journal of Sensors*, vol. 2016, Article ID 9783072, 9 pages, 2016.
2. **M. Saud Khan** and Noor M. Khan, SEER: Secure and Energy Efficient Routing in Wireless Sensor Networks, *IEEE Sensors Journal*, Paper Submitted

**Muhammad Saud Khan**

(PC111009)



## *Acknowledgements*

Foremost, I would like to express my sincere gratitude to my advisor Prof. Dr. Noor. M. Khan for the continuous support during my Ph.D. study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me throughout this research and writing of this thesis. I could not have imagined a better advisor and mentor for my Ph.D.

Besides my advisor, I would like to thank my brother-in-law Dr. Laiq Khan who was always ready to help me whenever I was stuck or stressed during my Ph.D.

My sincere thanks also go to Dr. Ahmad Khan and Dr. Zia ur Rehman who guided and helped me cordially. I will be failing in my duties if I do not acknowledge the cooperation of the Dean, Faculty of Computing and the University management, whose co-operation enabled me to conclude my Ph.D. Last but not the least, I would like to thank my family members for their trust and constant encouragement for me to experience new frontiers.

# *Abstract*

During the last decade, authentication of sensor node and secure routing of data been remained an open challenges in Wireless Networks due to their applications in various vulnerable environments. These challenges become more significant when Wireless Sensor Networks (WSN) composed of tiny inexpensive nodes are considered. This is due to the fact that the solutions proposed for the similar purposes in conventional wireless networks cannot be exploited for sensor networks because of high complexities and power consumptions involved in their algorithms.

This thesis proposes a two-fold solution for the issues of node authentication and secure routing in Wireless Sensor Networks. In the first part of the thesis, a low complexity Sybil attack detection mechanism for Wireless Sensor Networks is proposed; while in the second part, a Secure Energy Efficient Routing scheme called SEER is presented for the data security. Both of the proposed schemes are based on the Signed Response (SRes) authentication and voice encryption mechanism developed for Global System for Mobile (GSM) communications. The proposed Sybil attack detection scheme use pre-distributed key embedded in the sensor nodes. A modified version of A3 algorithm used in node authentication produces a SRes with the help of pre-distributed keys against a random challenge number sent by the sink or Cluster Head (CH). The 32 bit SRes is sent back to the sink or CH by the node to prove its legitimacy. The design of node authentication scheme is made flexible so that it can be implemented in both hierarchical and centralized Wireless Sensor Networks. The scheme is analyzed for its performance under various Sybil attacks. The scheme is evaluated for its probability of detecting Sybil nodes when different authentication key pool sizes are utilized. After extensive simulations, it is observed that the proposed scheme is able to counter Sybil attacks with higher probability as compared to notable existing schemes. Moreover, it has also been observed that the proposed Sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same Sybil attack detection performance.

In the second part of the thesis, a secure mechanism for routing of data in Wireless Sensor Networks; SEER is proposed. The proposed protocol is based on A5 encryption scheme developed for voice encryption in GSM. After successful authentication, a modified version of A5 algorithm is used to encrypt data during its routing from source to the sink or relay node. SEER uses GRACE (GRADient Cost Establishment) routing protocol for transmission. For this purpose, a 64-bit ciphering key is used which is produced through a complicated process of perturbation in order to make it harder to be traced. SEER has been tested through simulations in *MATLAB*<sup>®</sup> by setting up hostile and vulnerable Wireless Sensor Network scenarios with respect to data integrity. The results obtained are then compared with two notable existing secure routing protocols. It is proved that the proposed mechanism SEER helps achieve the desired performance under dynamically changing network conditions with various numbers of malicious nodes. Due to its linear complexity, lesser power consumption and more dynamic route updation, the proposed Sybil detection and SEER schemes can be easily extended to cater to the needs of emerging industrial wireless sensor networks, Dust Sensor Networks and IoT. Emerged from the conventional Wireless Sensor Networks, all the aforementioned networks have got the same nature of vulnerabilities and threats along with the inherited limitations with respect to their hardware and processing capabilities.

# Contents

<b>Author's Declaration</b>	<b>iv</b>
<b>Plagiarism Undertaking</b>	<b>v</b>
<b>List of Publications</b>	<b>vi</b>
<b>Acknowledgements</b>	<b>vii</b>
<b>Abstract</b>	<b>viii</b>
<b>List of Figures</b>	<b>xiii</b>
<b>Abbreviations</b>	<b>xv</b>
<b>Symbols</b>	<b>xvi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Overview . . . . .	1
1.2 Components of a Sensor Network . . . . .	2
1.2.1 Sensor Node . . . . .	3
1.2.2 Cluster Head (CH) . . . . .	3
1.2.3 Sink or Base Station . . . . .	4
1.2.4 Beacon . . . . .	5
1.3 Evolution of Wireless Sensor Networks . . . . .	6
1.4 Applications of Wireless Sensor Networks . . . . .	7
1.4.1 Military Applications . . . . .	8
1.4.2 Environmental Applications . . . . .	9
1.4.3 Health Applications . . . . .	9
1.4.4 Home Applications . . . . .	10
1.4.5 Industrial Applications . . . . .	10
1.5 Highlighted Issues in WSN . . . . .	11
1.6 Security in Wireless Sensor Networks . . . . .	12
1.7 Attacks in Wireless Sensor Networks . . . . .	15
1.7.1 Physical Layer Attacks . . . . .	15

---

1.7.2	Link Layer Attacks . . . . .	15
1.7.3	Network Layer Attacks . . . . .	16
1.7.3.1	Spoofing Attack . . . . .	16
1.7.3.2	Selective Forwarding . . . . .	16
1.7.3.3	Sinkhole Attack . . . . .	17
1.7.3.4	Sybil Attack . . . . .	17
1.7.3.5	Wormhole Attack . . . . .	17
1.7.3.6	Blackhole / Grayhole Attack . . . . .	18
1.8	Research Objectives . . . . .	18
1.9	Research Contributions . . . . .	18
1.10	Significance and Application of the Proposed Research . . . . .	19
1.11	Thesis Organization . . . . .	21
<b>2</b>	<b>Related Work</b>	<b>22</b>
2.1	Sybil Attacks in Wireless Sensor Networks . . . . .	23
2.2	Energy Efficient Routing in Wireless Sensor Networks . . . . .	25
2.3	Secure Routing in Wireless Sensor Networks . . . . .	28
2.4	Provision of complexity reduction and energy efficiency in authentication and secure routing . . . . .	30
2.5	Problem Statement . . . . .	31
2.6	Chapter Summary . . . . .	32
<b>3</b>	<b>Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks</b>	<b>33</b>
3.1	Introduction . . . . .	33
3.2	Working of authentication algorithm in GSM . . . . .	34
3.3	The Proposed Signed Response Based Sybil Attack Detection Mechanism . . . . .	36
3.3.1	Network model and assumptions . . . . .	36
3.3.2	Proposed Methodology . . . . .	37
3.3.3	Attack model and defense strategy . . . . .	39
3.4	Probabilistic Model of the Proposed Scheme . . . . .	42
3.5	Results and discussion . . . . .	44
3.5.1	Probability of usable sybil . . . . .	45
3.5.2	Traffic Analysis . . . . .	48
3.5.3	Node power consumption . . . . .	48
3.5.4	Probability of attack detection . . . . .	49
3.6	Chapter Summery . . . . .	49
<b>4</b>	<b>SEER: Secure and Energy Efficient Routing mechanism</b>	<b>51</b>
4.1	Overview . . . . .	51
4.2	Working of A5 algorithm used in GSM . . . . .	54
4.3	The Proposed Secure and Energy Efficient Routing (SEER) . . . . .	56
4.4	Data Encryption Algorithm for the Proposed SEER . . . . .	58
4.4.1	Probability of Interception . . . . .	64

---

4.5	Results and Discussion . . . . .	65
4.6	Chapter Summery . . . . .	67
<b>5</b>	<b>Conclusion and Future Work</b>	<b>69</b>
	<b>Bibliography</b>	<b>71</b>

# List of Figures

1.1	Components of a Sensor Node . . . . .	2
1.2	A sensor network with static infrastructure, data is collected at cluster head and forwarded to the center (sink) . . . . .	4
1.3	A sensor network with a mobile sink. The mobile sink gathers the data by visiting each cluster where the respective cluster head transmit the data after connection establishment. . . . .	5
1.4	ZigBee Protocol Stack. . . . .	7
1.5	various applications of WSN . . . . .	8
1.6	An example of application of WSN in health care . . . . .	10
1.7	Design Issues in WSN . . . . .	13
1.8	Some of the attacks in WSN . . . . .	14
3.1	Authentication Process in GSM . . . . .	35
3.2	Block Diagram of A3 Algorithm Generating 32 bit SRes . . . . .	37
3.3	An Overview of Sensor Network with Sybil Nodes . . . . .	38
3.4	Block Diagram of Proposed Authentication Scheme for Wireless Sensor Networks . . . . .	41
3.5	Successful Probability of at least one Sybil node in a pool of M Sybil nodes . . . . .	44
3.6	Probability of Successful attacks by Sybil nodes . . . . .	45
3.7	Probability that a Sybil Node will go Undetected by the Various Algorithms. . . . .	46
3.8	Simulated Traffic behavior of the WSN while executing the proposed and existing authentication schemes . . . . .	46
3.9	Power Consumption and Remaining Number of Alive Nodes as a Result of Power Consumption by Participating Nodes During the Process of Authentication in Various Algorithms . . . . .	47
3.10	Probability of Sybil Node Detection by the Proposed Algorithm in Comparison with the Existing Algorithms . . . . .	47
4.1	Encryption and Decryption of voice in GSM . . . . .	56
4.2	A: Formation of CIPHERING key . . . . .	57
4.3	B: Final 64 bit CIPHERING key . . . . .	58
4.4	Block diagram of data encryption/decryption in WSN . . . . .	60
4.5	Data Routing in a Wireless Sensor Network With the Presence of Malicious Nodes . . . . .	60
4.6	Lifetime Comparison of SEER with SRCE and ETRAP . . . . .	61

---

4.7	Lifetime Comparison of SEER with SRCE and ETRAP without Energy Harvesting Module with SRCE . . . . .	62
4.8	Energy Consumed by Each sensor node . . . . .	62
4.9	Message exchanged at various number of nodes . . . . .	63
4.10	packet delivery ratio in presence of compromised nodes . . . . .	63
4.11	End to end delay by each protocol . . . . .	63



# Abbreviations

<b>WSN</b>	Wireless Sensor Network
<b>AoI</b>	Angle of Arrival
<b>MEMS</b>	Micro Electrical and Mechanical System
<b>AOI</b>	Area of Interest
<b>CH</b>	Cluster Head
<b>BS</b>	Base Station
<b>BN</b>	Beacon Node
<b>SoSuS</b>	Sound Surveillance System
<b>DSN</b>	Distributed Sensor Network
<b>DARPA</b>	Defense Advanced Research Projects Agency
<b>SN</b>	Sensor Node
<b>WBAN</b>	Wireless Body Area Network
<b>IEEE</b>	Institute of Electrical and Electronic Engineering
<b>WPAN</b>	Wireless Personal Area Network
<b>SRes</b>	Signed Response
<b>GSM</b>	Global System for Mobile
<b>SIM</b>	Subscriber Identity Module
<b>MS</b>	Mobile Station
<b>MSC</b>	Mobile Switching center
<b>HLR</b>	Home Location Register
<b>SEER</b>	Secure and Energy Efficient Routing

# Symbols

$\alpha$	Key Size
$\beta$	Pool size of key
$K_i$	Pre distributed key
$K_a$	Random key generated by Sybil node
$P_{max}$	Conventional and modified gate-to-drain capacitance
$K_c$	Ciphering key
$\Upsilon$	19 bit Shifted in X register
$\Omega$	22 bit Shifted in Y register
$\Psi$	23 bit Shifted in Z register
$maj(x8, y10, z10)$	Major function of registers X,Y and Z

# Chapter 1

## Introduction

### 1.1 Overview

A Wireless sensor network is composed of a large number of sensor nodes that are deployed to monitor an area of interest like environment, medical, industrial, agricultural, security, fire zones and military fields etc. [1]. A Sensor Node is an output of research in advanced Micro-Electro-Mechanical System (MEMS) technology consisting of a power unit, a sensing unit, a processing unit and a communication unit as shown in Fig 1.1. The interaction of these tiny sensor nodes that possess the capabilities of sensing, data processing, aggregation and communication etc. leads to the concept of a Wireless Sensor Network (WSN) in which a large number of sensor nodes communicate wirelessly in a collaborative manner . Due to their diversity and dynamic characteristics, the WSNs have been used in various fields of research and industry. Some of these applications include health monitoring, battlefields surveillance, security, fire zones, factory automation, habitat monitoring, inventory control etc. [2]. Furthermore, the WSNs are mostly used in hostile and vulnerable environments e.g. monitoring of active volcanoes, nuclear reactors, flooded area, collapsed buildings etc. In a WSN, the sensor nodes are deployed either inside the Area of Interest (AoI) or close to its proximity depending upon the nature of its deployment (aerial or manual). To ensure reliability and extend

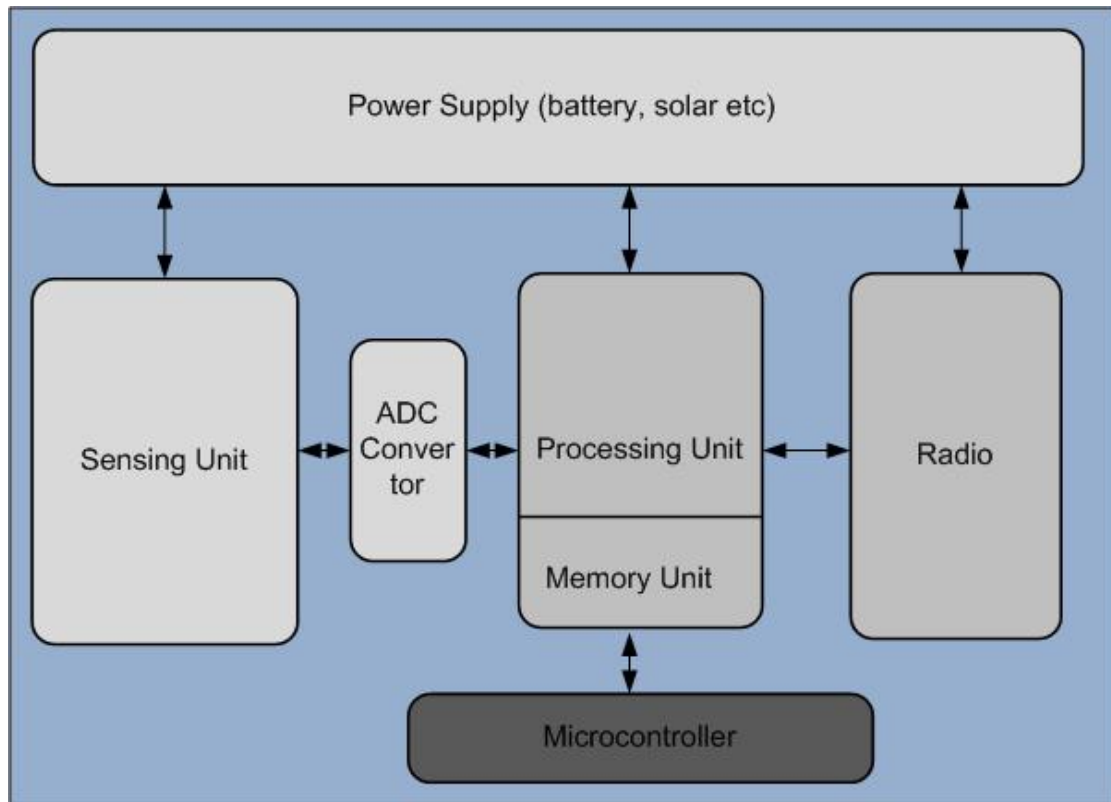


FIGURE 1.1: Components of a Sensor Node

the accuracy in decision making, it is important to extract the right features about the phenomenon from the information provided by the sensor nodes [3].

In a WSN, all nodes are equipped with the abilities of self-organization and connectivity after their deployment . These nodes work in a cooperative manner in a network which mostly involves the collection of raw data in sensor field locally and onward transmission of its processed version to the sink. Only the required data is transmitted to the destination and the undesired or repeated data is discarded . This is done to save energy and processing time of the sensor node as most of the energy is consumed during the transmission and reception of data.

## 1.2 Components of a Sensor Network

The deployment of a WSN is purely subject to the needs, objectives, and geography of the Area of Interest (AOI). However, there are certain responsibilities

inside a WSN which needs to be addressed to achieve accurate results and better management of the network. These responsibilities require some designated components in a network. Some of the very common components of a WSN are discussed below:

### 1.2.1 Sensor Node

A sensor node is the most responsible entity of any Wireless Sensor Network. The accuracy of calculations and results are solely dependent upon the readings provided by the sensor node. A node also has the capabilities of processing and communicating with other nodes. The deployment of sensor nodes may range from tens to hundreds, therefore, its cost is kept as low as possible.

### 1.2.2 Cluster Head (CH)

Although CH is not a core component but some of the sensor networks and their respective routing protocols are widely dependent on it. A cluster head is responsible to handle a region in a distributed WSN. One of the main responsibilities of a CH is to collect data from sensor nodes and to forward it to the destination through other CHs. It can also perform processing to discard duplicate data to save bandwidth and energy. Moreover, the dissemination of control messages and other necessary information among the sensor nodes is also performed by CH. The deployment of CH may or may not be deterministic. In case of deterministic deployment, we can choose the location of a CH and determine the number of nodes to be associated with it. Where as in case of nondeterministic deployment, the location of CH is impossible to determine; therefore, CH is elected by sensor nodes. There are many procedures proposed by researchers for the election of a CH. There may be as many CHs as required in a WSN. All the CHs communicate with each other to route the data and other control messages. Fig 1.2 shows a distributed sensor network with multiple static CHs.

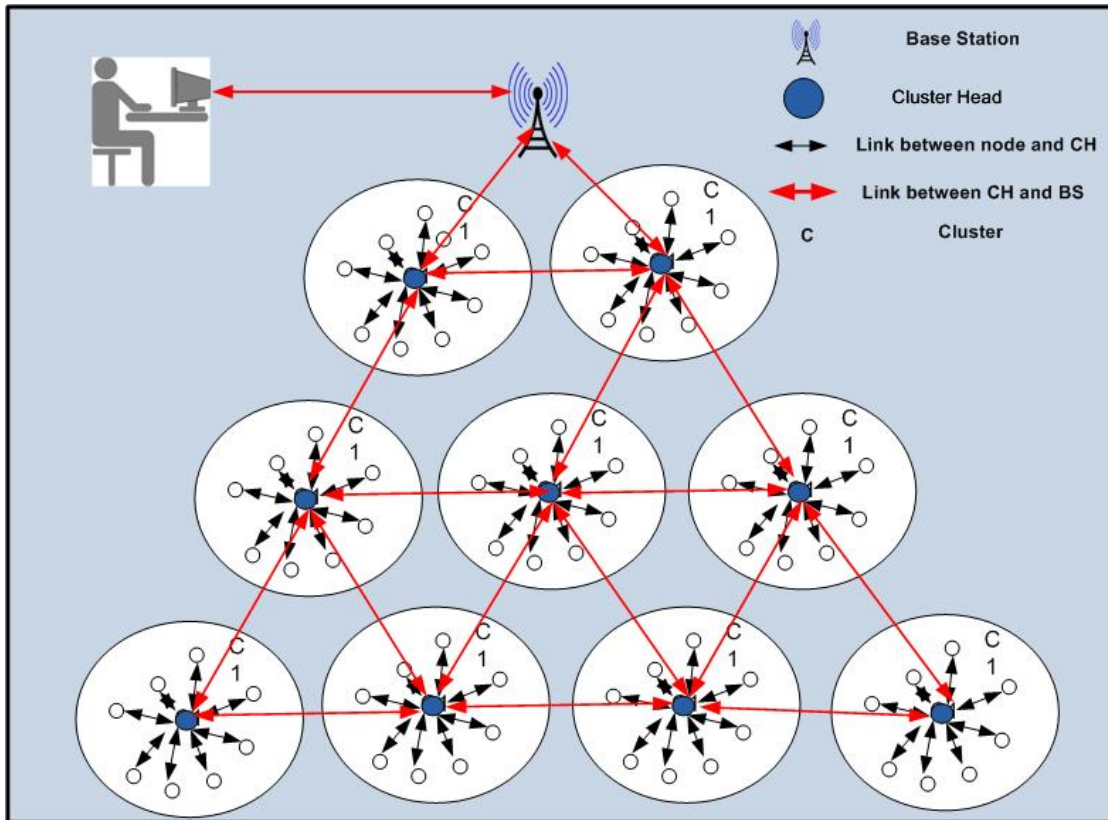


FIGURE 1.2: A sensor network with static infrastructure, data is collected at cluster head and forwarded to the center (sink)

### 1.2.3 Sink or Base Station

A sink has a leading role in a WSN. All the nodes or CHs take instructions for processing from the sink. The data sensed by the nodes is forwarded to sink for onward processing and decision making; therefore, the right placement of sink in the network is very important. The nature of a sink may be static or mobile depending upon the nature of WSN. The static sink collects data form nodes or CHs (which ever applicable). A routing protocol is responsible to ensure the delivery of data from nodes to the static sink. If the sink in a network is mobile then it gathers the data by visiting all the CHs or designated nodes. The mobile sink shown in figure 1.3 is assumed to be a powerful node both with respect to energy and processing. Since a mobile sink collects data from CH at a shorter distance; therefore, it can also help extend the network lifetime by reducing the long ranged communication overhead that usually occurs between CHs and base

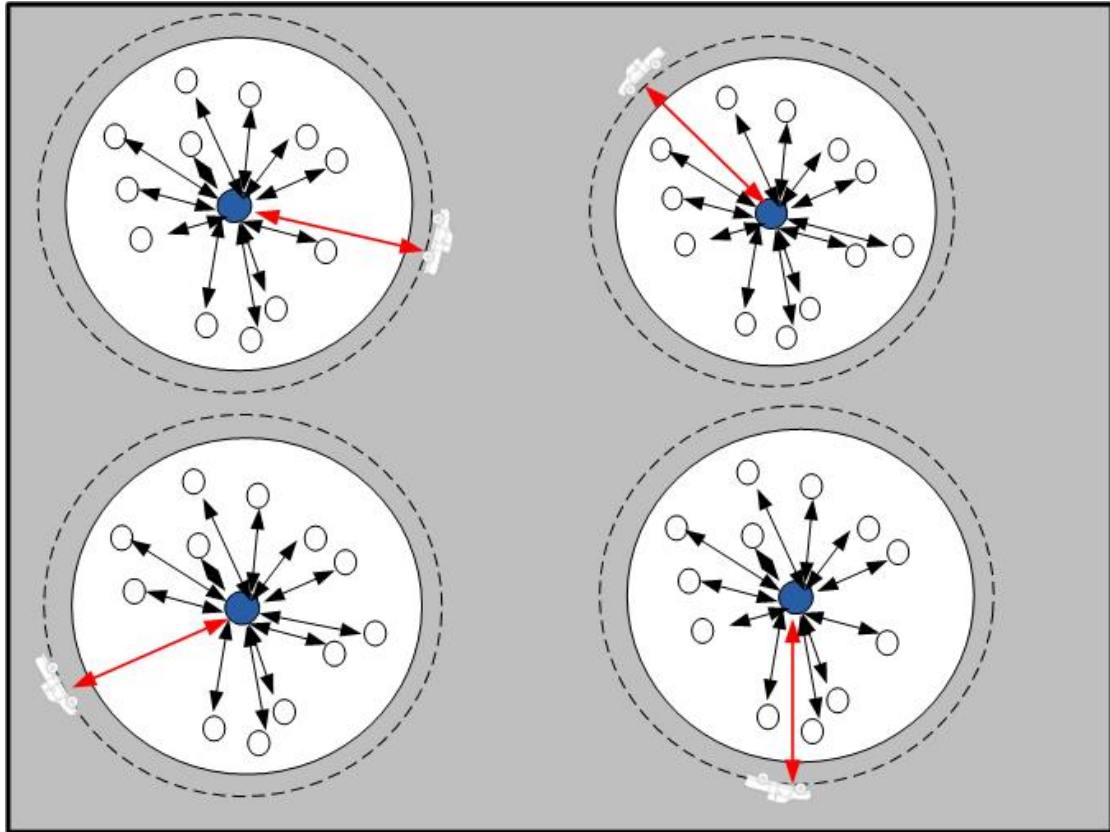


FIGURE 1.3: A sensor network with a mobile sink. The mobile sink gathers the data by visiting each cluster where the respective cluster head transmit the data after connection establishment.

station. Secondly a mobile sink can also act as a bridge between the two disconnected partitions of a network. The Partitions usually occur due to the death of a sensor node lying at a critical location of a WSN. However, a mobile sink requires complex algorithms to control its trajectory. Such algorithms need to monitor real time topology changes. Moreover, the mobile sinks can only be deployed in smooth sensing fields [4] [5].

#### 1.2.4 Beacon

Deployed in deterministic Wireless Sensor Networks, a beacon is a powerful node that can transmit strong signals to communicate with the nodes. Usually, the beacon nodes are used to guide the sensor nodes or help them to calculate their locations [6]. Some of the routing protocols also use beacon concept for the delivery of data towards sink [7].

### 1.3 Evolution of Wireless Sensor Networks

Like all other communication technologies, the WSN also arose as solution to one of ad-hoc and wireless communication problems in defense institution [8]. The very first wireless network that has resemblance to the existing modern WSN is the Sound Surveillance System (SOSUS) developed in 1950 by United States Military. The purpose of SOSUS system was to detect the Soviet submarines and track their movement. The surveillance system was composed of submerged acoustic sensors and hydrophones which was deployed in Atlantic and Pacific oceans. Looking back in the history, the research on WSNs started with Distributed Sensor Networks (DSN) program assigned to Defense Advanced Research Projects Agency (DARPA) in 1980. This was the time when ARPANET has already launched few successful computer networks with over 200 hosts in different universities. The task of DSN was to develop spatially distributed collaborative and autonomously operative sensor network with data routing abilities. The components used in DSN were presented for the first time in Distributed Sensor Net Workshop held in 1978. The components included Sensor Nodes (SN), Communication and processing units and a software to operate the node. Later on, the operating system known as the accent[9] was developed for DSN . The first demonstration of DSN program was a helicopter tracking and monitoring system developed at MIT. In 1998, the WSNs found its position in research community in order to increase its strength and scope of application[10]. Moreover, the cost and size of sensor node became to decrease and with this, the WSN stepped into commercial applications like habitat, vehicular sensor networks, Wireless Body Area Networks (WBAN) etc. Later on, IEEE launched a new standard IEEE 802.15.4 which deals with the low data rate of Wireless Personal Area Network (WPAN). Latter on, the ZigBee alliance published the ZigBee standard which provide a suite of communication protocol and procedures used in low data rate networks as shown in Fig 1.4.



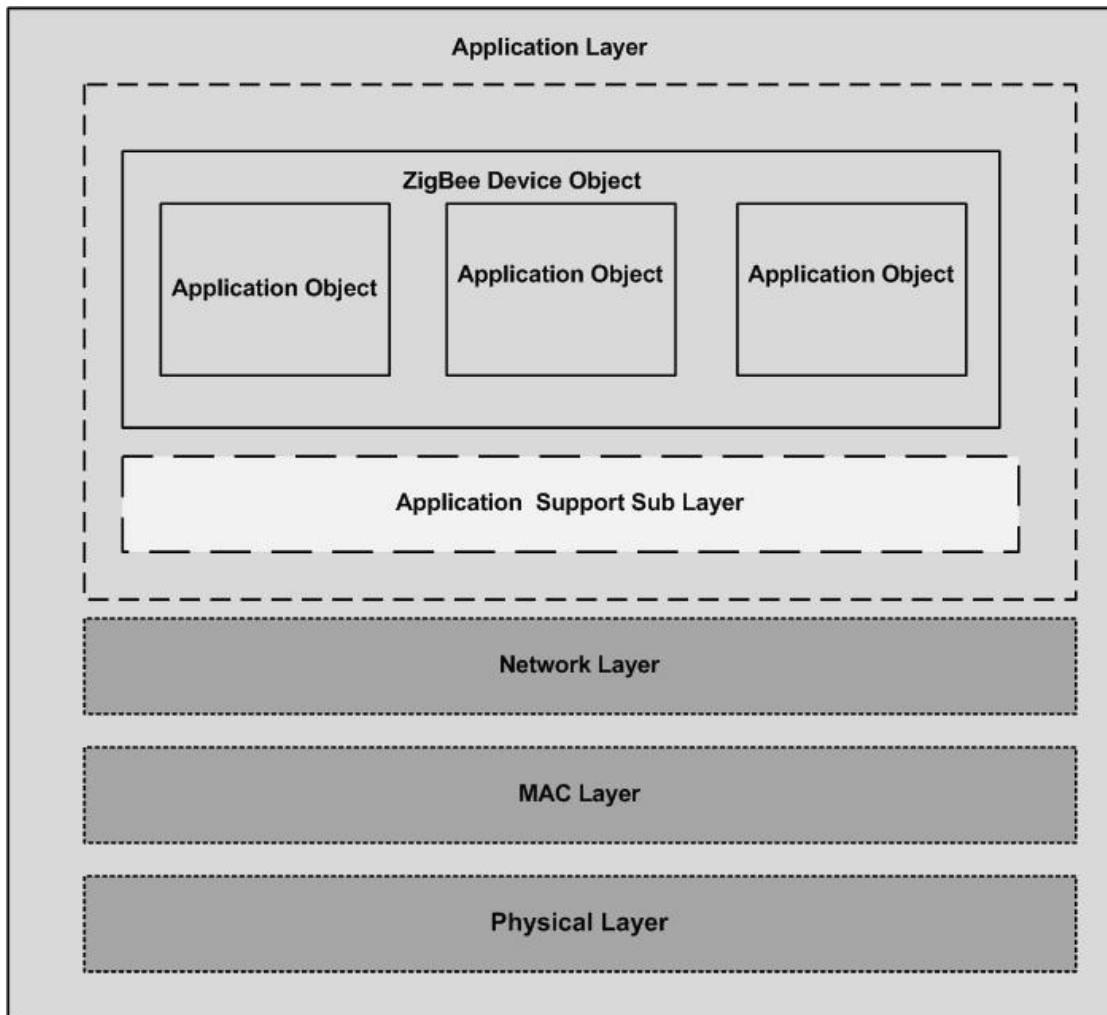


FIGURE 1.4: ZigBee Protocol Stack.

## 1.4 Applications of Wireless Sensor Networks

Currently, the technology of Wireless Sensor Networks has been deployed in various domains for monitoring purposes like health, environment, agricultural, vehicle control, battlefield surveillance and smart grid etc. as shown in Fig 1.5. A wireless sensor networks may consist of various types of sensor nodes like seismic, magnetic, audial, visual, infrared, acoustic, thermal etc., which have the capability to monitor a wide range of ambient conditions [11, 12]

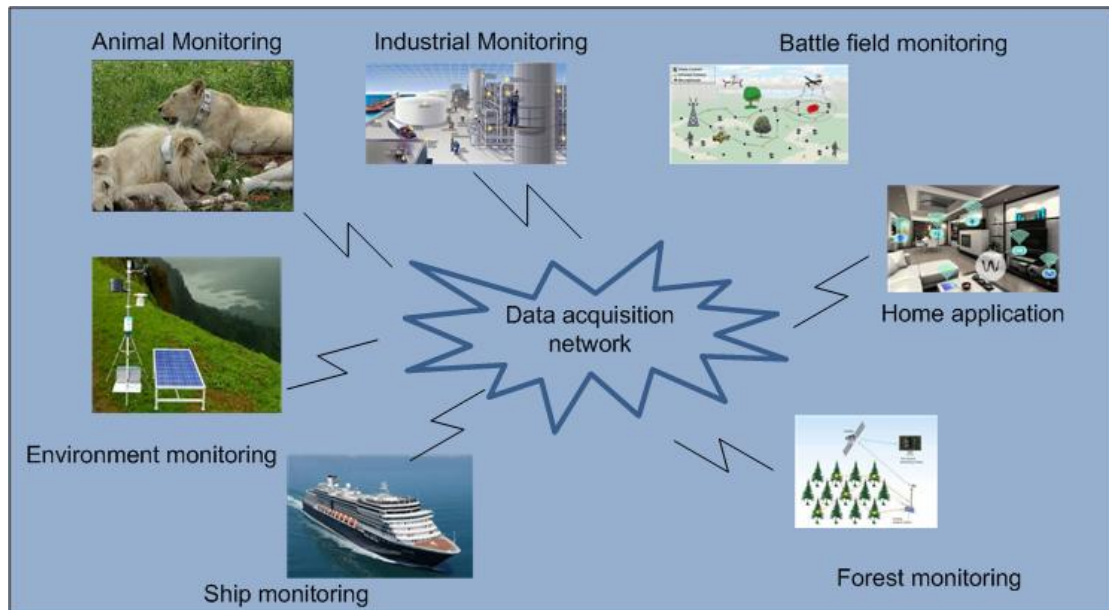


FIGURE 1.5: various applications of WSN

### 1.4.1 Military Applications

WSNs can be an essential part of military operations especially in battlefields. The leaders and commanders can monitor the status battlefield. Sensor nodes are attached to every vehicle, equipment, and soldier etc. to update their status to the high command. Similarly, targeted terrains, supply routes, and logistics etc. of enemy force can be closely observed. New operational plans and decisions can be made through the sensor network deployed in the battlefield. Smart Dust is another project launched by DARPA for military applications which lead to the establishment of dust networks Inc. [13]. The sniper detection system [14] is another example of WSN application in military fields. The system was developed to locate the location of shooter. This system has also been widely used by many countries to ensure public safety. Similarly VigilNet [15] is another surveillance network developed for tracking of objects in hostile areas. Based on Mica2 sensor nodes, the network detects the magnetic fields and its location generated by military vehicles and other objects.

### 1.4.2 Environmental Applications

One of the examples of WSN in environmental applications is the Columbia River Ecosystem (CORIE) developed by the Center for Coastal and Land-Margin Research at the Oregon Graduate Institute USA [16]. The main purpose of CORIE is to monitor the wild life deep down in the river with the help of sensor nodes. WSN is also used to prevent mass destruction caused by a fire in forests. Since these nodes are left unattended soon after deployment therefore they are equipped with power scavenging approaches like solar cells etc. In order to overcome communication obstacles like trees, rocks etc., the sensor node work in a collaborative manner to perform distributed sensing [17] [18] [19]. Some of other environmental applications of WSN include, habitat monitoring, observing the weather and crop,livestock conditions, nuclear reactors monitoring etc. [20].

### 1.4.3 Health Applications

WSN are widely used in hospital to monitor the condition of patients. Small scaled and low radio range sensor nodes are placed over the body of patient to monitor different parameters like blood pressure, sugar level, heartbeat rate etc. The data collected by the sensor is forwarded to a server where the doctor make their decision accordingly [21]. Similarly, the physiological data collected by a sensor network can be stored and used for scientific and medical exploration and experimentation [22] [23]. The medical sensor networks can also monitor and detect the behavior of the patient, e.g., a fall or change in moving pattern, abrupt change in heart beat and blood pressure etc. The application of Wireless Body Area Network enabled the patients and other research subject (human,animal and birds etc.) to move in a large proximity and allow the doctors to identify the symptoms remotely. For example, a project known as Health Smart Home (HSM) [24] which is developed to provide health felicities to the patients who needs special care and wish to remain at home.

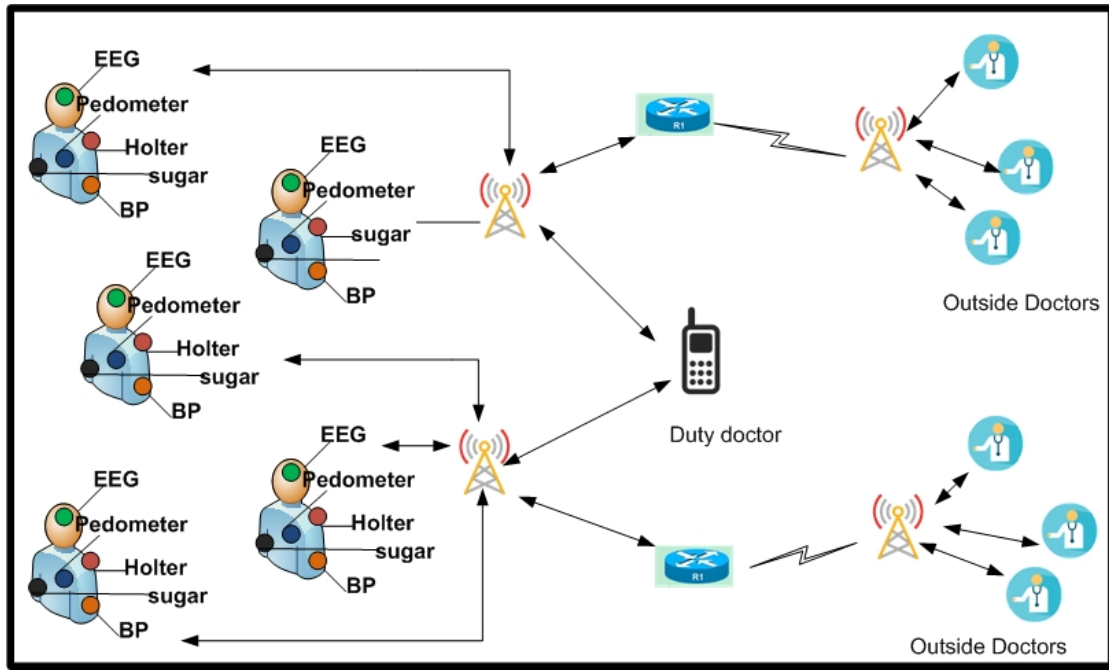


FIGURE 1.6: An example of application of WSN in health care

#### 1.4.4 Home Applications

The sensor technology also become an integral part of our daily life. All the electrical appliances like vacuum cleaner, microwave ovens, deep freezer, television etc are fully equipped with sensors and actuators. This allows the user to manage the home externally with the help of Internet. The blood sensor, motion sensor and heat sensors are also used to detect the entrance of an unauthorized person [25][26].

#### 1.4.5 Industrial Applications

Wireless Sensor Networks have become a source of developing and maintaining the quality products in a cost effective way. Each item in the industry is equipped with the sensor so that exact location and number of items can be observed. This also helps in inventory control and sale/purchase of the products. Similarly, the domestic and commercial vehicles are also now equipped with intelligent sensors to improve the efficiency and provide quality service to the user. Other commercial application of WSN includes material testing, building monitoring, robot

command and control, automatic manufacturing, smart toys, machine diagnostics, smart grids etc. [27][28].

## 1.5 Highlighted Issues in WSN

The wide range applications of WSN pose various design issues. This section is focused on key design issues required to establish a fully-operational, efficient, robust and secure sensor network. Generally, the WSN has a dynamic nature both with respect to topology control and routing of data that takes place in a self-organizing manner once the network is deployed. Keeping in view these properties, we classify the design issues of WSN in Figure 1.7 on the basis of some requirements that ensure the extended network life, availability of the network and integrity of data.

Node deployment has a great impact over the data collection and routing process. It may be a deterministic deployment in which each sensor node is placed physically in the sensing field. For example, the forest monitoring or habitat monitoring requires the sensor nodes to be installed over targeted locations or animals. Similarly, in a hostile field, the deployment may be aerial. Both require different strategies of routing and data gathering. Similarly power consumption of a sensor node is another vital issue that plays an important role in network lifetime. Power consumption refers to all the processes that consume power while performing some activity like processing, communication, memory management etc. Different schemes have been developed in order to prolong the network lifetime. Scalability of a network is the ability to accommodate additional sensor nodes in the network when required in such a way that it does not affect the overall performance of the network. A WSN is always assumed to be scalable up to some extent. The scalability is considered a major factor while designing a routing protocol. This also requires a strict topology control in case of addition or unwanted partition occurrence. Another issue of WSN is the routing of data with the help of some protocols. A routing protocol is designed on the basis of

some metrics like energy efficiency, availability, reliability security etc. Each routing protocol has its own mode of operation. For example in event driven mode, a protocol is only activated when some event or activity is noticed by the node in the field. Similarly, some protocols are designed in periodic fashion in which the node starts sensing the field after a specific interval and sends the information to the sink or CH accordingly. Query based routing is another mode of routing in which the base station initiates a command to nodes or CHs for updating the results. For a reliable sensor network, some protocols incorporate all the above mentioned strategies in order to operate a node in dynamic condition.

Fault tolerance quality of a sensor node shows its ability to remain functional in case of partial failures by attempting for recovery. Quality of service is the combination of metrics required to fulfill the maximum performance of network. These metrics include availability, delay, throughput and reliability of network.

Security is an open and imperative research issue in WSN. The sensitive data carried by sensor network must be protected from various attacks. Two main modules i.e. the authentication of a node in the network and secure data routing are usually focused in the domain of security in WSN. There are many schemes which use encryption /decryption for data security and exchange of control messages. Since the scope of a WSN has been extended to various fields during the past decade, this lead to develop two groups of routing architectures i.e. flat and hierarchical to be deployed in the respective sensing field. In a flat architecture, each node has equal rights and scope in the network; while a hierarchical structure designates nodes to perform special roles in the network i.e. of Cluster Head (CH) to collect and forward data and of a Beacon Node (BN) to guide other nodes respectively.

## 1.6 Security in Wireless Sensor Networks

As discussed earlier, WSN has a variety of applications. We also know that sensors have limited energy resources and processing capabilities. Moreover, they are usually deployed in open and critical areas exposed to various attacks like jamming ,

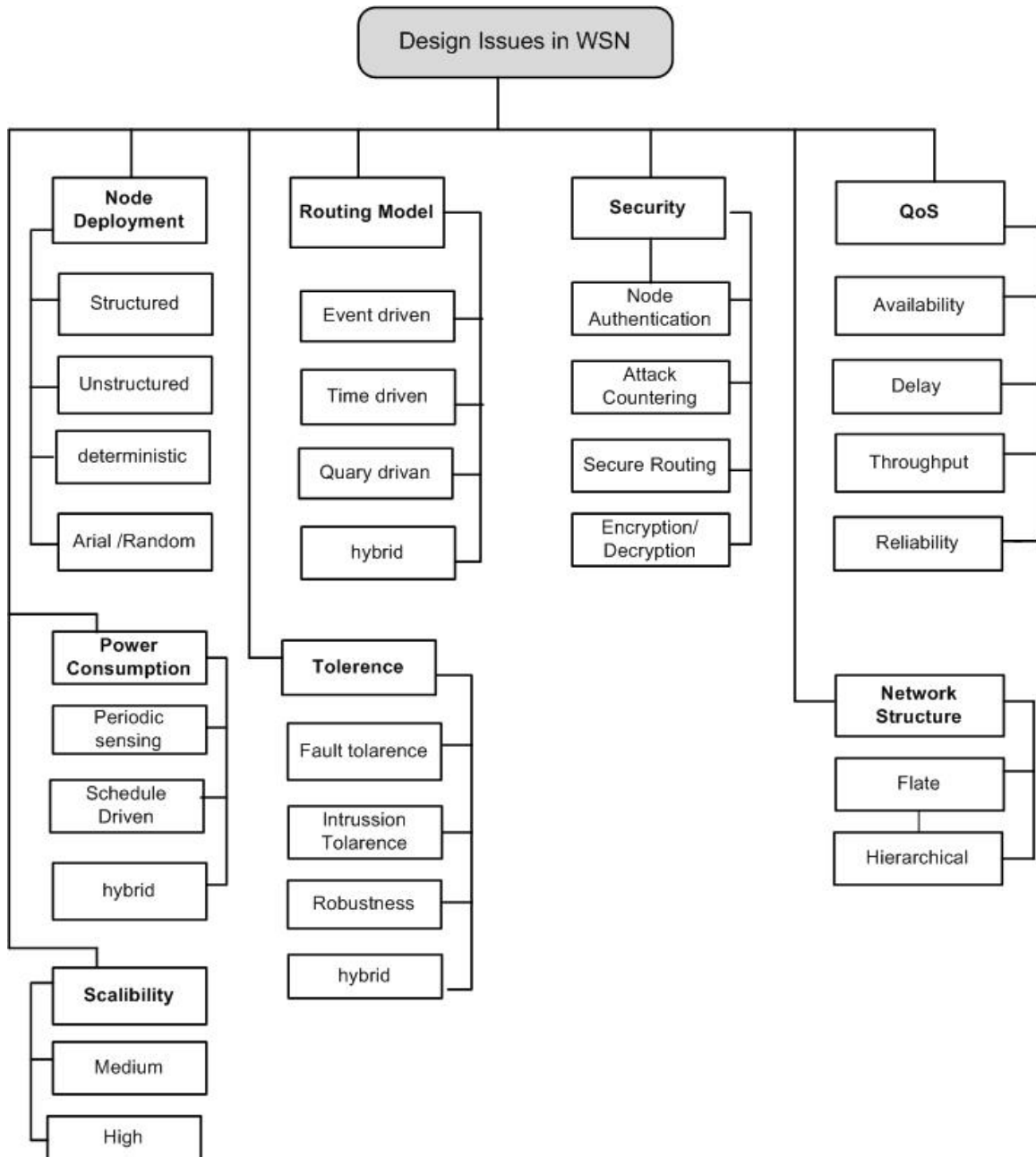


FIGURE 1.7: Design Issues in WSN

node capture, tampering, Sybil etc. [29]. These attacks or threats directly influence the application and services of a Wireless Sensor Network. Figure 1.8 shows some of the attacks designed for WSN. Due to its diverse nature, many traditional security methodologies designed for other data networks become difficult or impossible to implement in WSN [30]. One of the major obstacles in implementing these methodologies is their processing complexities which lead to a rapid drainage of the battery of a sensor node [31]. Also, the complexity and processing power of

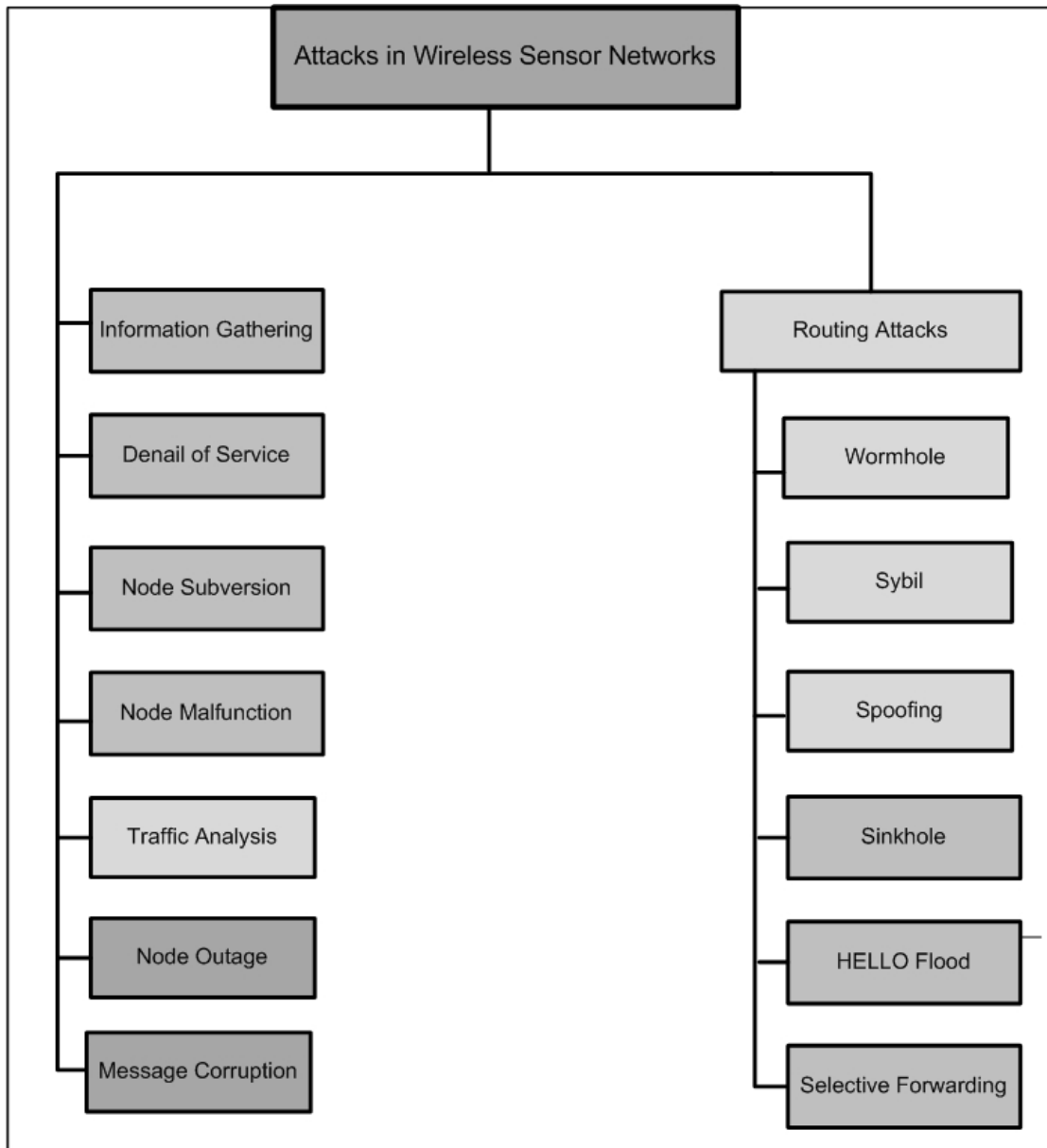


FIGURE 1.8: Some of the attacks in WSN

attacking nodes are evolving day by day. Not only the quantity and complexity of these attacks are increasing, but also their momentum and nature of attacks. Thus the need for effective and efficient security mechanism grows with the development and growth of WSN and its vulnerabilities. The sensitive information routed in a sensor network must be guaranteed with security and safety i.e. its integrity and confidentiality. In nutshell, it is imperative to address the security issues during or at the beginning of system design [32],[33],[34].



## 1.7 Attacks in Wireless Sensor Networks

One of the most challenging aspects in WSN is its vulnerability to various security attacks which affect its performance. Malicious nodes exploit the network security weaknesses and vulnerabilities to get and forge the sensitive information. There is a variety of attacks that can be launched on a wireless sensor network. Some of the most widely launched attacks are discussed below:

### 1.7.1 Physical Layer Attacks

The physical layer in WSN is responsible for selection and generation of the carrier frequency, signal detection and modulation etc. There are two major attacks at the physical layer of WSN, the jamming and tampering attacks. The Jamming attack is used to interfere the radio frequencies used by the node for communication in a network. Jamming sources are deployed to disrupt the communication between the nodes. Similarly, tampering attacks are used to get the cryptographic information (keys), temper the circuitry and set of instructions. Replacing a sensor node with a malicious node also comes under the umbrella of tampering attack [35],[36],[37].

### 1.7.2 Link Layer Attacks

The main responsibility of link layer is framing, multiplexing of data, error and medium access control etc. This layer is prone to attacks like intentional exhaustion of resources and collision, unfair allocation of resources. The attacker may cause collisions repeatedly to discard the data and make the node to content for the medium again and again. This repeated collision and contention also leads the network to resource exhaustion and battery drainage [38].

### 1.7.3 Network Layer Attacks

The network layer is always a hot target for attackers. Most of the attacks are designed for network layer which include:

- Spoofing attack
- Selective forwarding attack
- Sinkhole attack
- Sybil attack
- Wormhole attack
- Black hole and grayhole attack

#### 1.7.3.1 Spoofing Attack

The Spoofing attack is considered as a direct attack against the routing protocol. In a spoofing attack, the routing information is spoofed or altered to degrade the network performance. The main targets of spoofing attack may include routing loops, depriving a node of network traffic, misleading the nodes about routes, creating error messages, fake network partitions etc [39].

#### 1.7.3.2 Selective Forwarding

Ideally all the nodes in a sensor network are assumed to deliver accurate data to the sink. Some of the nodes may have sensitive or real-time information. In selective forwarding attack, the attacker changes the behavior of a sensor node in such a way that it starts sending only selected data to the sink. In other words, the compromised node selectively forward the data and drop the rest.[40].

### 1.7.3.3 Sinkhole Attack

In sinkhole attack, the attacker compromises a node in order to make it attractive to its nodes in the neighbor by creating fake routing information. As a result, the legitimate nodes chose the compromised node as its next hop and forward data to it. The sinkhole attack makes selective forwarding very easy since all the data flows through compromised node [41],[42].

### 1.7.3.4 Sybil Attack

In a Sybil attack, a malicious node in the network claims to be several different nodes with different identities at different locations simultaneously. The Sybil node can easily deceive a legitimate node if it has no physical information of the other nodes [43]. The success of Sybil attack in WSN depends on how cheaply the identities can be generated and issued. Apart from effective deployment in distributed data storage systems, the Sybil attack can also be effectively launched in data aggregation, and voting systems etc. In case of a powerful Sybil attacking node, it can create even an infinite number of fake identities. A Sybil attack can affect the network in different ways depending on the nature of the network. For example, a Sybil node can divert the traffic towards itself to capture the maximum information. Similarly, in a voting based WSN, it can increase its own priority by disseminating its fake identities with a fake location in the network [44] [45].

### 1.7.3.5 Wormhole Attack

In a wormhole attack, the attacking node captures the packets from a node on one location and transmits it to the node located at the distant location via a logical tunnel where the data is then distributed locally. The wormhole attack is very successful in a network where the nodes do not possess any additional information about the network or neighboring nodes[46] [47].

### 1.7.3.6 Blackhole / Grayhole Attack

In this kind of attacks, a malicious node advertises false and shortest path to the destination. This advertisement usually occurs during route updation or path finding process. The gray hole is an advanced and slippery version of black hole attack in which the attacking node or compromised node decides which data to forward and which to discard. Thus the main intention of a black hole or gray hole attack is to intercept or discard the data being sent by a sensor node towards the destination. These attacks can only be detected by analyzing the sent/received information at a sensor node [47] [48].

## 1.8 Research Objectives

The major objectives of this research are two folded. First, we aim to develop a low complexity authentication scheme for the sensor node in order to counter the attacks particularly Sybil attack which is the most widely launched attack in sensor networks. Secondly we intend to develop a secure and energy efficient module for data routing in WSN. In order to implement the secure module, we use GRACE (GRadient Cost Establishment) routing protocol [49] which is an energy efficient protocol but does not provide any security to the network. The energy efficiency of GRACE has been proved both by simulations and mathematical modeling by its authors and the results have also been verified by field measurements.

## 1.9 Research Contributions

In order to achieve the objectives mentioned in section 1.8, the research resulted in the following major contributions:

- A Signed Response (SRes) based Sybil attack detection scheme is developed for sensor networks that provides a better defense against Sybil attacks than

the existing schemes. The scheme is based on authentication mechanism known as Signed Response (SRES) used in the second generation of Global System for Mobiles (GSM).

- Secondly, a secure and energy efficient routing protocol known as SEER: Secure and Energy Efficient Routing in Wireless Sensor Networks is developed which is a hybrid scheme and is based on the Gradient Cost Establishment for route selection proposed for WSNs and voice encryption mechanism used in GSM .
- In order to evaluate the performance of the proposed schemes, extensive simulations are carried out over sensor networks of various densities and traffic scenarios. The obtained results are then compared with the notable existing authentication and secure routing schemes.
- Expressions for the interception probabilities (The probability that an encryption mechanism is being intercepted by an attacker) of both authentication and secure routing schemes are developed and modeled.

## 1.10 Significance and Application of the Proposed Research

The advancements in the research and development of Wireless Sensor Networks have changed its dynamics and scope. Low cost authentication and energy efficient secure routing are still open issue that need to be addressed. The research proposed is aimed to fulfill the current security needs of a wireless sensor network without affecting its lifetime. This research work can be applied to prevent Sybil attacks in various ways in order to assist designing of a safe Wireless Sensor Network both for industry or general use (a targeted sensing field). The proposed secure routing protocol will be applicable in WSNs deployed in hostile environments like fire zones, battlefields, dense forests for habitat monitoring and spying zones etc.

This research work can also be exploited to develop a suite for location-based routing in order to ensure accuracy and integrity of the data. Our proposed scheme can also be applied to MANETS and robot colonies to prevent their respective moving nodes from being deceived in Sybil attacks. Through such attacks, a Sybil node can create a nonexistent congestion to divert the traffic creating troubles for the drivers. Similarly, in a voting based system, a Sybil node can modify data by rigging the polling decisions. By implementing the proposed security mechanism in the areas of conflict, one can ensure the integrity of the voting system by guaranteeing non-rigged results. Moreover, the proposed energy efficient secure routing protocol (SEER) also lead us to the development of a new approach of hardware-based security module using advancements in embedded systems that may avoid high-level language overheads. The high level languages have no way to communicate directly with underlying hardware. Hence, a compiler is needed to generate machine code in order to implement the instruction written in high level language. Compiler generated machine code is always general and the price to pay for its generality is the extra lines added to the code known as translation overhead. Optimizers in compilers may reduce translation overhead but they can never eliminate it. On the other hand, the hardware level implementation can overcome the above mentioned issues. Assembly language is used for hardware implementation. The Assembly language has one to one correspondence with the machine language. Assembler does the translation procedure without imposing any translation overhead This implies that each instruction of assembly code is translated to exactly one machine instruction. Therefore, the same code written in assembly/machine language always results in less number of executable machine instructions as compared to code written in high level languages such as C, C++. This new approach will certainly help to design even more energy efficient algorithms than those are present today.

## 1.11 Thesis Organization

The rest of the thesis is organized as follow:

Chapter 2 presents a detailed overview of the related work in the fields of node authentication and secure routing. The chapter highlights the security issues, presents a gap analysis and formulates problem for the proposed study. Chapter 3 proposes a signed response based node authentication scheme for sensor networks and presents a comparative analysis on the basis of simulation results along with its result comparison with existing schemes. In Chapter 4, a secure energy efficient routing scheme is presented. Chapter 5 concludes the thesis and discusses future directions for the extension of proposed theory.

# Chapter 2

## Related Work

Although security is a common concern for all wired and wireless networks but wireless sensor networks are comparatively more exposed to security threats due to their unattended nature. Since the security mechanisms developed for traditional networks are not applicable in WSN; therefore a rich field of research has emerged in the name of WSN security in last few years. Due to limited resources, a WSN requires less complex and light weight solutions. As discussed in chapter 1, there are many attacks that can be launched on a sensor network. The research community has proposed various counter mechanisms for these attacks in order to keep the network safe ensuring the privacy of data.

A wireless sensor network faces security threats at many levels. An attacker can become part of the wireless sensor network if there are no proper procedures for authentication and authorization. Thus a node must be authenticated before it becomes part of a wireless sensor network. The second most important intention of the attacking nodes is to get routing information in order to steal or forge the data. This issue leads us towards the development of securer routing protocols in order to protect the integrity of routed data in a wireless sensor network by consuming less processing time and energy.

This chapter presents a literature survey on the issues and challenges related to the issues and challenges related to the security of a WSN and its energy efficient



solution. In the start, the impact of Sybil attacks and its counter measures proposed by the research community is highlighted. The chapter also documents the published literature related to energy efficient and secure routing.

## 2.1 Sybil Attacks in Wireless Sensor Networks

The scope of wireless sensor network deployment gets increased day by day due to its low cost, large scaled deployment and self-organizing nature [50–53].

The existing designs of wireless sensor nodes for various applications allow a better flexibility in terms of communication, exchange of data etc. But their inadequate battery life, short communication range and limited processing are some of the main limitations that make them vulnerable to a number of attacks. [52, 54–56]. Through one or more of these attacks, an attacker can have access to the confidential information. [57]. Sybil attack is one of the most widely launched attacks in Wireless Sensor Networks. The Sybil attack is considered very easy to be launched because of the open and broadcast nature of the wireless sensor network. The very first Sybil attack problem was introduced by Douceur in peer to peer networks [58].

Later on the authors in [59] proved that the Sybil attacks may have a significant effect over the routing protocols. In such attacks, the Sybil node creates multiple identities at different locations deceiving the Cluster Heads (CH) or the other nodes of the network and tries to become part of the network.

The current mechanisms to detect Sybil attacks are mainly based upon centralized and decentralized approaches. In centralized approach, a central entity is responsible to determine the attack and point out the attacking node where as in decentralized approach, a distributed approach is used for this purpose. In [60], the authors proposed an attack detection model for Sybil attacks based on RSSI. According to the author, the model does not require any extra resources like third party or antennas and also the mobility of nodes is supported by the model. One

of the implemented solutions is certification of the nodes [61]. This mechanism requires the presence of trusted and authorized third party for the validation of participating entities. The authors in [62] presented a taxonomy which describes how the Sybil nodes are created. The authors also proposed few techniques to counter the Sybil attacks based on radio resource testing, random key distribution, code attestation etc, and position information.

The authors in [63] proposed a solution for Sybil attacks based upon social networks known as Sybil control which is an admission based control designed for distributed WSN. The proposed solution is basically a protocol in which a node calculates the computational work done by the other respective node in order to detect a malicious or misbehaving node present in the network. According to the authors, a malicious or attacking node does not have the capability to calculate the computational work of other nodes properly. Similarly another protocol known as Gatekeeper [64] which is a decentralized admission control protocol is also based on social network approach.

Another RSSI based solution is proposed in [65]. The authors used K-means algorithm for the detection of attacking node. According to the authors the proposed solution can also detect the location of attacking node and enough robust to handle the variable transmission power level of attacking nodes. The RSSI based solutions are considered to be lighter in overhead since only one message is communicated but on the other hand, RSSI being a time varying and unreliable parameter exhibits non-isotropic behavior most of the time. In [66] and [67], a ranging method based approach is proposed for Sybil attack detection. However range-based algorithms involve the distance estimations by using the measurement of various physical properties of signal such as RSSI, time of arrival (TOA) and time difference of arrival (TDOA). In [68], a scheme for the detection of Sybil attack is proposed on the basis of radio resource testing and registration but such approaches use high power and violate the limitation of battery power consumption. In [69] and [70], the authors use Gaussian mixture model to read RSSI readings but the paper does not clearly explain how the Sybil attacks are localized. In [71] the authors proposed a defense mechanism for Sybil attacks based

upon various resource testing like radio resource testing, position verification and registration etc. In [72], a hop by hop authentication procedure is proposed. The authors in [73] proposed a key management mechanism that refreshes all authentication keys in order to prevent them being compromised. The authors in [74] proposed a framework that is performed by cluster heads in hierarchical WSN.

Similarly the authors in [75] proposed a Sybil attack detection scheme for mobile networks. The proposed scheme uses watch dog nodes which monitor the network traffic and its mobility and determine the activities of a sensor node. The authors in [76] proposed a Sybil attack detection scheme based on Fujisaki Okamoto algorithm. Fujisaki and Okamoto developed a technique to secure the networks through Asymmetric and Symmetric schemes. The scheme was introduced in Random Oracle Model, which is widely used in cryptographic scenarios. The authors in [77] proposed an event based reputation system (EBRS) for VANET which is a form of ad-hoc wireless network. The false messages sent by a Sybil vehicle is suppressed with the help of trusted values calculated for each event like car crashes, traffic jams, congestion etc. These trusted values help the EBRS to isolate the fabricated messages and their respective sender from the network .

## 2.2 Energy Efficient Routing in Wireless Sensor Networks

Energy efficiency and security of data always remained an open research issue in WSN. Most of the battery power is consumed by the routing of data from one node to another and therefore the life time of a network mainly depends upon the efficiency of its routing protocol. More the energy efficient routing, the longer will be its network life. The delivery of data to the destination without being captured or forged by the attackers is also a vital issue. There is a variety of protocols designed for routing data securely while being energy efficient. The authors in [78] proposed an energy harvesting based protocol known as Intelligent Solar Energy Harvesting (ISEH). The ISEH helps a node to switch between battery and solar

power source. The protocol also uses solar point tracking system for the maximum utilization of sunlight when available. Here again the energy harvesting mechanisms mounted on a sensor not only increases the cost of the sensor node but also restricts its deployment to dry weather conditions. Moreover, it is also not feasible to deploy a solar tracking mechanism on a low cost sensor node. A hierarchical routing protocol known as Low Energy Adaptive Clustering Hierarchy (LEACH) is proposed in [79] which is considered as one of the initial hierarchical routing protocols in WSNs. LEACH uses distributed clustering mechanism in which nodes are selected randomly as a cluster head for a balanced energy consumption and prolonged network life. The energy level of each node is calculated and compared with threshold level at the time of CH selection. A node can only become a cluster head if its energy level is equal or greater than the threshold level. The LEACH become less efficient when the distance between CH and the base station increases. Another variant of LEACH is TL-LEACH [80] where TL stands for Two Level. The TL-LEACH works on a two level of CH, a primary and secondary CH. The authors proved that TL-LEACH can provide better throughput without affecting the network life as compared to LEACH. Similarly another hierarchical routing protocol known as Threshold sensitive Energy Efficient sensor Network protocol (TEEN) is proposed in [81]. TEEN is a reactive protocol that accepts data from a sensor node based on some threshold values. A hard threshold value means that the data is closely relevant to set of predefined attribute and a soft threshold means that the data differs from the attribute set. A node may never send the data if the sensed data does not reach the hard threshold. Also, the protocol may not work efficiently where the regular transmission of data is required. Another energy efficient protocol known as Power-Efficient Gathering in Sensor Information System (PEGASIS) is proposed in [82]. The PEGASIS uses hop-by-hop communication to deliver data from a node to the base station. The proposed protocol also consumes lesser bandwidth since only local communication is allowed between the nodes. Moreover, PEGASIS does not require any CH selection and efficiently works in flat wireless sensor networks. Energy-efficient, Delay-aware, and Lifetime-balancing Data Collection Protocol for Heterogeneous Wireless Sensor Networks

(EDAL) is another routing protocol proposed in [83] which is stemmed from open vehicle routing problem of operations research method. The protocol can work both in centralized and distributed network. According to the authors, the EDAL can also utilize compressive sensing, an emerging technique which can reduce the traffic and its cost while collecting and transmitting in loose delay bounds.

Moreover, the authors in [84] proposed an energy efficient routing protocol. The technique is focused on the minimal use of power but requires the location information of each node through GPS or other location techniques. In [85], the authors proposed a scalable cost aware routing in WSNs. Cost awareness refers to longer network life by choosing the optimum route having maximum residual energy. Similarly, another approach based upon minimum cost packet delivery is proposed in [85]. The proposed technique calculates the minimum cost path from a source to the sink. However, this approach may be suitable for static WSN but not for mobile WSN as the random movement of mobile nodes can create considerable changes in network topology. A new approach of routing based on renewable energy is proposed in [86] known as Energy Harvesting Aware Routing Protocols. This technique proposes a mechanism to harvest the energy from external resources such as energy from wind, solar, motion, noise etc. However this technique requires additional resources to be mounted over the node. Moreover, another energy harvesting protocol is the Distributed Energy Harvesting Aware Routing Algorithm (DEHAR) [87] which operates on a metric named as energy distance for selecting the optimum route. This metric calculates the route with minimum total energy distance instead of spatial distance. But this shortest energy distance is calculated by methods such as directed diffusion or flooding which incurs routing overhead.

The authors in [88] designed a routing protocol with energy management functionalities known as Opportunistic Routing algorithm with Adaptive Harvesting-aware Duty Cycling (OR-AHaD). OR-AHaD is an opportunistic and adaptive protocol which can dynamically tune the duty cycle of a sensor node based upon the remaining power in order to prolong its life in the network. The protocol however requires a regular update of energy levels and geographic information of a node.

Moreover, the frequency of power updates increases with the passage of time as the power level of nodes decreases.

## 2.3 Secure Routing in Wireless Sensor Networks

Although there are many commonalities of WSNs with both of the wired and ad hoc network, they also exhibit a number of distinctive properties which make them different from the latter two networks. These unique properties include special low-cost physical design of a node, ability to work in the hostile environment and hop-by-hop communication etc. Secure routing in WSN is another most challenging and hot topic which attracted the research community in last few years. As we know that WSNs have diverse and distinguished characteristics from the traditional networks; therefore, the secure routing protocol designed for these traditional networks does not comply with that used WSN. There are many secure routing protocols designed for WSN explicitly.

A secure routing protocol known as SAODV which is the extension of AODV is proposed in [89]. The mechanism used in SAODV known as double signature used for authenticity but increases the processing overhead since signature on every chunk of data is an expensive process. To solve this limitation of SAODV, the authors in [90] proposed another protocol known as A-SAODV. In A-SAODV, the nodes use request/reply mechanism like wireless networks. Reply to the request will be sent by node only if it is not overloaded. Also, the replying node can determine whether to use single signature or double signature based upon processing overhead. This mechanism is good in theory but again not suitable for resource constrained WSNs. Similarly, the authors in [91] proposed an encryption and authentication based protocol. The proposed scheme named as Efficient and Secure Routing Protocol Based on Encryption and Authentication for Wireless Sensor Networks (BEARP) which claims routing information confidentiality, authentication and integrity of data. As discussed earlier the network life and

processing overhead, convergence time, network traffic etc. are the challenges that arose while designing a secure routing protocol. The BEARP exchanges too many control messages like confidential data enquiry (CDE), Routing Path Selection System (RPSS), Confidential Enquiry Reply (CDER), Confidential Route Reply (CRR), Acknowledgement. Even though all the communication between Base Station (BS) and sensor nodes remains encrypted, still the BS add a random number RB and a time stamp TB as an additional secure layer which obviously adds the processing overhead to the nodes. The BEARP does not explain what is the probability of success and failure of the proposed scheme. Moreover, the paper lacks about the explanation what is the convergence/setup time of the proposed scheme. Similarly, the authors in [92] represents a secure ant colonization based routing protocol. According to the paper the proposed methodology has the capability to cop with multilayer security threats however, the term multilayer has not been explained clearly. The proposed methodology in the paper uses Ant Clony Optimization and claims to achieve the security by four features like route discovery, route selection, route security and data forwarding. The route is discovered by launching a broadcast request that reaches to destination and the destination responds with acknowledgment through back ward broadcast. The path through which the packet arrives earlier is elected as shortest path. The watch dog algorithm is used to decide whether a packet needs to be secured before sending or not, if yes, the RC4 algorithm used to encrypt the data. The paper does not explain how the RC4 algorithm is embedded with the proposed scenario also the probability of success or failure of secure model is also not highlighted.

The WSN faces the same security challenges as any ah-hoc network would [93] [94]. There are other routing protocols that attempts to secure the network like TinySec [95], Spins [96], TinyPK [97], TinyECC [98], [99] LS-LEACH [100] The most popular technique in security domain of routing is the encryption and decryption of data. This technique is used to prevent or detect the unauthorized parties or malicious behavior of a sensor node. However, these solutions mostly run over application level resulting in a complex code implementation in higher level language which adds processing over heads for the processor of a node. This phenomenon

eventually fails the claim of secure and energy efficient routing protocol.

## **2.4 Provision of complexity reduction and energy efficiency in authentication and secure routing**

Usually, authentication and secure routing are complex mechanisms involving a number of searching, matching and executing procedures that exert high computation burden on a computationally constrained node and cause major battery drainage. It is thus very important that the procedures used for authentication and secure routing must be light weight in terms of processing and size of the algorithm. Similarly, secure data routing is another challenge in WSN which is considerably investigated by the researchers [101–104]. There are many secure routing protocols designed for wired and wireless networks but they are not feasible for a sensor node due to their high space and time complexities [105]. Thus a low complexity and energy efficient routing is a major challenge a WSN has to cope with. Until now, a significant research has been carried out to design energy efficient and secure routing protocols but still, there is no single viable solution acceptable for all scenarios of WSN. It is worth mentioning here that the attacking strategies are evolving along with efficient processing techniques of sensor nodes. Keeping in view the momentum of WSN demand in data sensitive environments and other commercial products, a time will come when a single layer security shield would become insufficient to counter the attacks. An attacking node will easily forge or steal the data even in the presence of an efficient single layer security algorithm. Due to the ever increasing processing power of sensor node, the probability of breaking a single security shield will become higher day by day.



## 2.5 Problem Statement

As discussed earlier in literature survey, there are varieties of attacks that intend to compromise a Wireless Sensor Network. Each of the attacks has a specific objective like altering the information, choking the network, minimizing the network life, creating partitions etc. Sybil attack is one of the most widely launched attacks in WSN. A Sybil node creates multiple identities in the network to deceive the corresponding nodes.

The Sybil node once becomes part of the network can get all the routing information and forward the data to its own base station. Moreover, a secure and energy efficient routing protocol is still an open issue in WSN. Energy efficient routing protocols mostly proposed in the literature do not consider the security of their data and focus only on data routing.

Similarly, on the other hand, most of the security algorithms proposed so far are either based on symmetric key cryptography or provide solutions only for the attacks. Thus a node has to run more than one protocol if security and energy efficient routing are required. As the attack mechanism and processing capabilities of attacking nodes are strengthening day by day and it seems that only one-tier security protocols (either only Secure or Energy Efficient Routing protocols) may not be enough to prevent a network from being attacked while consuming lesser energy. Even most of the secure routing protocols do not embed authentication procedures along with data encryption techniques.

Moreover, there is no viable single protocol in WSNs that can cater to the needs of the security of the network while processing security procedure and routing data in an energy efficient manner. The goal of this research work is thus to design a secure and energy-efficient routing protocol for WSN in order to improve the network life and data integrity. For this purpose, the aim is to use the Signed Response (SRES) security mechanism and A5 based voice encryption implemented in 2nd generation Global System for Mobile Communication (GSM). Based on public key cryptography, the SRES is responsible for authenticating a mobile node whereas

the A5 encrypts the voice data of two parties during dwell time. We develop a 2-tier security mechanism consisting of node authentication and secure data routing without exhausting the network life and throughput. The proposed protocol is evaluated and compared with current state-of-the-art solutions both in terms of energy efficient routing and security.

In order to extend the simplicity in our research, the Sybil attack is targeted in the security module of the proposed protocol. A developed model for the proposed solution will be implemented in *MATLAB*<sup>®</sup> since it provides more liberty in the simulation environment at physical layer as compared to other simulators.

## 2.6 Chapter Summary

Chapter two is focused on the work done in order to improve the authentication and data security processes in wireless sensor networks. A Sybil attack which is the most widely launched attack in WSN is discussed in terms of solution proposed by research community through different techniques. Energy efficiency in data routing is one of the key research issue which plays a vital role in the network lifetime of a WSN. Various protocols have been designed for energy efficient data routing but this is not enough. The data transmitted in a WSN is prone to various attacks and a one-tier secure module is becoming incapable to counter these attacks. Thus there is a need of various modules that ensure maximum security with minimum complexity and energy consumption. The goal of this research work is to design and develop a node authentication and secure data routing mechanism in order to improve the network life and data integrity. The Signed Response (SRES) and voice encryption of GSM is used to achieve the desired results.

# Chapter 3

## Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks

### 3.1 Introduction

Security is always a major concern in Wireless Sensor Networks (WSNs). Identity based attacks such as Spoofing and Sybil not only compromise the network but also slow down its performance. In this chapter, a Sybil attack detection scheme is proposed that is based on Signed Response(SRes) authentication mechanism developed for Global System for Mobile (GSM) communications. A probabilistic model is presented which analyses the proposed authentication mechanism for its probability of Sybil attack. The chapter also presents a simulation based comparative analysis of the existing Sybil attack schemes with respect to the proposed scheme. It is observed that the proposed Sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same Sybil detection performance.

As discussed earlier in Chapter 1 and 2, almost every existing protocol proposed for the detection of location based attacks (like Sybil attack) in sensor networks

focused only, on security and prevention from attacks neglecting the effect of its computational complexity on the resource-constrained and bottleneck parameters like power consumption, processing capability, traffic intensity and message latency. These parameters may lead the network towards poor performance if not handled properly. In this chapter, an algorithm is proposed to prevent the sensor network from location based attacks like spoofing attack and Sybil etc. The scope of this work is intentionally made limited to Sybil attack in order to extend simplicity for the reader. The proposed authentication scheme is inherited from the SRes (Signed-RESponse) authentication mechanism used in second generation cellular mobile communication system, the Global System for Mobile communication (GSM) [106]. The SRes mechanism is responsible for authenticating the user and encrypting the voice data. In order to implement the SRes in WSNs, we modified the original scheme to fit it into ad-hoc scenario. Simulations are performed to validate the performance of the proposed algorithm in *MATLAB*<sup>®</sup>. From the simulation results, we prove that the proposed scheme is not only efficient to detect the Sybil attack, but also requires lesser processing and battery power as compared to notable existing authentication schemes. Moreover the scheme creates little message overhead resulting in negligible increase in the traffic of the network. In order to prove the efficiency, comparison of the proposed algorithm is carried out with two notable attack detection and authentication schemes i.e. Detecting and Localizing Location Based Attack Detection in Wireless Sensor Networks (LBAD) [65] and Light Weight Sybil Attack Detection in MANETs (LwSAD) [60]. Both the schemes are evaluated over probability, processing overhead and power consumption.

## **3.2 Working of authentication algorithm in GSM**

The signed response procedure is originally designed for second generation GSM based networks. This mechanism is responsible for hand set authentication to the network. The A3 algorithm is used to produce a Signed Response against the challenge (SRes) as elaborated in Fig 3.1 . The Subscriber Identity Module (SIM)

also contains the ciphering key generating algorithm (A8). The A8 algorithm is used to calculate the 64-bit ciphering key ( $K_c$ ) which is used to encrypt the voice data before it is sent over the channel. The ciphering algorithm A5 is used to authenticate and ensure the secure communication between the Mobile Station (MS) and the network. The GSM network initiates a request and sends to mobile station over the channel. The A3 algorithm which is embedded in the handset is responsible to generate the signed response (SRes). The block diagram of A3 algorithm is shown in Fig 3.2 which involves the process of creating a 32 bit signed response from 128 bit key (RAND). The detailed step by step procedure of mobile

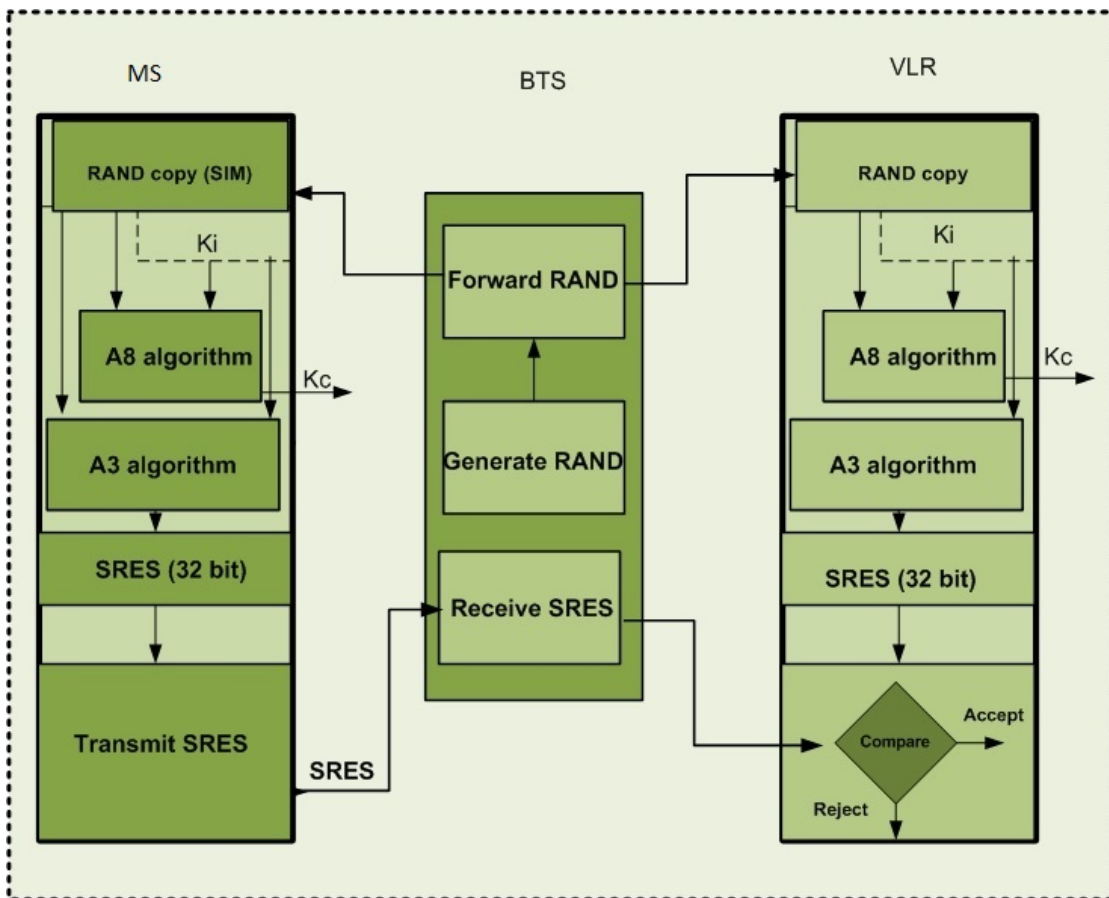


FIGURE 3.1: Authentication Process in GSM

authentication and voice encryption in GSM is given below

1. The Mobile Station (MS) initiates process to sign in to the network.
2. A request for 5 triples to Mobile Services Switching Center (MSC) is forwarded from the Home Location Register (HLR).

3. The triples are created by Home Location Register and sent to MSC comprising of following main components:
  - 128-bit random challenge (RAND)
  - 32-bit matching SRes
  - 64-bit ciphering key used as a Session Key ( $K_c$ )
4. From the first triple, a random challenge is sent to Base Transceiver Station (BTS) from The Mobile Services Switching Center. The BTS then forwards the challenge to Mobile Station.
5. After receiving the challenge from BTS, the mobile station starts the process of encryption with with authentication key  $K_i$  assigned to it. The encryption process is carried out with the help of A3 algorithm.
6. Mobile Station creates a SRes and sends to the BTS.
7. The Base Transceiver Station forwards the SRes to the Mobile Services Switching Center.
8. The SRes is verified by Mobile Services Switching Center.

The use of A8 algorithm for session creation by a mobile station is not discussed in this section since it does not come in our scope.

### **3.3 The Proposed Signed Response Based Sybil Attack Detection Mechanism**

#### **3.3.1 Network model and assumptions**

Fig 3.3 illustrates a distributed network with hierarchical structure having Cluster Heads (CHs) along with the member sensor nodes. We assume that the CH be a powerful node that may become a sink in case of a centralized network. The Sybil

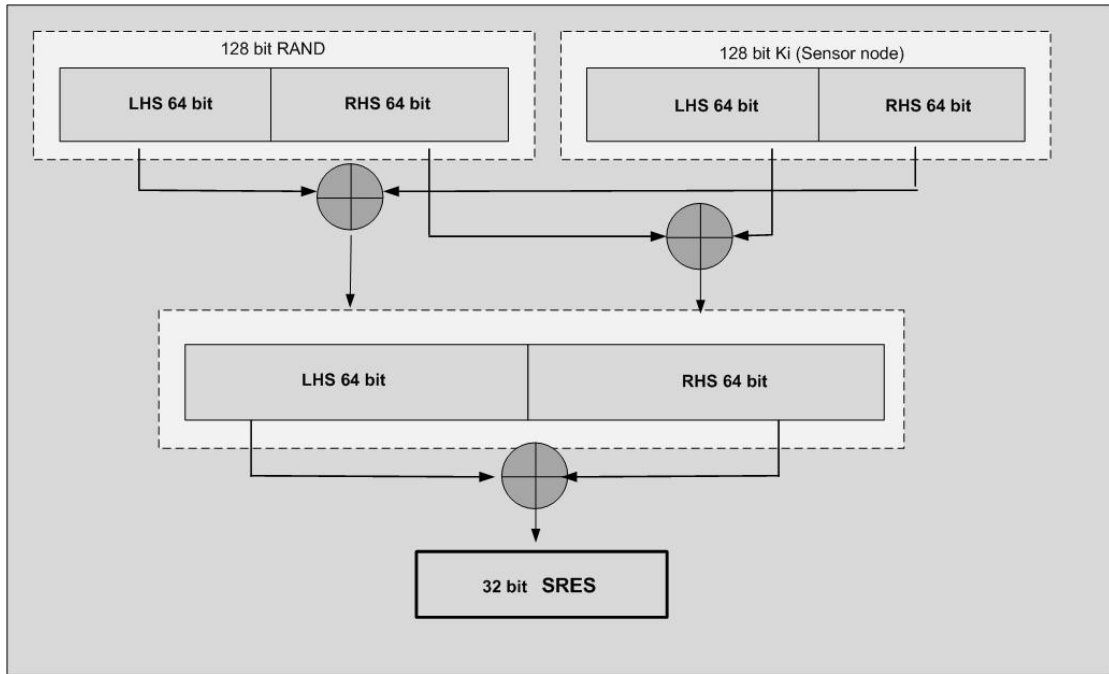


FIGURE 3.2: Block Diagram of A3 Algorithm Generating 32 bit SRes

Nodes S are assumed to be present in the network and they have the complete information of security mechanism of the network. The CH is responsible to monitor the behavior of sensor nodes in its vicinity and ensure that there is no attacker or Sybil Node. The CH sends the attack information to the BS or any controlling entity if determined. Although only one BS is shown in Fig 3.3 but there could be as many BS as required by the network and environment. The deployment of nodes can be arial or manual depending upon the nature of physical environment. Each sensor node is assigned an ID and the position of the sensor node is assumed to be known to it. We also assume that the sink or cluster head has all the necessary information about member sensor nodes like sensor ID, sensor MAC address and the assigned authentication key  $K_i$ .

### 3.3.2 Proposed Methodology

In order to implement the SRes Mechanism in WSN, we make necessary modifications in the existing authentication scheme and implemented in GSM. The proposed mechanism can also be used both in centralized and clustered ad-hoc environment. In ad-hoc mode a sink is responsible to coordinate with all the nodes

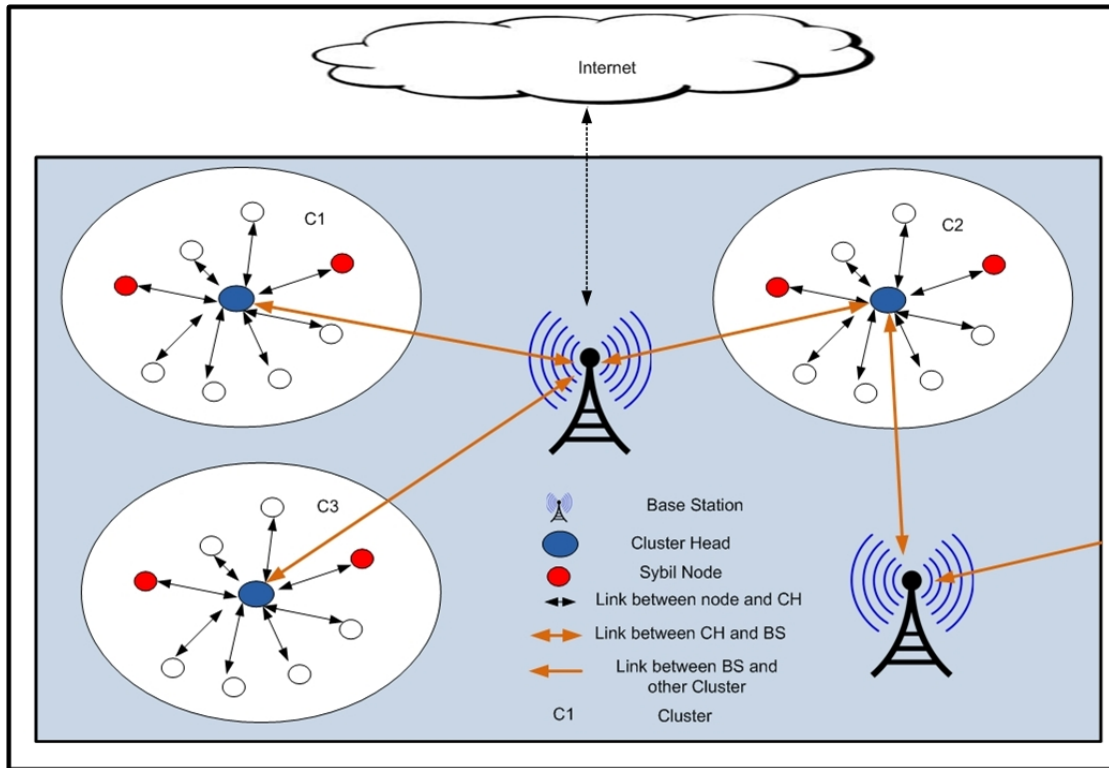


FIGURE 3.3: An Overview of Sensor Network with Sybil Nodes

in the network where as in clustered mode, a cluster head can authenticate the node. The step by step procedure of the proposed algorithm is given below:

1. The triples are generated and provided by the server or Cluster Head (CH) or sink side. The triples are comprise of the following:
  - 128-bit random challenge (RAND)
  - 32-bit matching SRes
  - 64-bit ciphering key used as a Session Key ( $K_c$ )
2. RAND is forwarded to the sensor nodes as a challenge in order to authenticate it.
3. This challenge can be sent either as a broadcast if all the nodes need to be authenticated through single challenge number or as a unicast if a specific node is meant to be authenticated.



4. Every node has a MAC address and is also provided a pre-shared key  $K_i$ . Thus, a node can produce the SRes either with MAC address or  $K_i$  depending upon the implementation.
5. The signed response SRes can be sent by the node either directly to a server, CH or SN depending upon the nature of the wireless sensor network.
6. The Server, CH or sink verifies the SRes sent by the node and acts accordingly (allow or disallow the node)

Fig 3.4 shows the block diagram of proposed authentication scheme where a sink generate and forward a challenge to the node(s). The MAC address of each node that can be considered as  $K_i$  is required to be registered with the sink or CH. The GSM does not allow a mobile station to authenticate the network. However in our proposed scheme, we will use the SRes to authenticate the network by each member node of the network. In order to verify the network, a node N can request the sink or cluster head to resend its already sent SRes to it for confirmation. It means, a node can verify that it is communicating with the right and authentic network or not. However this verification can be carried out after certain number of SRes have already been generated by the node N. As an extension of this work in future, we will enable the node to reverse the authentication process without sending any challenge to the network.

### **3.3.3 Attack model and defense strategy**

In order to launch the attacks and test the efficiency of the proposed scheme, we establish a network of 1000 sensor nodes deployed randomly in an arbitrary area. It is assumed that each node is able to communicate with at least one neighboring node in the network. Since the proposed scheme can work both in centralized and hierarchical networks, we take both structures on board in our simulations while launching attack and executing defense mechanism. The Sybil Node present in the network is assumed to be a powerful node with respect to both processing and battery power. A Sybil Node cannot be registered to the network until it

successfully verifies itself as a member sensor node of the network either to the server, CH or SN. To become a member of the network the Sybil Node launches repeated attacks in two ways; it either generates and sends the fake IDs to the respective SN or CH or attempts for stealing the ID of a valid member sensor node from the network. If the Sybil Node with a fake  $ID'$  gets success to participate in the network without being identified, we will call it a valid Sybil identity. In order to make the situation harder for a Sybil Node, we will perform validation test. There are two types of validations, Direct Validation and Indirect Validation. In direct validation, a node can directly check whether the node in its neighborhood or vicinity is having a valid identity or not based upon the knowledge it possesses. In indirect validation, different nodes can communicate during validating a targeted node so that a globally consistent decision can be made. The indirect validation mechanism is considered to be costly as compared to direct validation because in the latter case, if a node  $A$  having an identity  $ID_i$  tries to validate an identity  $ID_j$  of a node  $B$ , the messages need to be exchanged only between nodes  $A$  and  $B$  via a single hop; whereas in the former case, other nodes of the network have to be taken on board for an identity validation. In order to prove the efficiency of the proposed authentication protocol, we evaluate it on both direct and indirect validation processes. To verify a node and its identity in the network through direct validation, the verifier (CH or SN) challenges the identity by sending challenge to the targeted node laying in its one-hop neighborhood. The challenge in our case is a 128 bit random number generated by authenticating party i.e. the server or CH or SN. Upon the reception of challenge number, the targeted node will encrypt it with either its MAC address or  $K_i$  with the help of A3 algorithm to generate the SRes. At the same time the authenticating party also calculates the SRes from the random number sent and the same  $K_i$  from the database as with the targeted node. When the authenticating party receives the SRes from the targeted node, both the values of SRes are compared. These values must be the same if the node is a valid one otherwise it will be declared as Sybil Node. In case of indirect validation, the authenticating node  $N$  sends a challenge to a targeted node  $T$  which is not in its one-hop neighborhood  $N$ . Thus, this challenge has to reach the targeted node

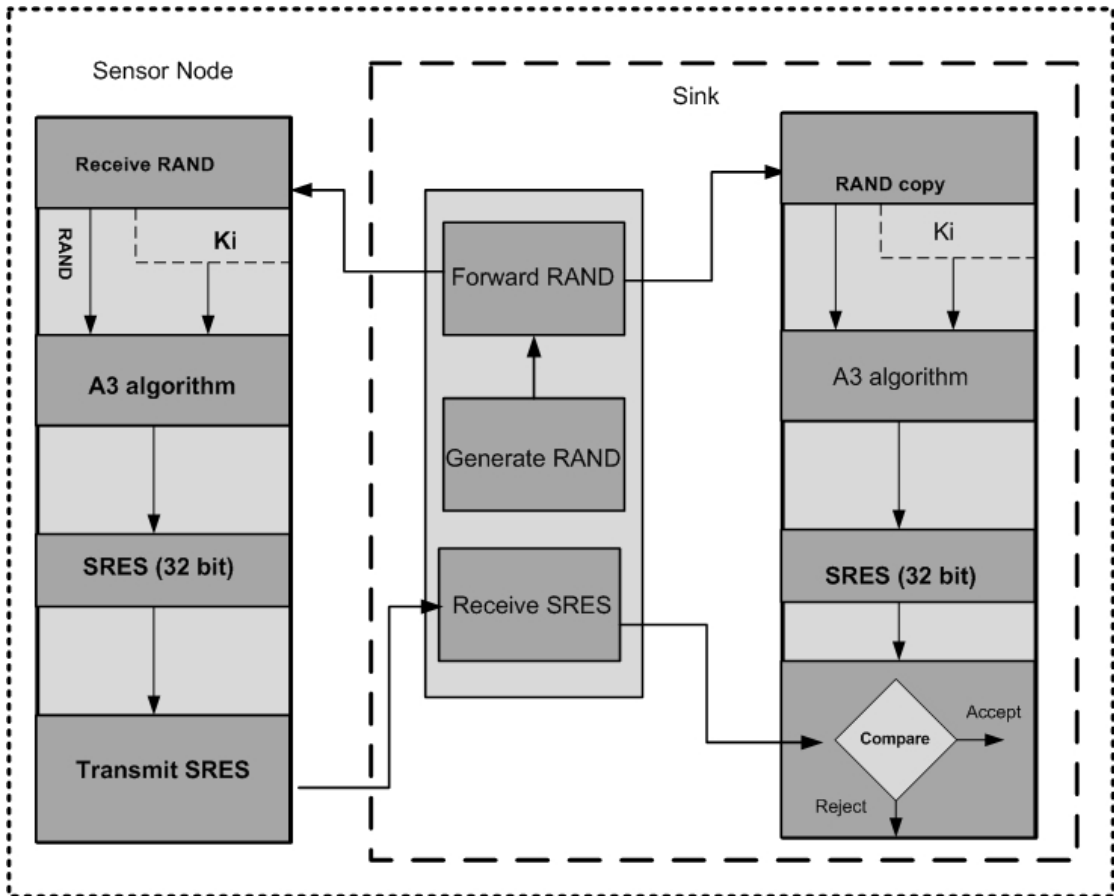


FIGURE 3.4: Block Diagram of Proposed Authentication Scheme for Wireless Sensor Networks

in a hop-by-hop manner. Upon the reception of the challenge, the node T will calculate the SRes through A3 algorithm and sends back to node N. The process of calculating the SRes is the same as discussed for direct validation.

The steps involved in proposed authentication scheme is represented in algorithm 1. The Line 1 generates five vectors of sizes 32,64,128,256 and 512. Note that each value of table  $T_i$  ranges from 0 to  $2^{4+j-1}$ , where  $j = 1, 2, \dots, 5$ . In line 4 the Sybil node generates and forward the SRes to the authenticating party through  $\Psi_a(T, R_k, \Psi_{r,16}(0 \text{ to } 2^8 - 1))$  where as the authenticating party validate the SRes received from attacking node through  $\Psi_a(T, R_k, K_{i,j}, \text{where } j = 1 \text{ to } Pool \text{ Size})$  Similarly the lines 10-23 shows the step by step process of  $X \oplus R$  by dividing the RAND and  $K_i$  in to LHS and RHS to produce the 32 bit SRes.

---

**Algorithm 1** Algorithm of Proposed Authentication Scheme

---

```

1:  $T_{i,1:2^{4+i}} \leftarrow \Psi_r(0 \text{ to } 2^{(4+i-1)} - 1), i \in \{1, 2, 3, 4, 5\}$ 
2: {Sybel attack}
3: for 1 to number of attacks do
4:   if  $\Psi_a(T, R_k, \Psi_{r,16}(0 \text{ TO } 2^8 - 1)) = \Psi_a(T, R_k, K_{i,j}),$  where  $j = 1$  to Pool
      Size) then
5:     useble Sybil
6:   else
7:     sybel detected
8:   end if
9: end for
10: SRes =  $\Psi_a(T, R_k, K_i)$ 
11: for  $i \leftarrow 1 \text{ TO } 8$  do
12:    $X_{1:16} \leftarrow K_i$ 
13:   for  $j \leftarrow 1 \text{ TO } 5$  do
14:     for  $l \leftarrow 1 \text{ TO } 25 - j$  do
15:        $m \leftarrow l$ 
16:        $n \leftarrow m + 25 - j$ 
17:        $y \leftarrow ((X_m + 2 * X_n) \bmod 29 - j) + 1$ 
18:        $z \leftarrow ((2 * X_m + X_n) \bmod 29 - j) + 1$ 
19:        $X_m \leftarrow T_{j,y}$ 
20:        $X_n \leftarrow T_{j,z}$ 
21:     end for
22:   end for
23: end for
24: Convert  $X$  to corresponding binary key  $B$ 
25: Permute  $B$ 
26:  $SRes \leftarrow B_{1:32}$ 

```

---

### 3.4 Probabilistic Model of the Proposed Scheme

let the key size be  $\alpha$ , and the pool size in the sink be  $\beta$ .

$K_i$  where  $(1 \leq i \leq n)$  is the pre-distributed  $i$ th key from a vector space  $K = K_1, K_2, K_3 \dots K_n$  of size  $n = 2^\alpha$ . If the Sybil node generates a random key  $K_a$ , than the probability of this key being a valid key is

$$P(K_a) = P(K_i) = \frac{1}{|K|}$$

where  $|K|$  is the cardinality of the vector space  $K$ . Since  $|K| = n$  therefore

$$P(K_i) = \frac{1}{2^\alpha}$$

This gives us the probability of a randomly generated key to be accepted by the sink. let us suppose that a node uses a pool size of  $\beta$  of pre-distributed keys, then  $S$  be the subspace of pre-distributed keys in the pool such that  $S \subseteq K$  where  $S = \{S_i \in K \mid 1 \leq i \leq \beta\}$ . Now the probability of any key  $S_i$  being in the subspace  $S$ ,  $P(S_i)$  becomes

$$P(S_i) = \beta P(K_i)$$

Probability that a key  $S_a$  is being attacked by the Sybil node from the pool of  $\beta$  keys is:

$$\text{Prob}(S_a) = P(S_i) = P$$

Suppose we have  $M$  number of Sybil nodes attacking on a network. The probability that  $j$  attacking Sybil nodes are successful out of  $M$  nodes is given as:

$$\text{Prob}(j \text{ Sybil nodes are successful out of } M \text{ nodes})$$

$$\begin{aligned} &= \binom{M}{j} P^j (1 - P)^{M-j} \\ &= \binom{M}{j} [\beta P(k_i)]^j [1 - \beta P(k_i)]^{M-j} \\ &= \binom{M}{j} \beta^j \frac{1}{2^{\alpha j}} \left[1 - \frac{\beta}{2^\alpha}\right]^{M-j} \\ &= \binom{M}{j} \frac{\beta^j}{2^{\alpha j}} \left[\frac{2^\alpha - \beta}{2^\alpha (m-j)}\right]^{(M-j)} \\ &= \binom{M}{j} \frac{\beta^j (2^\alpha - \beta)^{M-j}}{2^{\alpha j} \cdot 2^{\alpha M} \cdot 2^{-\alpha j}} \\ &= \binom{M}{j} \frac{\beta^j (2^\alpha - \beta)^{M-j}}{2^{\alpha M}} \end{aligned}$$

Therefore probability of total successful Sybil attacks if M nodes attack the network is given as:

$$P_{max} = \sum_{j=1}^M \binom{M}{j} \frac{\beta^j}{2^{\alpha M}} (2^\alpha - \beta)^{M-j}$$

Fig 3.5 shows the probability that at least one Sybil node is successful out of M attacking Sybil nodes in the proposed Sybil prevention scheme. Moreover Fig 3.6 shows the maximum probability when one or more attacking Sybil nodes become successful under different sizes of authentication key. This figure shows a sharp exponentially declining trend in the probability as the number of useful Sybil nodes increases.

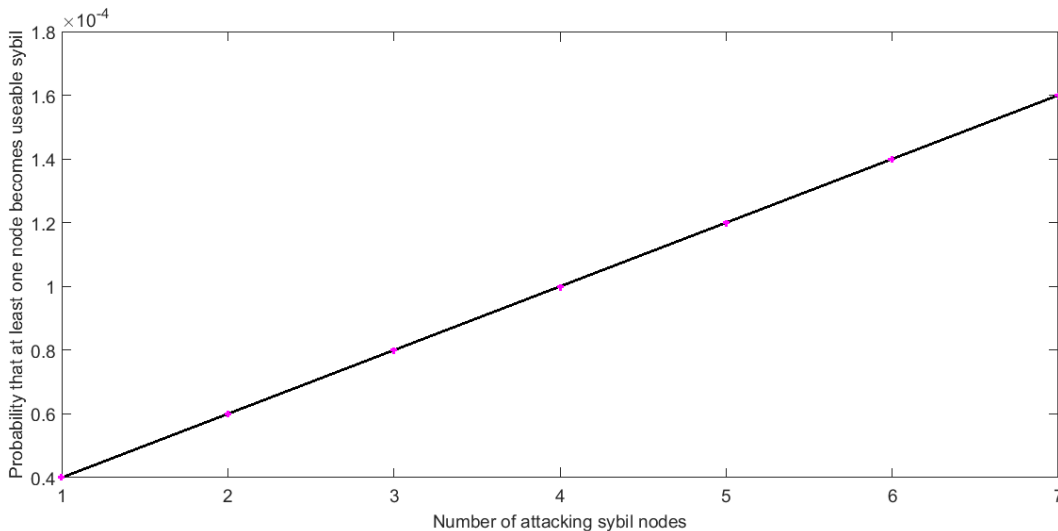


FIGURE 3.5: Successful Probability of at least one Sybil node in a pool of M Sybil nodes

### 3.5 Results and discussion

In this section, we discuss the simulation results and provide a detailed performance analysis of the proposed scheme. As discussed earlier, the simulations are based on a network of 1000 sensor nodes. The parameters that we consider for performance are probability of usable Sybil, traffic behavior, power consumption and probability of attack detection.

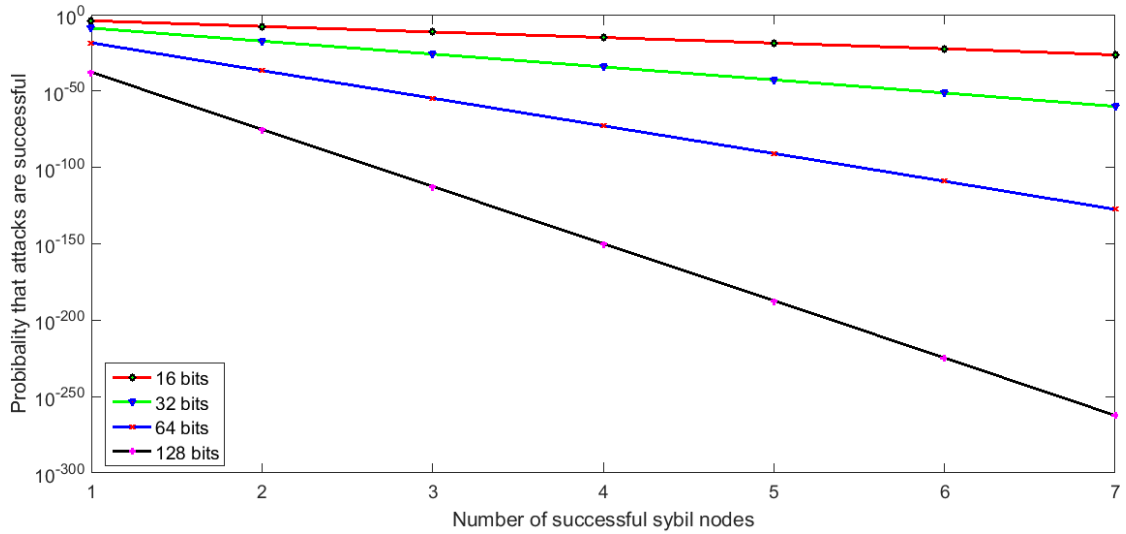


FIGURE 3.6: Probability of Successful attacks by Sybil nodes

### 3.5.1 Probability of usable sybil

The capability of a security algorithm can be better judged on the basis of its probability of letting Sybil nodes successfully utilize the network. Fig 3.7 shows the probability of successful Sybil attacks as exhibited by the proposed and referenced mechanisms. If a Sybil Node is successfully injected to the network without being detected, we call it usable attack. The attacks are launched and tested with the pool sizes of  $N_{K_c}=1$  and  $N_{K_c}=2$ . The case of  $N_{K_c}=2$  is even more harder for Sybil Node to get through as compared to  $N_{K_c}=1$ . However the earlier case requires relatively more processing overhead than the latter one. The result shows that the proposed scheme provides a batter protection since the probability of usable Sybil Node is lower in both cases ( $N_{K_c}=1$  and  $N_{K_c}=2$ ) than the LBAD and LwSAD.

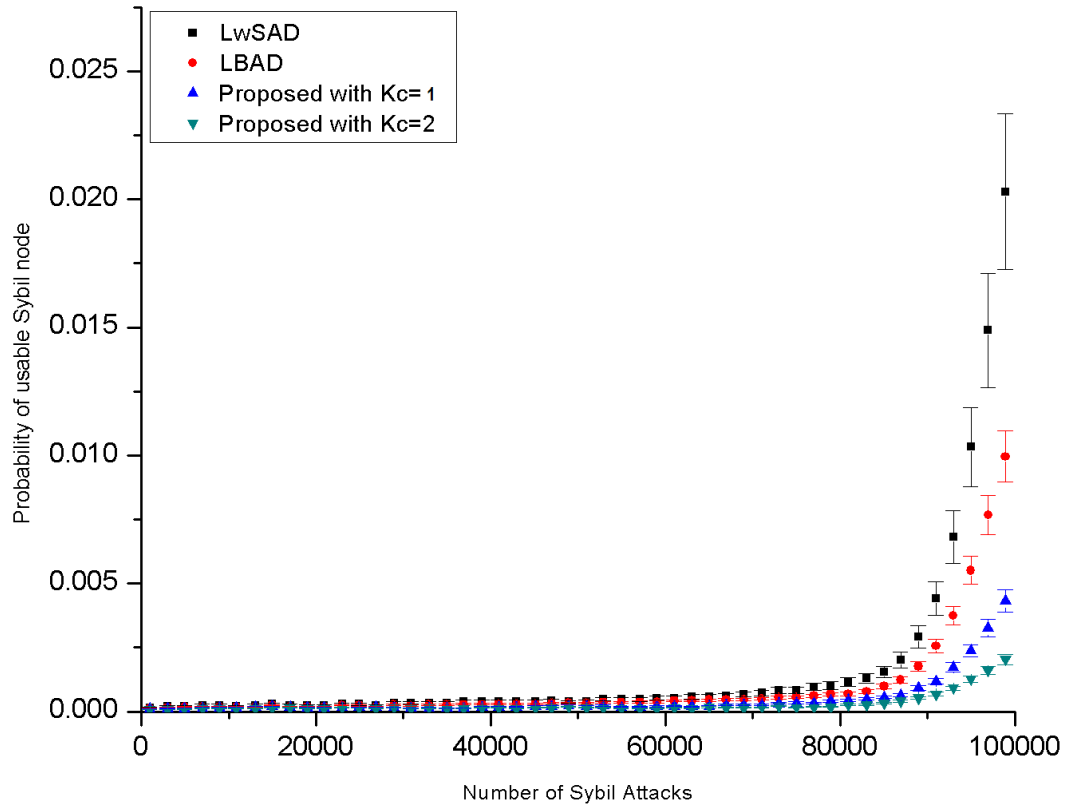


FIGURE 3.7: Probability that a Sybil Node will go Undetected by the Various Algorithms.

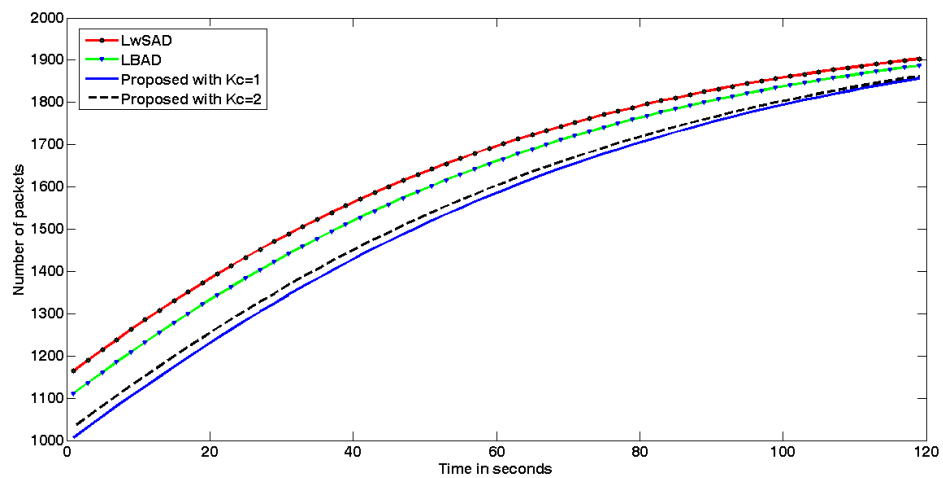


FIGURE 3.8: Simulated Traffic behavior of the WSN while executing the proposed and existing authentication schemes



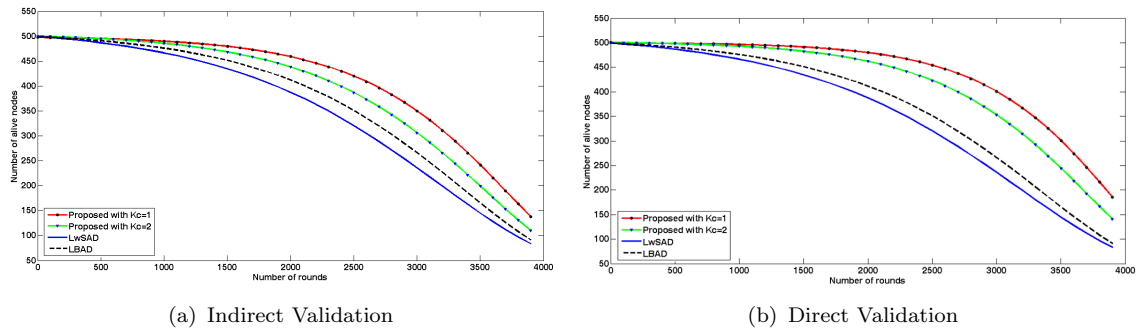


FIGURE 3.9: Power Consumption and Remaining Number of Alive Nodes as a Result of Power Consumption by Participating Nodes During the Process of Authentication in Various Algorithms

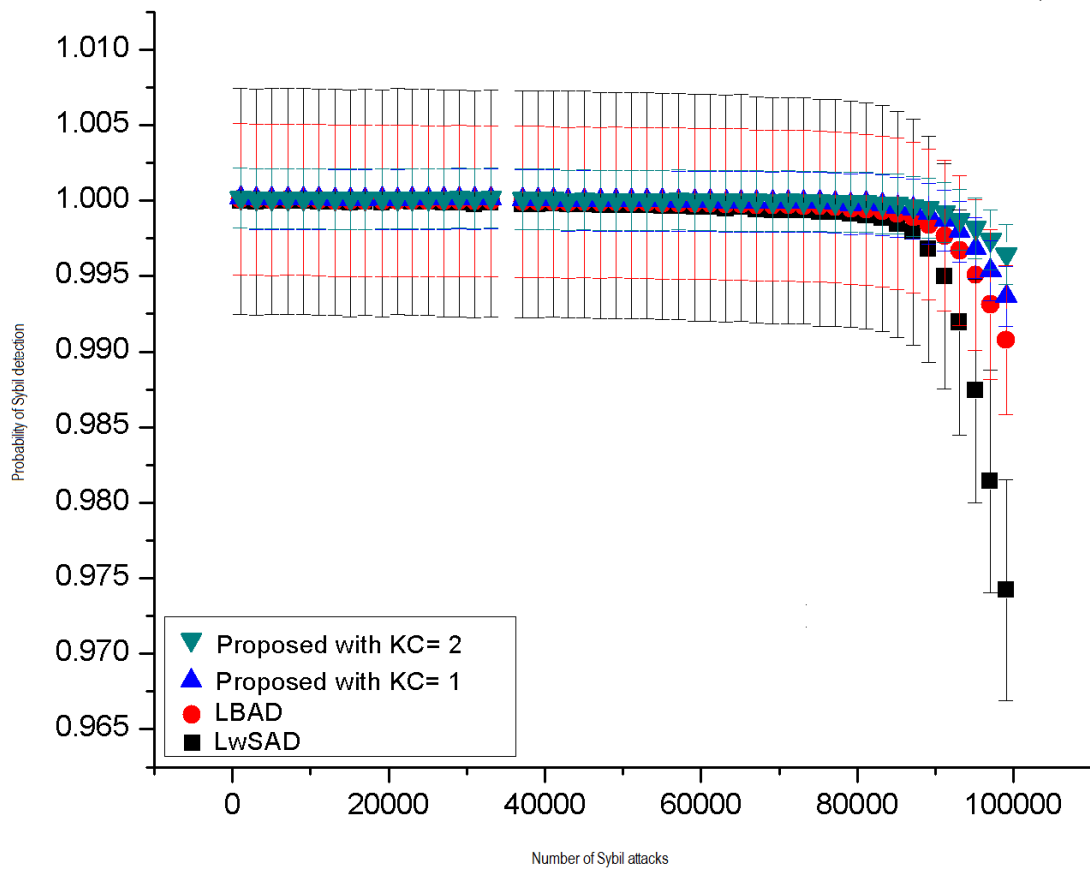


FIGURE 3.10: Probability of Sybil Node Detection by the Proposed Algorithm in Comparison with the Existing Algorithms

### **3.5.2 Traffic Analysis**

The life time of a Wireless Sensor Network is directly proportional to the rate of exchange of packets. Excessive amount of packet exchange leads to a rapid battery drain due to which the network may die out. Fig 3.8 shows the behavior of algorithms against the traffic of the network during authentication process. It can be observed from the figure that the proposed scheme produces lesser number of packets in both cases of  $N_{K_c}=1$  and  $N_{K_c}=2$  as compared to LBAD and LwSAD. The number of packets generated is also directly proportional to the number of authentication rounds launched by a node or CH and will thus be borne at the cost of enhanced security of the network. this result also verifies our claim that the proposed scheme consumes lesser processing power and does not adversely affect the network life time.

The little overhead produced as a result of exchange of packets regarding authentication of the nodes can be bared at the cost of secure network. The traffic overhead is directly proportional to the number of authentication procedure launched by CH or SN depending upon the network.

### **3.5.3 Node power consumption**

While designing a protocol for sensor nodes, the power consumption should always be taken on-board especially when the network has no resource of additional power supply once deployed. The power consumption of nodes is also calculated in case of direct and indirect validation of the nodes. As already discussed, the indirect validation requires more processing and communication power as compared to direct validation. Fig 3.9 (a and b) illustrates the results of simulation with respect to power consumption in both direct and indirect validation process against authentication rounds. The graph shows the combined power consumption of all nodes either at both ends of the communication link or at the intermediate nodes during the process of authentication of a node or a set of nodes. The proposed

authentication protocol consumes much lesser power in indirect validation as compared to direct validation as shown in Fig 3.9 (a and b). The power consumption in case of indirect validation is due to information exchange like challenge and SRes between the originating and destination sensor nodes. This operation engages all the nodes that come in the path. Power consumption in case of indirect validation thus depends significantly on number of nodes. Larger networks will consume more power in indirect validation and vice versa.

### **3.5.4 Probability of attack detection**

Probability of attack detection is a major parametric criterion to evaluate the performance of a security algorithm. Fig 3.10 represents the probability of detection shown by each algorithm applied on the network. It can be clearly seen that the proposed algorithm provides a better protection against the Sybil attacks. If we increase the pool size of keys in the sensor nodes, the situation will become even harder for the Sybil Node. However this may demand more memory and processing capability available at each sensor node. Therefore we limited the size up to  $N_{K_c}=2$ . The pool size thus is subject to the requirement of the desired security level, power availability at the sensor nodes and number of nodes in the network.

## **3.6 Chapter Summery**

The existing approaches of defense against the Sybil attacks are becoming incapable day by day due to increase in the processing power and capability of attacking nodes. A Sybil node can now launch thousands of attacks before its battery gets drained or its processing capability is exhausted. In this chapter, we have proposed a Sybil attack detection mechanism which is based on the SRes authentication mechanism developed for Global System for Mobile (GSM) communications. The SRes mechanism is responsible for authenticating the user and encrypting the voice data. The proposed scheme can be implemented in both hierarchical and centralized Wireless Sensor Networks. The proposed scheme has been

analyzed for its performance under various Sybil attacks. The scheme has been evaluated for its probability of detecting Sybil nodes when different authentication key pool sizes are utilized. After extensive simulations, it has also been observed that the proposed scheme is able to detect Sybil attacks with higher probability as compared to existing state-of-the-art existing schemes. It has been observed that the proposed Sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same Sybil detection performance.

# Chapter 4

## SEER: Secure and Energy Efficient Routing mechanism

### 4.1 Overview

Wireless Sensor Network (WSN) is a self-configuring wireless network composed of either static or mobile nodes without any infrastructure (ad-hoc mode). The Sensor nodes in a network are equipped with variety of functions like sensing, processing, aggregation, exchange of data etc[107]. The size of a WSN may range from a few hundred to thousands of nodes depending upon the requirement in the area of interest. Energy efficiency and security are two major and all time open issues in WSN [108]. Energy efficiency is the process of preventing a node to drain its power while performing various functions like processing, sensing, communication and other internal executions. One of the beauty of WSN is its function in hostile environment where the power source can not be replaced once a node is deployed [109]. Also, with the advent of MEMS technology, the scope of a sensor node can be enhanced by mounting new features over its sensor board. However, such features will expedite the energy drainage of a node [110]. Thus, a sensor node may die in relatively lesser time after its deployment if its operations are handled improperly. In other words, an energy efficient node is the one whose

operations consume minimum power during execution. Such operations include routing, sensing, processing, authentication and security. Apart from the usual operations that any sensor node has like sensing, processing and routing, security can be termed as a top-up for enhanced features. Traditionally, the security in WSN is referred to three main domains, confidentiality, integrity and availability of data. Violating confidentiality of data refers to the learning of sensitive information by unauthorized entity [111]. Integrity violation occurs when someone modifies the information without having proper rights and finally the violation of availability of a system is when the system starts malfunctions or is prevented to perform its desired function [112]. This research mainly focuses on the use of WSNs in such hazardous areas like battle field, fire zone etc. where security and energy efficiency are the issues of major concern. In a battle field, various types of sensor nodes can be deployed like soldier trackers and acoustic sensors to monitor the approach of enemy while securing the parameters [113]. Other extreme application is the fire zone where human access is not possible. Here, the sensor is mainly used for detecting life inside the building, taking the readings of fire and collecting building information.

A Wireless Sensor Network is always prone to various types of attacks that can be launched to interfere the operation and steal or forge the data like wormhole, sinkhole, Sybil attacks [114]. The network once gained by the attacker may start malfunctioning in various ways which must be monitored and isolated after detection [115]. The sensor nodes once deployed mostly become vulnerable and inaccessible in hostile situation for the replacement of power source or other modules. Thus, in addition to securing data during routing, the nodes in such situation must also be able to prevent the wastage of energy in order to prolong the network life. The routing protocol must be able to select the most optimum path for the routing of data to minimize the energy consumption. Thus, there are two focused objectives, energy efficiency, and security of the data. Most of the existing routing protocols can handle either energy efficiency or security of data at a time [114]. Moreover, the security algorithms are mostly implemented as part of application

layer causing additional cosmetics and overheads for processor, which at one side, although provides the security but consumes much more processing power at the other side. The routing protocol must balance the two objectives of energy and security by implementing the security algorithm at hardware level instead of its implementation at application level.

This chapter proposes a secure and energy efficient scheme for routing of data known as Secure and Energy Efficient Routing (SEER) that not only provides end to end security of data but also strives to minimize energy consumption. The proposed scheme is designed to be implemented at hardware level to minimize the processing overhead and save battery power. We use GRACE routing protocol as a platform for the routing of data in an energy efficient way. The GRACE protocol is necessarily modified in order to fit-it-in the scenarios of secure routing. The simulation results show that the proposed security module is not only energy efficient but also provides a strong security against data interception attacks. In order to prove the efficiency, the proposed algorithm is compared with two notable secure routing i.e. An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks (ETRAP) [116] and secure routing protocol using cross layer design and energy harvesting in wireless sensor networks [117].

The proposed scheme introduces a secure and energy efficient routing mechanism by embedding A5 encryption scheme with the energy efficient routing protocol. The A5 encryption scheme is also used for voice encryption in Global System for Mobile communications (GSM) [106]

We embed packet securing info in to header for the safe arrival of data at the destination. One of the beauty of A5 algorithm is that it can create a key for encryption of any length. Thus, the proposed scheme can support the data packet of 32,64 and 128 bits. The proposed routing protocol can be implemented both at centralized as well as hierarchical sensor network depending upon the needs and requirements. Simulations are performed to validate the performance of the proposed algorithm in *MATLAB*<sup>®</sup>. From the simulation results, we prove that

the proposed scheme is not only secure enough to protect the data, but also requires lesser processing and battery power as compared to notable existing data securing schemes. Also, the proposed scheme consumes lesser convergence time to become ready for exchange of data. Moreover, the scheme creates little message overhead resulting in negligible increase in the traffic of the network.

## 4.2 Working of A5 algorithm used in GSM

As discussed earlier, the A5 encryption procedure is originally designed for second generation GSM based networks. This mechanism is responsible for the confidentiality of voice data between the parties. The Subscriber Identity Module (SIM) contains the ciphering key generating algorithm, the A8 algorithm. The A8 algorithm is used to calculate the 64-bit ciphering key ( $K_c$ ) which is used to encrypt the voice data before it is sent over the channel. The ciphering algorithm A5 ensures the secure communication between the Mobile Station (MS) and the network. The GSM network initiates a request and sends it to mobile station over the control channel. The mobile station is first authenticated through Signed Response utilizing A3 algorithm.

After successful authentication, the following steps are carried out in order to incorporate voice encryption mechanism:

1. The mobile station receives a random number RAND from the Base Station (BS) as a challenge.
2. The Mobile Station generates a key known as Session Key  $K_c$ .
3. This session key is produced by utilizing the A8 algorithm, the Subscriber Authentication Key  $K_i$  assigned to each Mobile Station, and the random challenge RAND.
4. The Mobile Station sends the Session Key  $K_c$  to the BTS.



5. In the meanwhile, the Mobile Services Switching Center also produces and sends its Session Key  $K_c$  to BS.
6. The BS receives the Session Key  $K_c$  from the Mobile Services Switching Center and the mobile station and compare them to verify its authenticity.
7. The BS verifies the Session Keys received from the Mobile Station and the Mobile Services switching Center. The voice encryption algorithm A5 is then initialized with the verification of the Session Key  $K_c$  . The A5 encryption scheme uses three shift register in processor i.e. X, Y, Z the values assigned to these registers are as follow:
  - (a) X= 19 bits (X0, X1, X2, X18) first 19 bits of  $K_c$  loaded to X
  - (b) Y= 22 bits (Y0, Y1, Y2, Y21) next 22 bits loaded to register Y
  - (c) Z= 23 bits (Z0, Z1, Z2, Z22) last 23 bits loaded to register Z

Fig. 4.2 and Fig. 4.3 represent the execution of process inside a processor. After the bits are shifted to the respective registers, a majority rule is applied to elect the successor. For this purpose, bits from position X8 Y10 and Z10 are picked from X, Y and Z registers respectively. The majority rule picks two successors based on bit one or bit zero. The position having maximum numbers of 1s or 0s will become successor like in our example the register X and register Z are the successors as there are two 1s and one 0. In the next step, the two registers X and Z are stepped forward. In register X the position 13th, 16th 17th and 18th are taken and XoRed with each other the result is saved at LSB by shifting the register values to right side. Similarly, from the Z register, the bits from position 7th, 20th, 21st and 22th are picked and XoRed with each other saving the result at LSB.

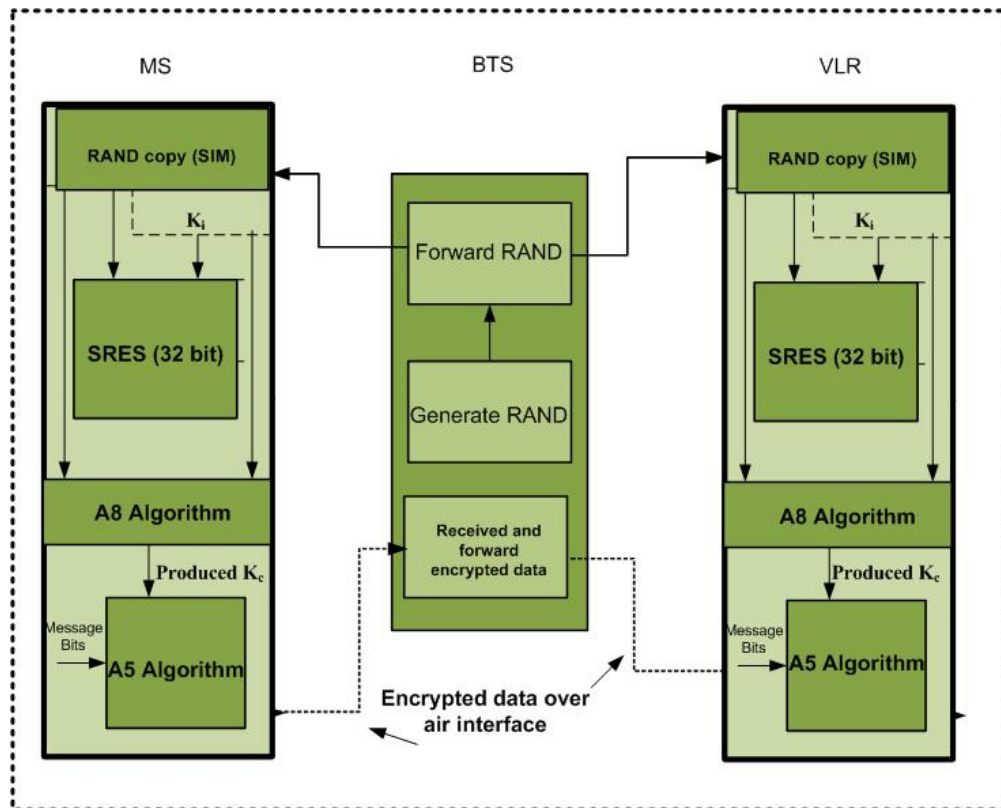


FIGURE 4.1: Encryption and Decryption of voice in GSM

### 4.3 The Proposed Secure and Energy Efficient Routing (SEER)

In order to implement the A5 encryption mechanism in WSN, necessary modifications have been made in the existing encryption/decryption scheme implemented in GSM as shown in Fig. 4.4. The A5 algorithm was originally designed for voice encryption in GSM technology. The wireless sensor networks, on the other hand, have different dynamics and requirements from mobile communication. Therefore necessary modifications have been carried out in order to implement it for secure data communication in WSNs. The data security mechanism can then be used in both in ad-hoc network environment. In ad-hoc mode a sink is responsible to encrypt/decrypt the data sent by a source node. As discussed earlier The A5 algorithm was originally designed for voice encryption in GSM technology. The wireless sensor networks, on the other hand, have different dynamics and requirements from mobile communication. The necessary modifications have been carried

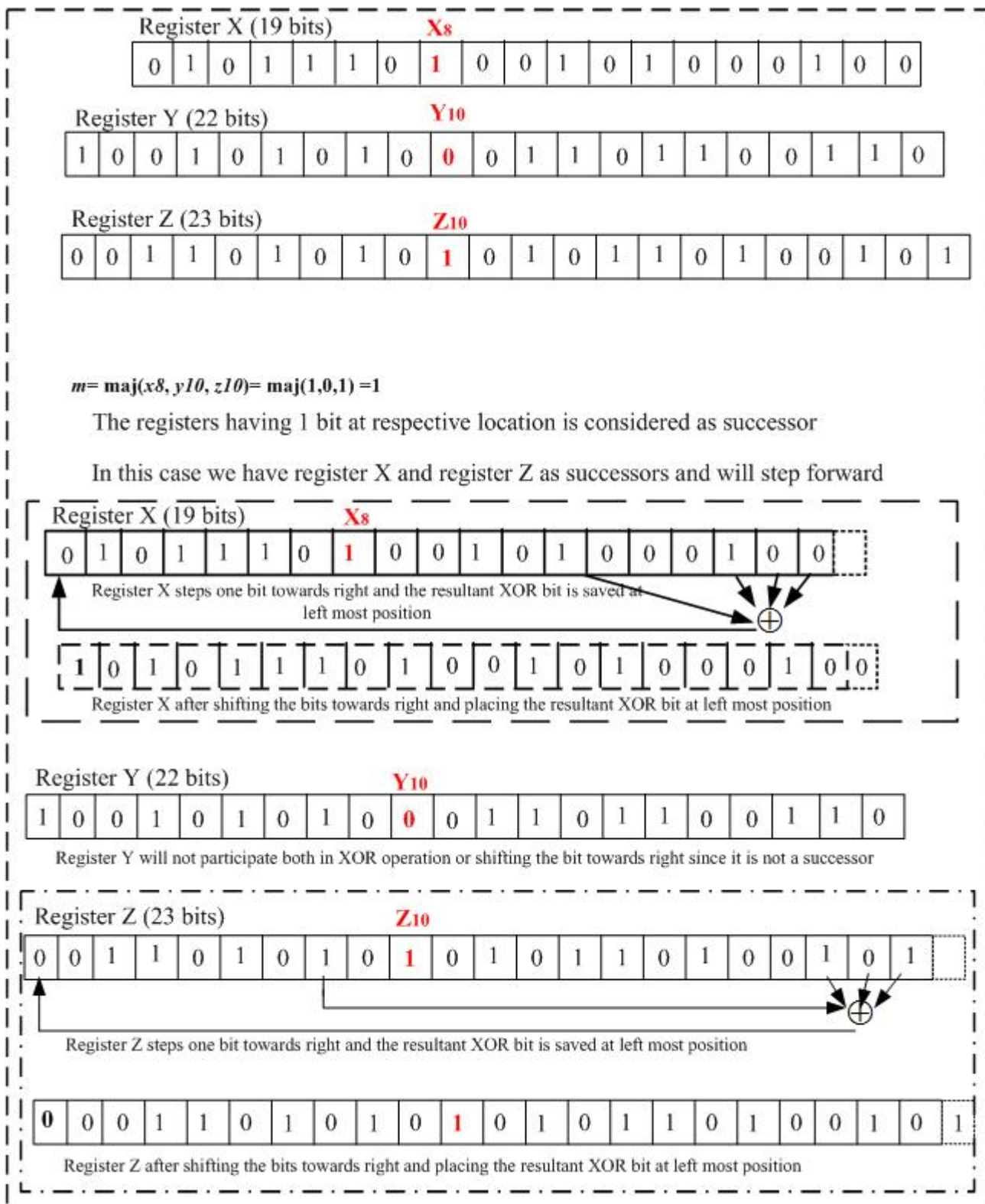


FIGURE 4.2: A: Formation of Ciphering key

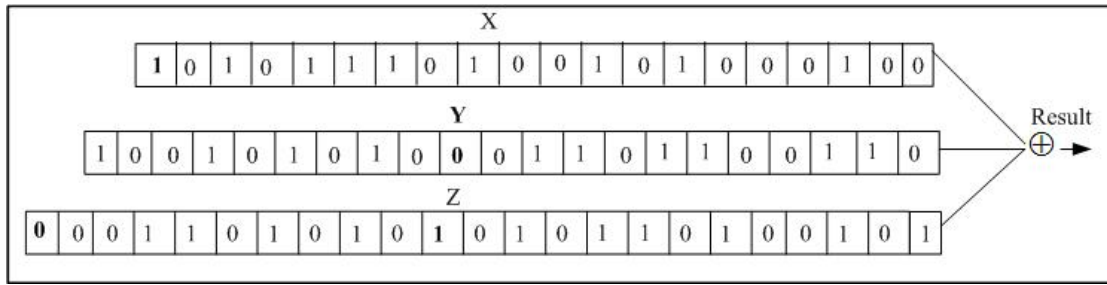


FIGURE 4.3: B: Final 64 bit Ciphering key

out in order to implement it for secure data communication in WSNs. The step by step procedure of the proposed algorithm is given below:

1. The Base Station generates a 128-bit random challenge known as RAND
2. RAND is forwarded to the sensor nodes as a challenge in order to authenticate it.
3. the sensor node starts to calculate the session key  $K_c$  with the help of A8 and  $K_i$ .
4. The algorithm A8 and the key  $K_i$  is already provided to the node
5. The BS also starts to calculate the session key  $K_c$
6. The Sensor node sends the  $K_c$  to the BS, CH, Sink or Server
7. The BS receives the  $K_c$  and matches it with its own produced  $K_c$
8. If both the  $K_c$ 's are same it means the communicating nodes is a valid node else, the  $K_c$  is discarded and node ID is black listed.
9. The data is sent encrypted over air interface

## 4.4 Data Encryption Algorithm for the Proposed SEER

The following are the terminologies used in the given algorithm:

$\mathcal{Y}$  is a 19 bit binary key

$\Omega$  is 22 bit binary key

$\Psi$  is a 23 bit binary key

$K_c$  represents the output key, used as a session key for data encryption

$\beta$  is the length (number of bits) of the output key

$\uplus$  used as an operator to add new bit to the current vector

---

**Algorithm 2** Pseudocode of the A5 Algorithm used in Proposed SEER for Data Encryption

---

$RAND$  is a 128 bit key, received from base-station

$K_i$  is a 128 bit key, stored in the node

$S \leftarrow (RAND_{1,64} \oplus RAND_{65,128}) \oplus (K_i1, 64 \oplus K_i65, 128)$

$\Upsilon \leftarrow S_{1,19}; \Omega \leftarrow S_{20,41}; \Psi \leftarrow S_{42,64}$

$epoch \leftarrow 1, \beta \leftarrow 16$

$\alpha \leftarrow mode(\Upsilon_8, \Omega_{10}, \Psi_{10})$

**foreach**  $epoch < \beta$  **do**

**if**  $\Upsilon_8 = \alpha$  **then**

        |  $b \leftarrow \Upsilon_{16} \oplus \Upsilon_{17} \oplus \Upsilon_{18} \oplus \Upsilon_{19}$  shift  $\Upsilon$  one bit right and append  $b$  to the left

**end**

**if**  $\Omega_{10} = \alpha$  **then**

        |  $b \leftarrow \Omega_7 \oplus \Omega_{20} \oplus \Omega_{21} \oplus \Omega_{22}$  shift  $\Omega$  one bit right and append  $b$  to the left

**end**

**if**  $\Psi_{10} = \alpha$  **then**

        |  $b \leftarrow \Psi_8 \oplus \Psi_{21} \oplus \Psi_{22} \oplus \Psi_{23}$  shift  $\Psi$  one bit right and append  $b$  to the left

**end**

$K_c \leftarrow K_c \uplus b$

**end**

$Data_{enryp} \leftarrow K_c \oplus Data_{sensing}$

---

The above steps are also explained in algorithm 2. Fig. 4.5 illustrates a distributed network with hierarchical structure having Cluster Heads (CHs) along with the member sensor nodes. We assume that the CH be a powerful node that may become a sink in case of a centralized network and are directly connected to gateway or base station. The malicious Nodes are assumed to be present in the network and they have the complete information of security mechanism of the network. The CH is responsible to convey encrypted data transmitted from low powered sensor nodes present in its vicinity to sink, gate way or base station. The CH sends report of any malicious activity to the BS or any controlling entity if determined. Although only one BS is shown in figure but there could be as many BS as required by the network and environment. The deployment of nodes can

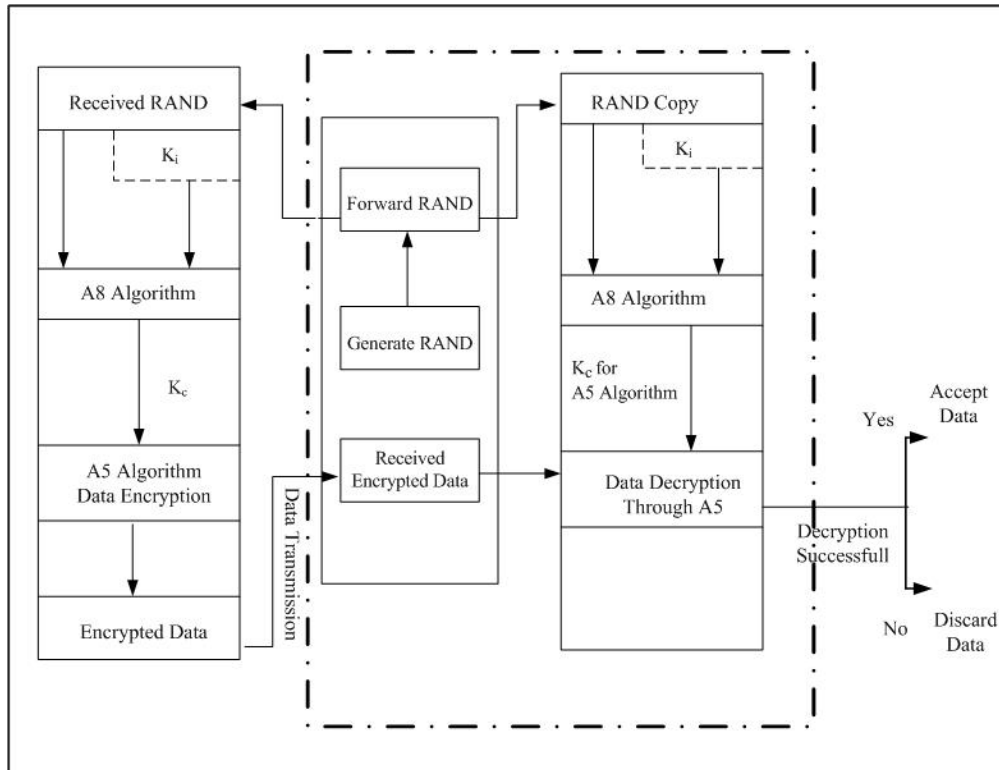


FIGURE 4.4: Block diagram of data encryption/decryption in WSN

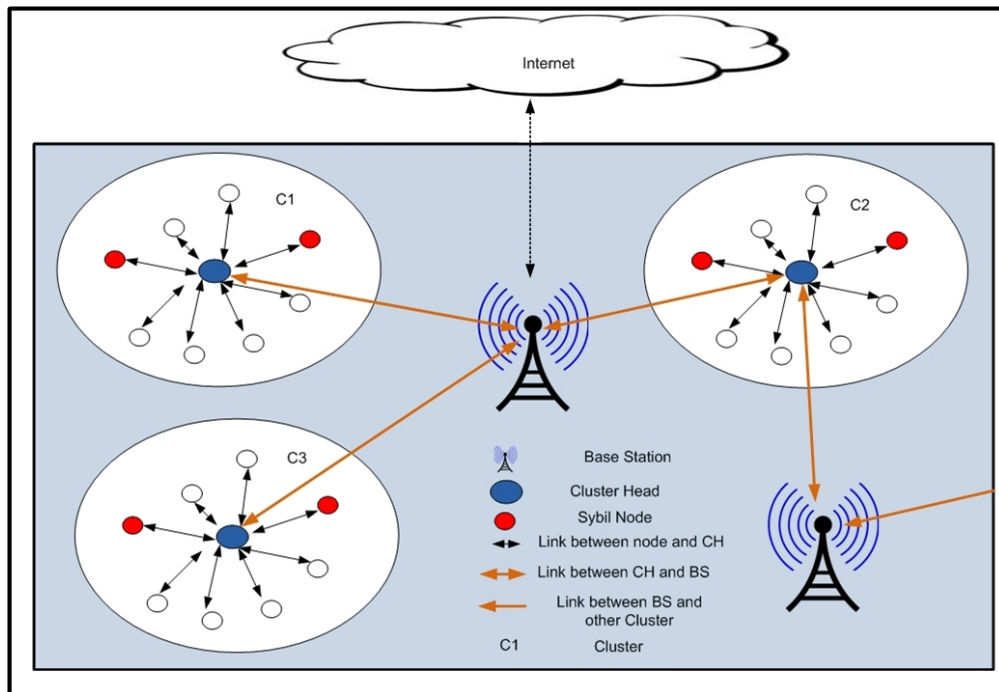


FIGURE 4.5: Data Routing in a Wireless Sensor Network With the Presence of Malicious Nodes

be Aerial or manual depending upon the nature of physical environment. Each sensor node is assigned an ID and the position of the sensor node is assumed to

be known to it. We also assume that the sink or cluster head has all the necessary information about member sensor nodes like sensor' ID, MAC address and the assigned authentication key  $K_i$

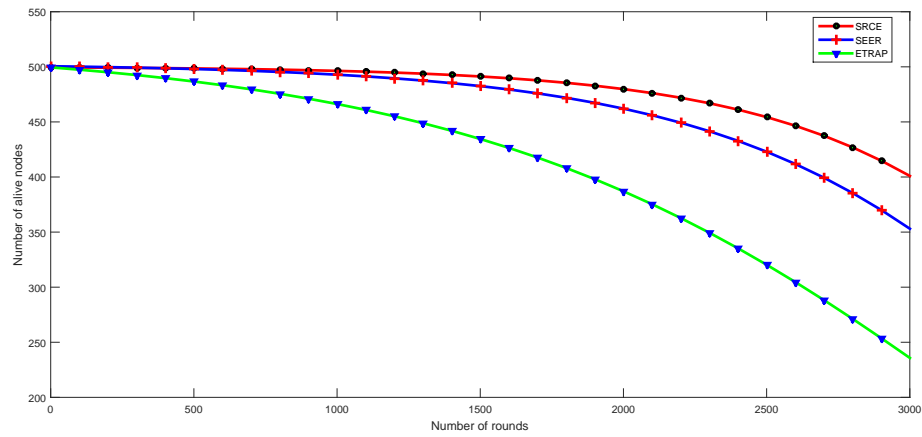


FIGURE 4.6: Lifetime Comparison of SEER with SRCE and ETRAP

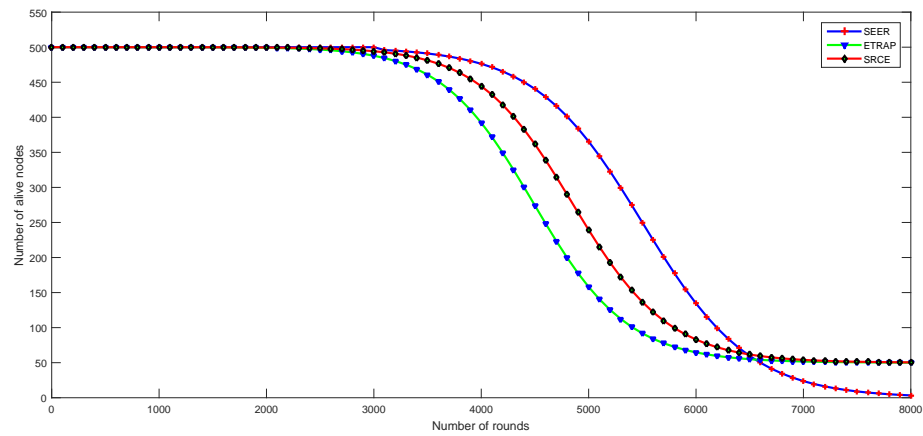


FIGURE 4.7: Lifetime Comparison of SEER with SRCE and ETRAP without Energy Harvesting Module with SRCE

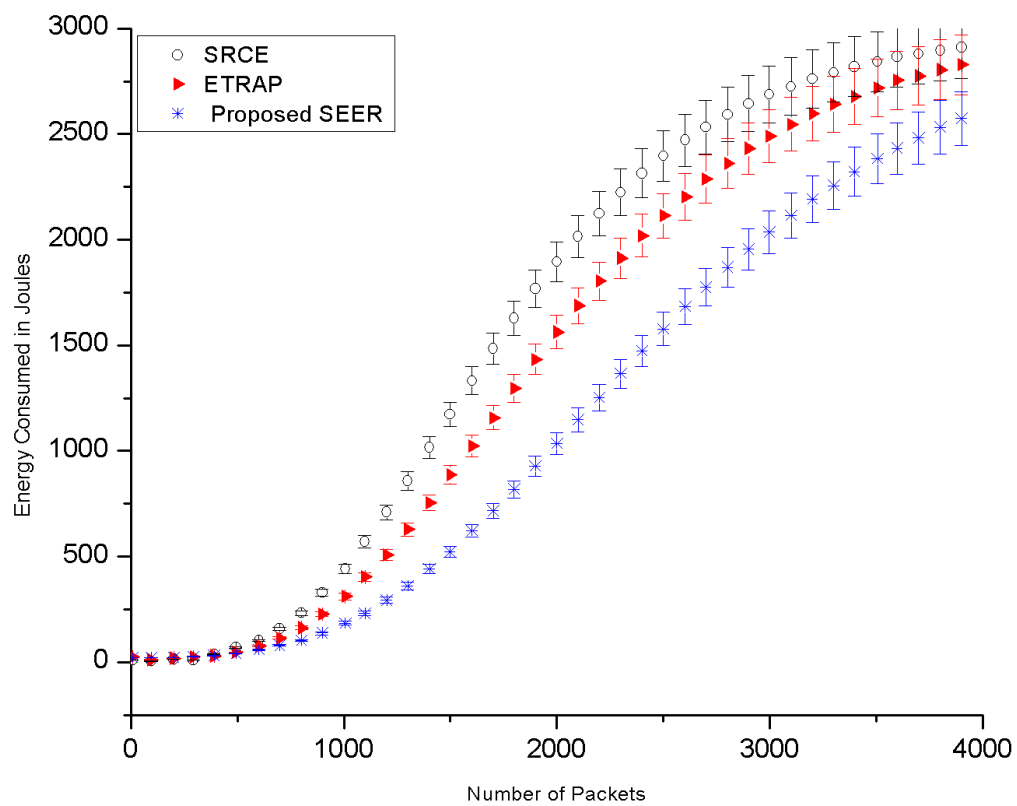


FIGURE 4.8: Energy Consumed by Each sensor node



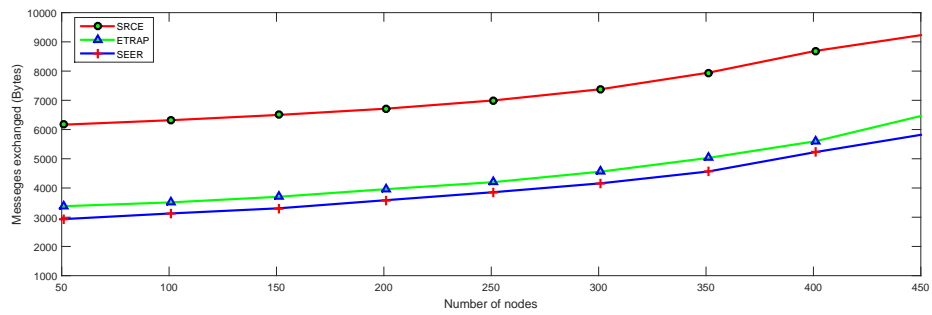


FIGURE 4.9: Message exchanged at various number of nodes

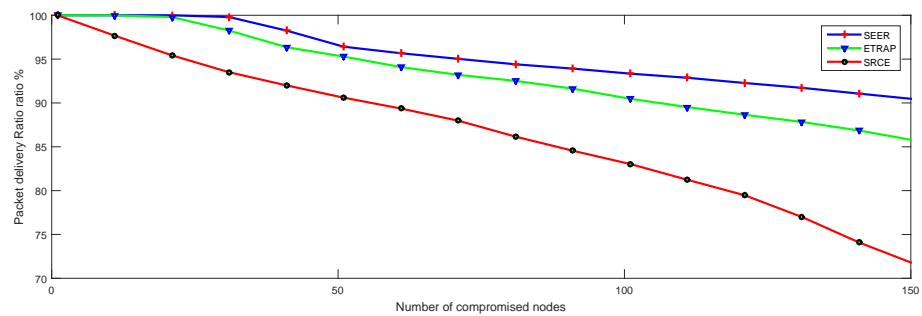


FIGURE 4.10: packet delivery ratio in presence of compromised nodes

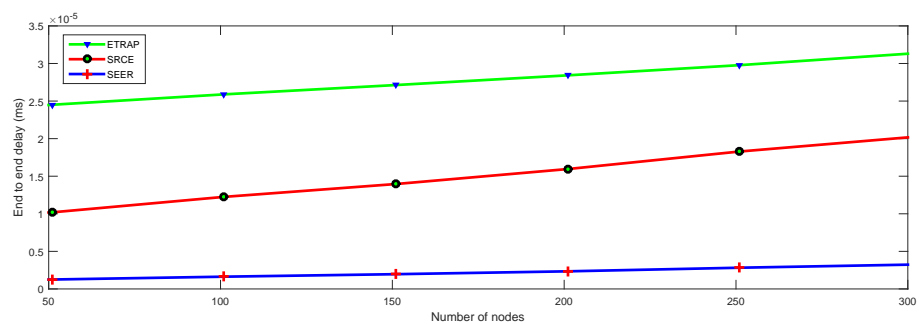


FIGURE 4.11: End to end delay by each protocol

#### 4.4.1 Probability of Interception

Let  $n$  be the length of random generated binary keys. Thus there are  $2^n$  different keys. the probability to generate a particular key  $K_i$  of  $i$ th node is given by

$$P(K_i \text{ generation}) = \frac{1}{2^n} \quad (4.1)$$

To split the key  $K_i$  into  $D$  distinct integral parts of lengths  $n_1, n_2, n_3, \dots, n_D$  such that

$$\sum_{d=1}^D n_d = n \quad (4.2)$$

Where  $n_d$  is the length of the  $d$ th part of  $k_i$  with the condition that:

$$1 < nd < n - 1 \quad (4.3)$$

In order to distribute the key  $K_i$  in  $d$  registers subject to equation 2. Total number of possible combinations  $C_n =$ :

$$\left[ \prod_{d=1}^{D-1} \frac{n - 2D + d}{d} \right] \left[ \sum_{i=0}^n \binom{n}{i} \right] \quad (4.4)$$

Where  $D$  is the number of distinct group registers and  $n$  is the length of  $K_i$ .

Thus the probability to split a key  $K_i$  of length  $n$  into  $D$  different keys is given by:

$$P(\text{group key}) = \frac{1}{C_n} \quad (4.5)$$

$$= \frac{1}{\left[ \prod_{d=1}^{D-1} \frac{n - 2D + d}{d} \right] \left[ \sum_{i=0}^n \binom{n}{i} \right]} \quad (4.6)$$

Thus the probability of selecting a random bit from each of these  $D$  group registers and its exploitation in  $l$  possible binary operations is given by:

$$P(\text{bits selection}) = \frac{1}{l} \prod_{i=1}^D \frac{1}{n_i} \quad (4.7)$$

Where  $n_i$  is the number of bit in  $i$ th group register. To perturb the register settings, any subset of bits of each register may be selected and one out of  $l$  different binary operations may be performed. The perturbation probability is given by:

$$P(\text{Perturbation}) = \frac{1}{l} \prod_{i=1}^d \frac{1}{|2^{n_i}|} \quad (4.8)$$

where  $|2^{n_i}|$  is the cardinality of power set of  $i$ th group registers having length  $n_i$ . Since the order of bits does not matter in case of binary operations, therefore we use the cardinality of power set. Now the probability to generate a valid key is given by:

$$\begin{aligned} &= P(\text{valid key}) = P(K_i \text{ generation}) \cdot \\ &\quad P(D \text{ distant group key generation}) \cdot \\ &\quad P(\text{bit selection}) \cdot P(\text{Perturbation}) \quad (4.9) \end{aligned}$$

$$= \frac{1}{2^n} \cdot \frac{1}{C_n} \cdot \frac{1}{l} \prod_{i=1}^D \frac{1}{n_i} \cdot \frac{1}{l} \prod_{i=1}^D \frac{1}{|2^{n_i}|} \quad (4.10)$$

$$= \frac{1}{l^2 2^n} \cdot \frac{1}{C_n} \cdot \prod_{i=1}^d \frac{1}{n_i |2^{n_i}|} \quad (4.11)$$

$$= \frac{1}{l^2 2^n} \cdot \frac{1}{\left[ \prod_{d=1}^{D-1} \frac{n-2D+d}{d} \right] \left[ \sum_{i=0}^n \binom{n}{i} \right]} \cdot \prod_{i=1}^d \frac{1}{n_i |2^{n_i}|} \quad (4.12)$$

## 4.5 Results and Discussion

The performance of the proposed SEER mechanism is evaluated through different parameters like number of alive nodes, energy consumed by the sensor nodes,

traffic overhead, packet delivery ratio and end-to-end delay. Extensive simulations have been carried out for the evaluation purpose using a simulation scenario of 500 nodes deployed randomly in 100 m x 100 m area. The simulation was run for multiple times in an attempt to obtain average results for the above mentioned parameters. The obtained results are then compared with the two notable secure routing protocols ETRAP and SRCE.

Energy consumption can only be verified by factoring in the comparison based on the number of alive nodes. It helps us analyze how much processing overheads are imposed by an algorithm on sensor nodes that suck their energy. Fig. 4.6 shows the life time comparison of SEER with SRCE and ETRAP. As discussed earlier, SRCE is an energy harvesting protocol; thus, the nodes harvest energy from an external source during its operation. Therefore the number of alive nodes of SRCE is greater than the SEER and ETRAP. However, the SEER still outperforms and stays longer even in extreme sensing environment. However, if SRCE is run without energy harvesting module, its lifetime curve falls much faster than SEER and ETRAP as shown in the figure. Fig.4.7 and Fig. 4.8 depicts the energy consumed by each sensor node for both scenarios when SRCE runs with and without energy harvesting module respectively. The total energy consumed by individual sensor node includes data packet formation, route selection, routing table, data security mechanisms and data routing. However, more energy may be consumed in procedures specific to particular protocol.

Fig. 4.9 represents a traffic overhead comparison of the three protocols. The comparison is done in terms of number of packet exchanged between nodes and the base station or gateway . These messages include control overheads, data packets, acknowledgments etc. The figure shows that ETRAP has a great traffic overhead as compared to SRCE and SEER. Both SRCE and SEER give almost similar result till the number nodes reach to 400 where the trend of the plot seems to be different. The plot shows a clear change when the number of nodes reaches to 450 where the similarity of SEER and SRCE performance begin to break.

Fig. 4.10 shows the packet delivery ratio in the presence of malicious nodes. The presence of malicious nodes deeply affects the performance of a network. This may lead the network to degrade its packet delivery. The figure shows a comparative analysis packet delivery ratio of SEER in comparison with ETRAP and SEER. This result has been taken in the presence of a variable number of compromised or malicious nodes. As it can be seen that ETRAP has a very rapid fall in throughput with the number of increased malicious nodes. SEER and SRCE, however, provide a better result against the initial number of compromised nodes as can be seen in the result. There is a slight fall in both SEER and SRCE in the malicious nodes between 40-50 but SEER again provides a constant and satisfactory data rate as compared to SRCE.

Fig. 4.11 shows the end to end delay of data among the nodes. The delay is calculated as the time taken by the protocol to take a packet from source to destination. This delay also includes the time taken by the node to place a bit on the medium after being encrypted. It has been observed that the SEER has the lowest end to end delay among all. This is because the GRACE by its self has a fast mechanism for selecting the most optimum route before transmitting the data and adds less overhead to it as compared to other ETRAP and SRCE. Since the SEER is designed to work at hardware level, therefore, it adds comparatively less overhead resulting a minimum end to end delay.

## 4.6 Chapter Summery

In this chapter, a secure mechanism for routing data from source to sink in wireless sensor networks known as SEER (Secure and Energy Efficient Routing protocol) is proposed. The proposed protocol is based on A5 encryption scheme developed for Global System for Mobile communications (GSM). SEER has been tested through simulations in *MATLAB*<sup>®</sup> by setting up hostile and vulnerable wireless sensor network scenarios with respect to data integrity. The results obtained were then compared with other two notable secure routing protocols. It is proved that the

proposed SEER helps achieve the desired performance under dynamically changing network conditions with various number of malicious nodes. Due to its linear complexity, lesser power consumption and more dynamic route updation, the proposed Sybil detection and SEER schemes can be easily extended to cater to the needs of emerging industrial wireless sensor networks, and IoT. Emerged from the conventional Wireless Sensor Networks, all the aforementioned networks have got the same nature of vulnerabilities and threats along with the inherited limitations with respect to their hardware and processing.

## Chapter 5

### Conclusion and Future Work

Wireless sensor networks have always been under serious security threats due to their diverse applications especially in vulnerable and hostile environments. The unattended nature of WSNs leads to various security attacks that are launched to gain control of a node or the entire network. Similarly secure routing of data in such vulnerable situations is another issue that needs to be addressed to avoid sensitive data from being captured or tempered. In this regard, we have proposed a Sybil attack detection mechanism and a Secure and Energy Efficient Routing (SEER). Both of the proposed schemes are based on the SRes authentication and voice encryption mechanisms developed for Global System for Mobile (GSM) communications.

In the proposed node authentication scheme, the Sybil attack, which is one of the most widely launched attack in WSNs and its counter measure is focused. In the proposed scheme, the A3 algorithm embedded in each sensor node, produces a signed response against the challenge sent by the Cluster Head (CH) or any relay node to validate itself as a legitimate node. Upon the reception of SRes from the source node, the CH or relay node verifies the response and acts accordingly.

The SRes mechanism is responsible for authenticating the user before it becomes part of network. The proposed sensor node authentication scheme can be implemented in both hierarchical and centralized Wireless Sensor Networks. The scheme has been analyzed for its performance under various Sybil attacks. The

scheme has been evaluated for its probability of detecting Sybil nodes when different authentication key pool sizes are utilized. After extensive simulations, it has been observed that the proposed scheme is able to detect Sybil attacks with higher probability as compared to existing schemes. Moreover, it has also been observed that the proposed Sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same Sybil detection performance.

SEER proposed in this thesis is a secure mechanism for routing of data in wireless sensor networks. The proposed protocol is based on A5 encryption scheme developed for Global System for Mobile communications (GSM). The A5 algorithm in GSM is responsible for encrypting the voice data between the two parties while the voice call is established. In our proposed SEER scheme, the sensor node produces a 64-bit key known as  $k_c$  and is perturbed by utilizing three shift registers. The resultant bit stream is then used for data encryption. We use GRACE routing protocol as a platform for the routing of data in an energy efficient way. The GRACE protocol is necessarily modified in order to fit-it-in the scenarios of the secure routing. SEER has been tested through simulations in *MATLAB*<sup>®</sup> by setting up hostile and vulnerable wireless sensor network scenarios with respect to data integrity. The results obtained were then compared with two existing secure routing protocols. We have proved that the proposed SEER helps to achieve the desired performance under dynamically changing network conditions with various number of malicious nodes. Due to its linear complexity, lesser power consumption and more dynamic route updation, the proposed Sybil detection and SEER schemes can be easily extended to cater to the needs of emerging industrial wireless sensor networks, and IoT. Emerged from the conventional Wireless Sensor Networks, all the aforementioned networks have got the same nature of vulnerabilities and threats along with the inherited limitations with respect to their hardware and processing.



# Bibliography

- [1] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks*. John Wiley & Sons, 2010, vol. 4.
- [2] C. Zhou and B. Krishnamachari, “Localized topology generation mechanisms for wireless sensor networks,” in *Global Telecommunications Conference, 2003. GLOBECOM’03. IEEE*, vol. 3. IEEE, 2003, pp. 1269–1273.
- [3] N. Bulusu, D. Estrin, L. Girod, and J. Heidemann, “Scalable coordination for wireless sensor networks: self-configuring localization systems,” in *International Symposium on Communication Theory and Applications (ISCTA 2001)*, Ambleside, UK, 2001, pp. 1–6.
- [4] G. J. Pottie and W. J. Kaiser, “Wireless integrated network sensors,” *Communications of the ACM*, vol. 43, no. 5, pp. 51–58, 2000.
- [5] V. P. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar, and N. Shroff, “A minimum cost heterogeneous sensor network with a lifetime constraint,” *IEEE Transactions on Mobile Computing*, vol. 4, no. 1, pp. 4–15, 2005.
- [6] M. L. Sichitiu and V. Ramadurai, “Localization of wireless sensor networks with a mobile beacon,” in *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on*. IEEE, 2004, pp. 174–183.
- [7] A. Koubaa, A. Cunha, and M. Alves, “A time division beacon scheduling mechanism for ieee 802.15. 4/zigbee cluster-tree wireless sensor networks,” in *Real-Time Systems, 2007. ECRTS’07. 19th Euromicro Conference on*. IEEE, 2007, pp. 125–135.

- 
- [8] K. A. Kumar, A. V. Krishna, and K. S. Chatrapati, "Interference minimization protocol in heterogeneous wireless sensor networks for military applications," in *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2*. Springer, 2016, pp. 479–487.
- [9] N. Vyas and R. Shah, "Intelligent and efficient cluster based secure routing scheme for wireless sensor network using genetic algorithm," *International Journal of Digital Application & Contemporary Research*, vol. 2, pp. 1–7, 2014.
- [10] D. Hortelano, T. Olivares, M. Ruiz, C. Garrido-Hidalgo, and V. López, "From sensor networks to internet of things. bluetooth low energy, a standard for this evolution," *Sensors*, vol. 17, no. 2, p. 372, 2017.
- [11] E. Fadel, V. Gungor, L. Nassef, N. Akkari, M. A. Maik, S. Almasri, and I. F. Akyildiz, "A survey on wireless sensor networks for smart grid," *Computer Communications*, vol. 71, pp. 22–33, 2015.
- [12] S. S. Iyengar and R. R. Brooks, *Distributed sensor networks: sensor networking and applications*. CRC press, 2016, vol. 1.
- [13] J. Liu, Y. Zhou, G. E. Faulkner, D. C. O'Brien, and S. Collins, "Optical receiver front end for optically powered smart dust," *International Journal of Circuit Theory and Applications*, vol. 43, no. 7, pp. 840–853, 2015.
- [14] E. M. Carapezza, D. B. Law, and C. J. Csanadi, "Darpa counter sniper program phase i acoustic systems demonstration results," in *Proc. SPIE*, vol. 2938, 1997, pp. 299–310.
- [15] Y. Liu and W. Zhang, "Static worst-case lifetime estimation of wireless sensor networks: A case study on vigilnet," *Journal of Systems Architecture*, vol. 59, no. 4, pp. 224–233, 2013.

- 
- [16] Y. Wang, Y. Zhang, J. Liu, and R. Bhandari, "Coverage, connectivity, and deployment in wireless sensor networks," in *Recent Development in Wireless Sensor and Ad-hoc Networks*. Springer, 2015, pp. 25–44.
- [17] A. Alkhatib, "Sub-network coverage method as an efficient method of wireless sensor networks for forest fire detection," in *Proceedings of the International Conference on Internet of things and Cloud Computing*. ACM, 2016, pp. 1–13.
- [18] G. Zhou, S. Tang, D. Lu, L. Liu, J. Han, and W. Dong, "Wireless sensor networks for agriculture and forestry," *International Journal of Distributed Sensor Networks*, vol. 2015, pp. 1–14, 2015.
- [19] W. Elghazel, K. Medjaher, N. Zerhouni, J. Bahi, A. Farhat, C. Guyeux, and M. Hakem, "Random forests for industrial device functioning diagnostics using wireless sensor networks," in *2015 IEEE Aerospace Conference*. IEEE, 2015, pp. 1–9.
- [20] M. Srbinovska, C. Gavrovski, V. Dimcev, A. Krkoleva, and V. Borozan, "Environmental parameters monitoring in precision agriculture using wireless sensor networks," *Journal of Cleaner Production*, vol. 88, pp. 297–307, 2015.
- [21] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of medical systems*, vol. 36, no. 1, pp. 93–101, 2012.
- [22] E. K. Choe, N. B. Lee, B. Lee, W. Pratt, and J. A. Kientz, "Understanding quantified-selfers' practices in collecting and exploring personal data," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 1143–1152.
- [23] M. Chen, Y. Zhang, Y. Li, M. M. Hassan, and A. Alamri, "Aiwac: affective interaction through wearable computing and cloud technology," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 20–27, 2015.

- [24] V. Rialle, F. Duchene, N. Noury, L. Bajolle, and J. Demongeot, “Health” smart” home: information technology for patients at home,” *Telemedicine Journal and E-Health*, vol. 8, no. 4, pp. 395–409, 2002.
- [25] P. Chahuara, A. Fleury, F. Portet, and M. Vacher, “Using markov logic network for on-line activity recognition from non-visual home automation sensors,” in *International Joint Conference on Ambient Intelligence*. Springer, 2012, pp. 177–192.
- [26] K. Baraka, M. Ghobril, S. Malek, R. Kanj, and A. Kayssi, “Low cost arduino/android-based energy-efficient home automation system with smart task scheduling,” in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on*. IEEE, 2013, pp. 296–301.
- [27] P. T. A. Quang and D.-S. Kim, “Throughput-aware routing for industrial sensor networks: Application to isa100. 11a,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 351–363, 2014.
- [28] K. Ovsthus, L. M. Kristensen *et al.*, “An industrial perspective on wireless sensor networks: a survey of requirements, protocols, and challenges,” *IEEE communications surveys & tutorials*, vol. 16, no. 3, pp. 1391–1412, 2014.
- [29] Y. Xiao, *Security in sensor networks*. CRC Press, 2016.
- [30] G. S. Oreku and T. Pazynyuk, *Security in Wireless Sensor Networks*. Springer, 2016.
- [31] D. Kotz, C. A. Gunter, S. Kumar, and J. P. Weiner, “Privacy and security in mobile health: A research agenda,” *Computer*, vol. 49, no. 6, pp. 22–30, 2016.
- [32] D. He, C. Chen, S. Chan, J. Bu, and L. T. Yang, “Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks,” *IEEE Transactions on Industrial Electronics*, vol. 60, no. 11, pp. 5348–5354, 2013.

- [33] H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 3, pp. 750–761, 2014.
- [34] M. Saud Khan and N. M. Khan, "Low complexity signed response based sybil attack detection mechanism in wireless sensor networks," *Journal of Sensors*, vol. 2016, pp. 1–9, 2016.
- [35] M. H. Yilmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th*. IEEE, 2015, pp. 812–817.
- [36] Y. M. Amin and A. T. Abdel-Hamid, "Classification and analysis of IEEE 802.15.4 PHY layer attacks," in *Selected Topics in Mobile & Wireless Networking (MoWNeT), 2016 International Conference on*. IEEE, 2016, pp. 1–8.
- [37] S. R. Ratna and R. Ravi, "Scrutiny of unruly and abuse in wireless networks to mitigate physical layer threats using discriminate based misbehavior prevention," *Cluster Computing*, vol. 19, no. 1, pp. 87–97, 2016.
- [38] S. Alsemairi and M. Younis, "Forming a cluster-mesh topology to boost base-station anonymity in wireless sensor networks," in *Wireless Communications and Networking Conference (WCNC), 2016 IEEE*. IEEE, 2016, pp. 1–6.
- [39] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.
- [40] A. Mathur and T. Newe, "Medical wsn: Defense for selective forwarding attack," in *2015 9th International Conference on Sensing Technology (ICST)*. IEEE, 2015, pp. 54–58.

- [41] S. A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," in *Space Science and Communication (IconSpace), 2013 IEEE International Conference on*. IEEE, 2013, pp. 361–365.
- [42] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.
- [43] X. Li, G. Han, A. Qian, L. Shu, and J. Rodrigues, "Detecting sybil attack based on state information in underwater wireless sensor networks," in *Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on*. IEEE, 2013, pp. 1–5.
- [44] F. Malandrino, C. Borgiattino, C. Casetti, C.-F. Chiasserini, M. Fiore, and R. Sadao, "Verification and inference of positions in vehicular networks through anonymous beaconing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2415–2428, 2014.
- [45] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in manets," *IEEE systems journal*, vol. 7, no. 2, pp. 236–248, 2013.
- [46] M. M. Patel and A. Aggarwal, "Security attacks in wireless sensor networks: A survey," in *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*. IEEE, 2013, pp. 329–333.
- [47] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.
- [48] H. Gao, R. Wu, M. Cao, and C. Zhang, "Detection and defense technology of blackhole attacks in wireless sensor network," in *International Conference on Algorithms and Architectures for Parallel Processing*. Springer, 2014, pp. 601–610.

- [49] N. M. Khan, Z. Khalid, and G. Ahmed, "Gradient cost establishment (grace) for an energy-aware routing in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–7, 2009.
- [50] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xia, "Securing dv-hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, Part A, no. 0, pp. 22 – 35, 2015.
- [51] M. Winkler, M. Street, K.-D. Tuchs, and K. Wrona, "Wireless sensor networks for military purposes," in *Autonomous Sensor Networks*, ser. Springer Series on Chemical Sensors and Biosensors, D. Filippini, Ed. Springer Berlin Heidelberg, 2013, vol. 13, pp. 365–394. [Online]. Available: [http://dx.doi.org/10.1007/5346\\_2012\\_40](http://dx.doi.org/10.1007/5346_2012_40)
- [52] D. Sun, X. Huang, Y. Liu, and H. Zhong, "Predictable energy aware routing based on dynamic game theory in wireless sensor networks," *Computers & Electrical Engineering*, vol. 39, no. 6, pp. 1601 – 1608, 2013, special Issue on Wireless Systems: Modeling, Monitoring, Transmission, Performance Evaluation and Optimization.
- [53] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.
- [54] I. Bekmezci and F. Alagaz, "Energy efficient, delay sensitive, fault tolerant wireless sensor network for military monitoring," *International Journal of Distributed Sensor Networks*, vol. 5, no. 6, pp. 729–747, 2009.
- [55] X. Xu, "Sequential anomaly detection based on temporal-difference learning: Principles, models and case studies," *Applied Soft Computing*, vol. 10, no. 3, pp. 859 – 867, 2010.
- [56] N. Aslam, W. Phillips, W. Robertson, and S. Sivakumar, "A multi-criterion optimization technique for energy efficient cluster formation in wireless sensor networks," *Information Fusion*, vol. 12, no. 3, pp. 202 – 212, 2011, special

- Issue on Information Fusion in Future Generation Communication Environments.
- [57] P. Schaffer, K. Farkas, A. Horvath, and T. B. Holczer, “Secure and reliable clustering in wireless sensor networks: A critical survey,” *Computer Networks*, vol. 56, no. 11, pp. 2726 – 2741, 2012.
- [58] J. R. Douceur, “The sybil attack,” in *International Workshop on Peer-to-Peer Systems*. Springer, 2002, pp. 251–260.
- [59] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.
- [60] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, “Lightweight sybil attack detection in manets,” *Systems Journal, IEEE*, vol. 7, no. 2, pp. 236–248, June 2013.
- [61] B. Viswanath, M. Mondal, A. Clement, P. Druschel, K. Gummadi, A. Misllove, and A. Post, “Exploring the design space of social network-based sybil defenses,” in *Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on*, Jan 2012, pp. 1–8.
- [62] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004, pp. 259–268.
- [63] F. Li, P. Mittal, M. Caesar, and N. Borisov, “Sybilcontrol: Practical sybil defense with computational puzzles,” in *Proceedings of the Seventh ACM Workshop on Scalable Trusted Computing*, ser. STC ’12. New York, NY, USA: ACM, 2012, pp. 67–78.
- [64] N. Tran, J. Li, L. Subramanian, and S. Chow, “Optimal sybil-resilient node admission control,” in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 3218–3226.



- [65] Y. Chen, J. Yang, W. Trappe, and R. Martin, “Detecting and localizing identity-based attacks in wireless and sensor networks,” *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 5, pp. 2418–2434, Jun 2010.
- [66] J. Yang and Y. Chen, “A theoretical analysis of wireless localization using rf-based fingerprint matching,” in *Parallel and Distributed Processing, 2008. IPDPS 2008. IEEE International Symposium on*, April 2008, pp. 1–6.
- [67] M. Demirbas and Y. Song, “An rssi-based scheme for sybil attack detection in wireless sensor networks,” in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, ser. WOWMOM ’06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 564–570.
- [68] D. B. Faria and D. R. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in *Proceedings of the 5th ACM Workshop on Wireless Security*, ser. WiSe ’06. New York, NY, USA: ACM, 2006, pp. 43–52.
- [69] A. Wool, “Lightweight key management for ieee 802.11 wireless lans with key refresh and host revocation,” *Wirel. Netw.*, vol. 11, no. 6, pp. 677–686, Nov. 2005.
- [70] D. Liu, P. Ning, and R. Li, “Establishing pairwise keys in distributed sensor networks,” *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 41–77, Feb. 2005.
- [71] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: Analysis & defenses,” in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, ser. IPSN ’04. New York, NY, USA: ACM, 2004, pp. 259–268. [Online]. Available: <http://doi.acm.org/10.1145/984622.984660>
- [72] M. Bohge and W. Trappe, “An authentication framework for hierarchical ad hoc sensor networks,” in *Proceedings of the 2Nd ACM Workshop on Wireless Security*, ser. WiSe ’03. New York, NY, USA: ACM, 2003, pp. 79–87.

- [73] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Lhap: a lightweight hop-by-hop authentication protocol for ad-hoc networks," in *Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on*, May 2003, pp. 749–755.
- [74] P. Bahl and V. Padmanabhan, "Radar: an in-building rf-based user location and tracking system," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, 2000, pp. 775–784.
- [75] M. Jamshidi, E. Zangeneh, M. Esnaashari, and M. R. Meybodi, "A lightweight algorithm for detecting mobile sybil nodes in mobile wireless sensor networks," *Computers & Electrical Engineering*, vol. 64, pp. 220–232, 2016.
- [76] K. N. Raja and M. M. Beno, "Secure data aggregation in wireless sensor network-fujisaki okamoto (fo) authentication scheme against sybil attack," *Journal of Medical Systems*, vol. 41, no. 7, pp. 1–6, 2017.
- [77] X. Feng, C.-y. Li, D.-x. Chen, and J. Tang, "A method for defending against multi-source sybil attacks in vanet," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, 2017.
- [78] Y. Li and R. Shi, "An intelligent solar energy-harvesting system for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, pp. 1–12, 2015.
- [79] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on*. IEEE, 2000, pp. 10–pp.
- [80] V. Loscri, G. Morabito, and S. Marano, "A two-levels hierarchy for low-energy adaptive clustering hierarchy (tl-leach)," in *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, vol. 3. IEEE, 2005, pp. 1809–1813.

- [81] A. Manjeshwar and D. P. Agrawal, "Teen: a routing protocol for enhanced efficiency in wireless sensor networks," in *null*. IEEE, 2001, p. 30189a.
- [82] S. Lindsey and C. S. Raghavendra, "Pegasis: Power-efficient gathering in sensor information systems," in *Aerospace conference proceedings, 2002. IEEE*, vol. 3. IEEE, 2002, pp. 1–7.
- [83] Y. Yao, Q. Cao, and A. V. Vasilakos, "Edal: An energy-efficient, delay-aware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 23, no. 3, pp. 810–823, 2015.
- [84] V. Rodoplu and T. H. Meng, "Minimum energy mobile wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1333–1344, Aug 1999.
- [85] J.-H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 1, 2000, pp. 22–31 vol.1.
- [86] S. Chalasani and J. M. Conrad, "A survey of energy harvesting sources for embedded systems," in *IEEE SoutheastCon 2008*, April 2008, pp. 442–447.
- [87] M. K. Jakobsen, J. Madsen, and M. R. Hansen, "Dehar: A distributed energy harvesting aware routing algorithm for ad-hoc multi-hop wireless sensor networks," in *World of Wireless Mobile and Multimedia Networks (WoW-MoM), 2010 IEEE International Symposium on a*, June 2010, pp. 1–9.
- [88] S. S. Beheshtiha, H. P. Tan, and M. Sabaei, "Opportunistic routing with adaptive harvesting-aware duty cycling in energy harvesting wsn," in *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on*, Sept 2012, pp. 90–94.

- [89] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM Workshop on Wireless Security*, ser. WiSE '02. New York, NY, USA: ACM, 2002, pp. 1–10.
- [90] D. Cerri and A. Ghioni, "Securing aodv: the a-saodv secure routing prototype," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 120–125, February 2008.
- [91] J. Zhou, "Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1–17, 2013.
- [92] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks," *IEEE communications surveys*, vol. 7, no. 4, pp. 2–28, 2005.
- [93] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, Nov 1999.
- [94] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ubiquitous computing," *Computer*, vol. 35, no. 4, pp. 22–26, Apr 2002.
- [95] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*, ser. SenSys '04. New York, NY, USA: ACM, 2004, pp. 162–175.
- [96] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.
- [97] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," in *Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, ser. SASN '04. New York, NY, USA: ACM, 2004, pp. 59–64.

- [98] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on*, April 2008, pp. 245–256.
- [99] H. W. Ferng and D. Rachmarini, "A secure routing protocol for wireless sensor networks with consideration of energy efficiency," in *2012 IEEE Network Operations and Management Symposium*, April 2012, pp. 105–112.
- [100] M. Alshowkan, K. Elleithy, and H. Alhassan, "Ls-leach: A new secure and energy efficient routing protocol for wireless sensor networks," in *Distributed Simulation and Real Time Applications (DS-RT), 2013 IEEE/ACM 17th International Symposium on*, Oct 2013, pp. 215–220.
- [101] C. Deepa and B. Latha, "Hhsrp: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks," *Cluster Computing*, vol. 20, pp. 1–17, 2017.
- [102] A. Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network," *Mobile Networks and Applications*, vol. 21, no. 2, pp. 272–285, 2016.
- [103] Y. Liu, M. Dong, K. Ota, and A. Liu, "Activetrust: secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013–2027, 2016.
- [104] C. Deepa and B. Latha, "Hhsrp: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks," *Cluster Computing*, pp. 1–17, 2017.
- [105] L. Harn, C.-F. Hsu, O. Ruan, and M.-Y. Zhang, "Novel design of secure end-to-end routing protocol in wireless sensor networks," *IEEE Sensors Journal*, vol. 16, no. 6, pp. 1779–1785, 2016.
- [106] M. Y. Rhee, *Mobile Communication Systems and Security*. Jon Wiley & Sons, 2009, vol. 1.

- [107] L. T. J. Noor Zaman and M. M. Yasin, "Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol," *Journal of Sensors*, vol. 2016, pp. 1–16, 2016.
- [108] W.-L. Chang, D. Zeng, R.-C. Chen, and S. Guo, "An artificial bee colony algorithm for data collection path planning in sparse wireless sensor networks," *International Journal of Machine Learning and Cybernetics*, vol. 6, no. 3, pp. 375–383, 2015.
- [109] E. Sisinni, A. Depari, and A. Flammini, "Design and implementation of a wireless sensor network for temperature sensing in hostile environments," *Sensors and Actuators A: Physical*, vol. 237, pp. 47–55, 2016.
- [110] N. D. Bokde, P. D. Peshwe, A. Gupta, and K. Kulat, "Remotewsn: A novel technique for remotely visualizing connectivity in wsn working on a weight based routing algorithm," in *Recent Advances in Electronics & Computer Engineering (RAECE), 2015 National Conference on*. IEEE, 2015, pp. 92–95.
- [111] V. M. Kuthadi, R. Selvaraj, and T. Marwala, "An enhanced security pattern for wireless sensor network," in *Proceedings of the Second International Conference on Computer and Communication Technologies*. Springer, 2016, pp. 61–71.
- [112] K. Hameed, M. S. Khan, I. Ahmed, Z. U. Ahmad, A. Khan, A. Haider, and N. Javaid, "A zero watermarking scheme for data integrity in wireless sensor networks," in *Network-Based Information Systems (NBIS), 2016 19th International Conference on*. IEEE, 2016, pp. 119–126.
- [113] P. N. . S. H. . P. Hamery, "Soldier detection using unattended acoustic and seismic sensors," in *Proc. SPIE 8389, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR III, 83890T*, 2012.
- [114] J. P. T. D. H. R. J. H. Vincent, "Low-cost acoustic sensors for littoral anti-submarine warfare (asw)," *SPIE 6538, Sensors, and Command, Control, Communications, and Intelligence*, 2017.

- 
- [115] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” *Ad Hoc Networks*, vol. 1, no. 23, pp. 293 – 315, 2003, sensor Network Protocols and Applications.
- [116] P. Gong, T. M. Chen, and Q. Xu, “Etarp: An energy efficient trust-aware routing protocol for wireless sensor networks,” *Journal of Sensors*, vol. 2015, 2015.
- [117] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, “Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.