



**ÇANKAYA UNIVERSITY
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES**

MASTER THESIS

**ACTIVE DEFENSE STRATEGY AGAINST JAMMING ATTACK
IN WIRELESS SENSOR NETWORKS**

Nawfal Fathi AL-SHAIKH

JANUARY 2018

**ÇANKAYA UNIVERSITY
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES**

MASTER THESIS

**ACTIVE DEFENSE STRATEGY AGAINST JAMMING ATTACK IN
WIRELESS SENSOR NETWORKS**

**A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF ÇANKAYA UNIVERSITY**

Nawfal Fathi AL-SHAIKH

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF SCIENCE IN THE DEPARTMENT OF
COMPUTER ENGINEERING**

JANUARY 2018

Title of the Thesis : **Active Defense Strategy Against Jamming
Attack in Wireless Sensor Networks**


Submitted by **Nawfal Fathi Abdulqader AL-shaikh**

Approval of the Graduate School of Natural and Applied
Sciences, Çankaya University




Prof. Dr. Can ÇOĞUN
Director

I certify that this thesis satisfies all the requirements as a thesis for
the degree of Master of Science.



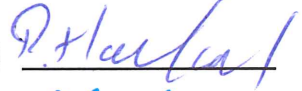
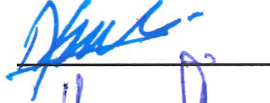
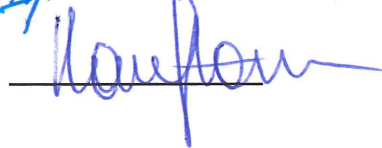
Prof. Dr. Erdoğın DOĞDU
Head of Department

This is to certify that we have read this thesis and that in our
opinion it is fully adequate, in scope and quality, as a thesis for
the degree of Master of Science.



Assoc. Prof. Dr. Reza ZARE HSSANPOUR
Supervisor

Examination Date : 12.01.2018
Examining Committee Members

Assoc. Prof. Dr. Reza ZARE HSSANPOUR (Çankaya Univ.) 
Assist. Prof. Dr. Abdül Kadir GÖRÜR (Çankaya Univ.) 
Assist. Prof. Dr. Kasim ÖZTOPRAK (Karatay Üniv.) 

STATEMENT OF NON-PLAGIARISM

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Nawfal Fathi AL-SHAIKH

Signature :

A handwritten signature in blue ink, consisting of a large, stylized loop followed by a horizontal line and a small arrowhead pointing to the right.

Date :

12.01.2018

ABSTRACT

ACTIVE DEFENSE STRATEGY AGAINST JAMMING ATTACK IN WIRELESS SENSOR NETWORKS

Nawfal Fathi AL-Shaikh

M.Sc., Department of Computer Engineering

Supervisor: Assoc. Prof. Dr. Reza Hassanpour

JANUARY 2018, 81 pages

Wireless Sensor Network WSN been utilized increasingly nowadays due to its benefits and its ability of collecting data from reachable or unreachable fields also if fields fixed or movable. Progressive developments in WSN techniques adds efficiency, reliability and better power management but it still vulnerable and sensitive to some kinds security threats. The most effective threat to WSN is DOS attacks which is detectable but unpreventable yet.

An authentication defense approach against DOS attack with additional Jamming attack that prevents transferring data between attacked node in a cluster and cluster head node is considered as a base to develop an algorithm with ability of bypassing attacked path via alternative safe one under control of cluster head to mitigate the False Node Excluding DOS due to jamming attack.

Both original and enhanced methods implemented using MATLAB and tested by comparing both results and behavior with arbitrary study case. Enhanced algorithm shows good response in mitigating FNEDOS attack.

ÖZ

KABLOSUZ SENSÖR AĞLARINDA KARIŞTIRMA SALDIRILARINA KARŞI AKTİF SAVUNMA STRATEJİSİ

Nawfal Fathi AL-Shaikh

Yüksek Lisans, Bilgisayar Mühendisliği Bölümü

Tez Danışmanı: Yrd. Doç. Dr. Reza Hassanpour

OCAK 2018, 81 sayfa

Kablosuz Sensör Ağı (WSN) yararları, erişilebilir veya erişilemeyen alanlardan ve sabit veya taşınabilen alanlardan veri toplama yeteneği sayesinde günümüzde artan bir şekilde kullanılmaktadır. WSN tekniklerindeki ilerleyen gelişmeler verimlilik, güvenilirlik ve daha iyi güç yönetimi getirmekte ancak yine de bazı güvenlik tehditlerine karşı savunmasız ve hassas kalmaktadır. WSN'ye karşı en etkili tehdit saptanabilir ancak henüz önlenemeyen DOS saldırıdır.

Küme içerisinde saldırılan düğüm ve küme başı arasında veri transferini engelleyen Karıştırma saldırıları ile birlikte DOS saldırılarına karşı kimlik doğrulama savunma yaklaşımı karıştırma saldırısı yüzünden Yanlış Düğümü Dışlama DOS saldırısını hafifletmek ve saldırılan yolu küme başının kontrolü altındaki güvenli bir yol vasıtasıyla atlama yeteneğine sahip bir algoritma geliştirmek için temel olarak düşünülmektedir.

Hem orijinal hem de geliştirilmiş yöntemler MATLAB kullanılarak uygulanmış ve rastgele seçilmiş inceleme vakaları ile hem sonuçlar hem de davranışlar karşılaştırılarak test edilmiştir. Geliştirilmiş algoritma FNEDOS saldırısını hafifletmekte iyi yanıt vermiştir.

TABLE OF CONTENTS

STATEMENT OF NON-PLAGIARISM	iii
ABSTRACT	iv
ÖZ	v
TABLE OF CONTENTS	vi
LIST OF FIGURES	ix
LIST OF TABLES	x
LIST OF ACRONYMS	xi
1. GENERAL INTRODUCTION	1
1.1 WSN Overview	1
1.2 Previous work	2
1.3 Motivation.....	3
1.4 Thesis Contribution.....	3
1.5 Thesis Structure.....	4
2. WSN AND CHALLENGES	6
2.1 What is WSN	6
2.2 WSN Applications	8
2.2.1 Military Applications	8
2.2.2 Environmental Applications.....	9
2.2.3 Health Care Applications	9
2.2.4 Home Intelligence Applications.....	9
2.2.5 Industrial Applications	9
2.2.6 Agriculture Applications	9
2.2.7 Structural Monitoring Application	10
2.3 Factors Affects WSN QoS	10
2.3.1 Power Management.....	10
2.3.2 Memory Used	11
2.4 WSN Challenges	12
2.4.1 Deployment	12
2.4.2 Reliability	13
2.4.3 Routing & Monitoring.....	13
2.4.4 Programmability	13
2.4.5 Power Supplying	13

2.4.6	WSN Security	14
3.	WSN SECURITY AND ATTACKS	15
3.1	Security Goals	15
3.1.1	Availability	16
3.1.2	Integrity	16
3.1.3	Confidentially	16
3.1.4	Freshness	16
3.1.5	Authentication	17
3.1.6	Access Control	17
3.1.7	Non-Repudiation	17
3.2	Constrains of WSN Security	17
3.2.1	Limited Resources	17
3.2.2	Communication Unreliability	18
3.3	Attacks in WSN	19
3.3.1	Passive Attacks	19
3.3.2	Active Attacks	20
3.4	Attacks Due to WSN OSI	22
3.4.1	Physical Layer	22
3.4.2	Data Link Layer.....	22
3.4.3	Network and Routing Layer	23
3.4.4	Transport Layer	23
4.	LITERATURE REVIEW	24
4.1	Introduction	24
4.2	Clustering and Energy Balancing Category	24
4.3	Frameworks and Schemes Category	27
4.4	Measurements and Analysis Category	30
4.5	Authentication Approach Category	34
5.	OREGIONAL AND PROPOSED METHODS	38
5.1	Introduction	38
5.2	Original FEDOS Defense Method	39
5.2.1	Initialization Phase	39
5.2.2	Report Generating Phase	39
5.2.3	Considering of Jamming Attack.....	40
5.2.4	Original Method Analysis	41
5.3	Proposed False-Exclusion Mitigation	41
5.3.1	Assumptions for Proposed Method	42
5.3.2	Structure of Proposed Model.....	42
5.3.3	Proposed Enhancement	43
5.3.4	Analysis of Enhanced Method	46
5.4	Algorithm Notation	47
5.4.1	Algorithm for Cluster Head CH	47

5.4.2	Algorithm for Query_Endorsement Function	48
6.	ORIGINAL AND ENHANSED ALGORITHMS	
	IMPLEMENTATION (RUNNING AND TESTING).....	49
6.1	Introduction.....	49
6.2	Simulation Environment	49
6.3	WSN configuration	49
6.4	Running Algorithms.....	50
6.4.1	Original Method Without Jamming Attack.....	51
6.4.2	Original Method With Jamming Attack.....	52
6.4.3	Original Method Second Endorsement	53
6.4.4	Running Enhanced Method.....	54
6.5	Test Case Scenarios	59
6.5.1	Scenario (1)	60
6.5.2	Scenario (2)	61
6.5.3	Scenario (3)	63
6.5.4	Scenario (4)	64
6.5.5	Scenario (5)	65
6.5.6	Scenario (6)	70
7.	CONCLUSION AND FUTURE WORK	70
7.1	Conclusion	70
7.2	Future Work.....	71
	RESOURCES	72

LIST OF FIGURES

Figure 2.1.	Simple block diagram for WSN node.....	7
Figure 4.1.	Shows the clustered WSN.....	25
Figure 4.2.	Architecture for detecting and defending system	28
Figure 4.3.	Shows the proposed defense scheme	29
Figure 4.4.	DoS attack by neighboring node in S-MAC	31
Figure 4.5.	Tree structure of cluster-based WSN.....	33
Figure 5.1.	Shows False Endorsement DOS attack FEDOS	38
Figure 5.2.	Shows Jamming attack model.....	40
Figure 5.3.	Shows the structure of a cluster	42
Figure 5.4.	a) Nodes distribution, b) Distance table to node CN, c) Sorted Distance table to node CN	43
Figure 5.5.	Shows case of first neighbor node failed	45
Figure 6.1.	a,b shows randomly distribution of nodes	50
Figure 6.2.	Scenario (1), shows 100 nodes and 5% attacked	60
Figure 6.3.	Scenario (1), shows 500 nodes and 10% attacked	61
Figure 6.4.	Scenario (2) attacked nodes, Jamming attack	62
Figure 6.5.	Scenario (3) Jamming attack and enhanced algorithm	63
Figure 6.6.	Scenario (4) Jamming attack and doubtful neighbors for enhanced algorithm.....	64
Figure 6.7.	Scenario (5) Jamming attack and doubtful neighbors for enhanced algorithm.....	66
Figure 6.8.	Scenario (6) Jamming attack and regionally attacked nodes.....	71

LIST OF TABLES

Table 3.1. Contains WSN OSI layers with their related attacks and defense solution.....	23
Table 6.1. Authentication failure due to jamming attack.....	53
Table 6.2. Correct authentication after jamming attack.....	53
Table 6.3. Second endorsement authentication failure due to jamming attack.....	54
Table 6.4. Shows nodes location.....	55
Table 6.5. Shows other nodes distance to attacked node.....	56
Table 6.6. Sorted distances to attacked node.....	57
Table 6.7. Sorted nodes left to communicate with attacked node.....	57

LIST OF ACRONYMS

AML	: Abnormal Message List
CH	: Cluster head
CN	: Cluster node
CTMC	: Continuous Time Markovian Chains
CTS	: Clear to Send
DOS	: Denial Of Service
Ed	: Event Detection
FEDoS	: False-Endorsement-Based Denial of Service
FNEDoS	: False Node Exclusion Denial of Service
FFUCA	: Fast and Flexible Unsupervised Clustering Algorithm
GW	: Gateway
H²BSAP	: Hop-by-Hop Broadcast Source Authentication Protocol
HAS	: Home Automation Systems
HEED	: Hybrid Energy-Efficient Distributed
LEACH	: Low-energy Adaptive Clustering Hierarchy
MAC	: Message authentication code
MLCG	: Multiplicative Linear- Congruential Generators
MoM	: Message Observation Mechanism
NML	: Normal Message List
PDOS	: Path-based Denial of Service
QoS	: Quality of Service
RHS	: Remote Home Server
RTS	: Request to Send
S-MAC	: Sensor-Medium Access Control
SPE	: Special Process Estimation
TID	: Temporary ID
VH	: Virtual Home
WSN	: Wireless Sensor Network

CHAPTER I

GENERAL INTRODUCTION

1.1 WSN Overview

Wireless Sensor Networks (WSN) worth's a higher interest nowadays due to the increasingly needs to monitoring, observing and gathering data for making decisions related to monitored field. The structure of WSN generally consists of clustered sensor nodes, cluster head and base station node (it named also as Sink node). WSN's widely differs from each to other depending on what application used for and what field designed to deployed in. WSN used with military purposes, environmental monitoring, industrial applications, agricultural applications, health care and medical applications, vehicle tracking and many other applications [6, 7]. WSN applications can classified mainly in to two categories Event Detection (ED) and Special Process Estimation (SPE) [5].

Due to widely utilizing of WSN, it faces several challenges that affects its efficiency and its duty life time. These challenges like deployment, Reliability, Routing and Monitoring, Programmability, Power supplying and Security [8]. Security is the most significant challenge due to its relation with securing collected and traveled data between nodes. So, data protection against outsider and insider adversaries or attacks is the most significant issue among other issues. The most dangerous and unpreventable attack is Denial Of Service DOS attack due to its ability to utilizing different forms and techniques to suspend functionality of effective nodes. In this thesis, a method developed to defense WSN against certain type of DOS attacks that is Jamming attack and mitigating its effect even it still attacking communication channels between nodes and cluster head.

1.2 Previous work

To study DOS attack forms and techniques, a set of research papers which involved with this kind of attacks been studied. It is best way to study different kinds of attack and their countermeasure strategies, is to categorize them according to their approach while defending WSN against DOS attacks.

The categories were Clustering and Energy balancing category, the main idea of this category about creation and distribution of Control Nodes Cnodes which takes the responsibility of monitoring node's behavior and power characteristics to keep WSN functioning and power balanced.

Another category is Frameworks and Schemes category, in this category, schemes and novel methods for detecting and defending DOS attacks. These method based on arranging well known DOS detecting and defending algorithms into such structures to provide high efficiency detection and defending.

In addition, Measurements and Analysis category, the popups of WSN is to collect data for its field whether it reachable or not, friendly area or hostile one. The significant issue is achieve highest efficiency within duty time. Therefore WSN designers and whom in concern of countermeasures of attacks, have to know information about the normal behavior for WSN and its behavior under attacks especially when talking about DOS attack where detecting it is not an easy job. For that reason, measurements and analysis is very important.

Last category is Authentication approach category where it is an important approach for security in WSN. Data collected from a certain field especially for hostile ones, should be protected from attackers whom try capturing a significant information, disturb transmitted data, changing transmitted data, etc. So authentication aim to make authenticated data available for only authorized users especially for sensitive applications like military, health care or environment control.

1.3 Motivation

DOS attack aim to disturbs either nodes or data transmission channels to prevent nodes from providing services or communication to each other. One type of these DOS attacks is Jamming attack. The original research paper [22] which is related to last category of authentication approach, presents a Grey-List method as an authentication defense against False Endorsement DOS attack. In this method, cluster head CH generate a report about occurrence of certain phenomenon and broadcast it to all corresponding cluster nodes to give their endorsement of generated report contents. Cluster nodes CN's check phenomenon time stamp and occurrence of phenomenon itself. If verification process passes, endorsement generated and forwarded to CH which authenticates endorsing node. Endorsement accepted unless an error occurred with endorsement message, in such a case, node grey-listed and CH waits till CN resend message as a proof for its last endorsement with the new one then CN be trusted again. If proof message delayed or prevented, CH excludes CN from further endorsement while CN still functioning correctly. Delay and prevention is due to Jamming attack.

As seen, excluding functioning nodes after one iteration of resending proof for last endorsement costs WSN to lose innocent nodes. In addition, original method did not provides alternatives to defense this pitfall especially when jamming attack acting for long time. Another problem available, the attacked node didn't informed that its endorsement was dropped. Therefore a countermeasure developed to overcome mentioned problems with original method.

1.4 Thesis Contribution

Instead of excluding innocent node as mentioned previously in (1.3), an alternative developed method that cluster head follows to deliver attacked node's proof endorsement. First, CH collect all nodes deployment locations. In next step, CH calculates distance for each node in the cluster to other nodes then sort them in ascending manner.

CH has an information also about other nodes with other kind of problems. So, CH treat them as untrusted nodes for delivery process. Therefore, CH send an endorsement request to attacked node via nearest safe neighbor selected from sorted distance table. Neighbor node forwards the request to attacked node. Attacked node, responds by sending its proof for last endorsement to its neighbor which in turn, replay it back to CN.

As a result, if authentication passed, attacked node will removed from Grey-list and added to trusted list for further endorsement processes. If node authenticated but received message itself is incorrect, then double attack detected and node added to doubtful node list. If jamming attack still acting also for first neighbor, CH picks the predecessor neighbor and repeat the whole process via different path till first correct authentication occurred. The enhanced method solves all problems mentioned in previous paragraph. So, False Node Exclusion DOS mitigated.

1.5 Thesis Structure

This thesis is organized in seven chapters as follows:

Chapter II, provides an overview for Wireless Sensor Network WSN, relation between nodes, WSN applications and challenges that WSN normally face them.

Chapter III, presents information about security importance, attacks that affect WSN efficiency, also provides an information about DOS attack and its effect on WSN.

Chapter IV, gives an explanation for previously research papers which related to DOS attack. These researches categorized due to approach followed to countermeasure the effect of different kinds of DOS attacks.

Chapter V, provides a detailed explanation for original method for defending FEDOS and its limited countermeasure against Jamming attack. Also provides a

detailed explanation for enhanced method that manipulates original method limitation.

Chapter VI, shows the implementation for both original and enhanced method using MATLAB and their results. Selecting an example as a study case to show the response of both methods. Comparing their results to show enhanced method success.

Chapter VII, provides analysis for results obtained in chapter 6 and what additional enhancement can added as future work to improve the overall resultant method.



CHAPTER II

WSN AND CHALLENGES

The field of Wireless Sensor Networks has an increasingly interest in last decade due to highly improvement in scientific and technological fields. The progressing in wireless communications leads to an efficient and easy way for sharing data and information between wireless devices from one side and between wireless devices and wired devices (i.e. Internet) through gateways from another side. In addition, sensing technologies makes discovering the ambient and collecting a valuable information from it easier and more reliable like measuring simple factors as temperature or sensitive and complex factors as military issues.

The progressing in sensing technology is tightly connected to the improvement of manufacturing and infrastructure technologies. For example the improvement of semiconductor technology, power supply devices (Batteries) and hardware memories leads to produce a more efficient, smaller and intelligent sensors with a high capability of intermediate communication and data storing for long duty time. These sensors has the ability to work as network group which covers the whole monitored field.

2.1 What is WSN

Wireless Sensor Networks WSN is an important technology has the ability of collecting information covering deferent fields [3]. WSN defined as "*The ensemble of spatially distributed, autonomous sensors that cooperate to monitor physical or environmental quantities of interest as temperature, sound, vibration, pressure, pollutants, etc...*" [4]. WSN uses particularly two communication standards (Wireless HART and ISA100.11a) [4]. Each sensor in WSN represents a node which

designed for monitoring its environment and controlling as response for simple calculations. In WSN each node usually consist of several parts which they are Sensor which sense the ambient and transforms the physical quantities into electric signals. Secondly, a simple Microcontroller which provides a simple computational processes, small amount of storage and conversion of analogue signals in to digital form. Also anode has a Radio transceiver part for wireless communicating with other nodes in same network. It also has a local power source almost be a small battery, in some cases the node has a power harvester that converts external physical quantities (solar, thermal, etc..) into useful energy for node as power supply [4]. Figure (1) below shows as simple block diagram for WSN node as explained previously

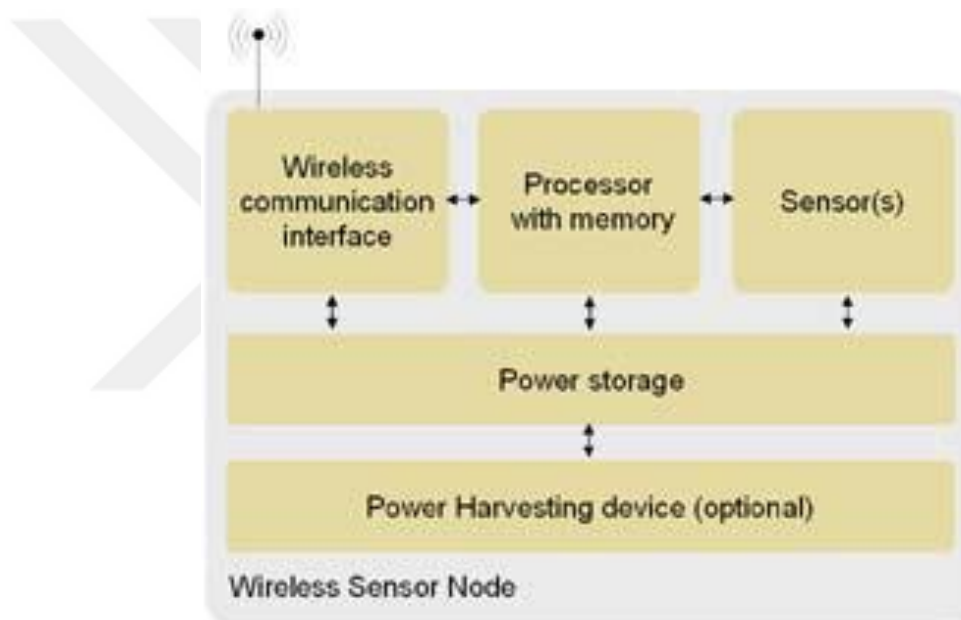


Figure 2.1. Simple block diagram for WSN node

WSN has its limitations due to huge amount of data been collected which needs a high computational processes in order to analyze and manage them. In addition, the power consumption for long time causes getting nodes out of service which is a big problem especially for far allocated WSN's, but the most critical limitation is the long distance connectivity where WSN's data cannot be shared for whom concern in computing, analyzing those data or even decision makers [1],[3],[4].

2.2 WSN Applications

WSN applications have a lot of fields of usage as much as sensing needed for different purposes. WSN applications can be classified mainly into two categories: Event Detection (ED) and Special Process Estimation (SPE) [5]. In the ED category, the data collected by WSN will be deployed depending on events. For example, if a WSN worked within a forest monitoring field, in a normal situation no data deployment is needed, but in the case of a fire occurring as an event, the data deployment starts accordingly.

On the other side, the SPE category means that WSN monitors specific phenomena like temperature variation. In this case, the aim of WSN is to take readings at specific time intervals and process them to estimate the behavior of that monitored value over a long time. In SPE, the processing activity is done either in a distributed intelligent sensor (Nodes) or data is deployed to a centralized node that takes responsibility of processing and estimation [5].

In addition, some WSN applications use both of the two categories, ED and SPE. For example, in environmental monitoring, if a WSN worked in forest fire monitoring, the event of detecting a fire belongs to ED, but on the other hand, monitoring the temperature and estimation of temperature behavior belongs to SPE [5,6].

WSN can also be classified according to the nature of the field that it monitors, as illustrated below.

2.2.1 Military Applications

WSN for military purposes can be integrated as "*military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) systems*" [6,7]. It is not for monitoring only hostile forces but also friendly forces and their activities.

2.2.2 Environmental Applications

They are the applications that deals with tracking small animals, bird and insects to monitor their live behavior or monitoring water resources, fire detection, chemical pollution study, weather monitoring and more [6,7].

2.2.3 Health Care Applications

These applications uses WSN to track or observe patients health situation an and alert them or their doctors about blood pressure, blood sugar level or any significant issue. The sensors may been worn on the patient's body or been deployed around patients to be observed [6,7] especially when health care WSN connected to internet.

2.2.4 Home Intelligence Applications

It used for providing an intelligent environment for houses. WSN can monitor a lot of house utilities like gas, water, electrical devices and the most important thing which is house security by using motion detection systems or monitoring doors and windows and gives alerts to whom it may concern through wireless connections [6,7].

2.2.5 Industrial Applications

In last years, artificial intelligence toke a wide range in industry so, the WSN and sensors are the most significant part in modern production lines like monitoring objects, counting them or monitoring chemical process in related productions and alerts in case of accidents or when products don't matches the desired quality [6,7].

2.2.6 Agriculture Applications

WSN is increasingly used in agriculture in last years because it provides a controllable environment for agriculture. The most important features that monitored

to be controlled are temperature, air humidity and the irrigation systems. WSN and wireless controllable I/O devices helps farmers to increase their fields and control them remotely and efficiently also it reduces the waist of water resources [6,7].

2.2.7 Structural Monitoring Application

WSN also useful in monitoring cities infrastructure like buildings, bridges, flyovers, roads, high ways, tunnels, air ports, .etc.[7].

2.3 Factors Affects WSN QoS

The important of WSN came from its ability of sensing the targeted field or environment and transferring collected date in a wireless manner. So accordingly, *Quality of Service (QoS)* must ensure in order to get a correct readings with accurate management and calculations. To ensure the desired QoS, there are several factors must be discussed when deploying or installing a WSN in a certain field as follows.

2.3.1 Power Management

In modern WSN applications it is required to install or deploy a long duty time sensors. It is obviously that duty life of sensors depends on the field environment especially with unreachable fields like volcanos. But the most significant issue is the power consuming of these sensors which affected by some parameters.

2.3.1.1 Number of sensor entries like temperature, air humidity, light,.....etc. where power consumption will increased accordingly.

2.3.1.2 Number of provided services like signal conditioning and data manipulation.

2.3.1.3 Wireless transmission duration which affects power dissipation.

2.3.1.4 The ambient nature where the WSN deployed.

2.3.1.5 The desired readings precision, whereas high accuracy needed as much power consumption occurs.

2.3.1.6 The RADIO frequencies used for transmitting and receiving data.

In old types of sensors an AA batteries used as a power supply which need to replace it manually but with unreachable environments and the WSN area of deployment with large number of sensors, these type been useless and there is a need for smaller, longer life batteries and lower power consuming. It also needed to find new clean power supplying strategies like solar cells for an example.

2.3.2 Memory Used

The memory used in WSN also an important factor that affects the quality of service because the small size of memory as in old types of sensors leads to a small size of collected data to be analyzed and that in turn leads to increasing of number of transmission operations. On the other side, now days the modern sensors follows the improvement in manufacturing technologies. As a result, modern sensors have a smaller physical size of memory chips, larger capacity and faster saving/retrieving data.

2.3.2.1 Ability of DATA Manipulation

Embedded controllers in WSN sensors take an important place in analyze and manipulate collected data either by the sensor itself or by a centralized node. Also controller responsible of encrypting data to send to the next hope (node). This operation needs controlling transmitting data via suitable RADIO frequencies. In addition, it has the responsibility of gathering that collected locally and received ones from previous hopes without any data collision.

2.3.2.2 Ability of Communication

Radio communication is the most important part in sensors due to wireless communication between themselves and between them and centralized node. It is also the most power consuming part where it takes 90% to 95% of total power dissipation. This dissipation is done due to either direct use of RADIO transmission or due to wasted time waiting for data manipulation to be sent. WSN uses some transmission standards like Bluetooth or ZigBee which is faster and lower power consuming. ZigBee technology permits 254 devices to be communicate simultaneously with radio frequency of 2.4 MHz.

2.4 WSN Challenges

The increasingly integration of modern and intelligent technologies with the WSN's that consists of cheaper and smaller sensors leads to produce a more efficient WSN's that have the ability of monitoring a wider range of parameters in monitored environment. Due to the nature of these low cost sensors, the WSN's faces a lot of challenges. In below illustration for some of these challenges.

2.4.1 Deployment

The first step in installing WSN's is deploying sensors in monitored field depending on the purpose behind it in other words, for what application these sensors deployed for. The deployment process affected by the nature of the field being monitored. Some of fields are reachable so, the deployment can be done by hand or by robots. But on the other hand, some of them unreachable therefore the deployment done by helicopters. Although it is more expensive way but it is an effective one. Since the WSN's are designed to be self-organized system, sensors should organize themselves after deployment and actually that is a challenge [8].

2.4.2 Reliability

There are several things in WSN's that appears as a challenge, one of them is reliability. It appears due to the transmission or receiving data failure or data collision caused by sensor failure, used frequency interference. In addition, the nature of transferred data whether it is continues packets or transmitted with successive short intervals. If the data has a sensitive nature as in military applications, the reliability is a challenge also [8].

2.4.3 Routing & Monitoring

The challenges that faces the WSN's due to routing and monitoring come from two reasons one of them due to limitations of sensors themselves like power source and sensor hardware design. The other one due to the increasingly needs for using them by some types of applications. Therefore it is a challenging issue especially in case of unexpected events. Moreover, routing protocols that deals with movable targets to be monitored, also presents a an additive challenging with finding suitable track between successive hopes or nodes and keeping the connections in stable manner [8].

2.4.4 Programmability

It is another challenging issue that let the programmers modifies the internal programs that describes the behavior of the node or sensor while they are in duty time. Like updating working protocols [8].

2.4.5 Power Supplying

The limitations of WSN's from side view of computational capabilities, data processing, memory storage and communication provides a challenge that can be improved and reduced with increasingly improvement of manufacturing technology.

But the most challenging parameter is the power consumption. Power source or batteries is slower progressing than other technologies. So, the challenging point is to find or produce a very long life batteries which have the ability of self-recharging from one side. On the other side, finding a power saving protocols for routing, self-organizing and transmission management are another challenging parameter [9,10].

2.4.6 WSN Security

Unlike traditional networks, WSN's are deployed in an open environment and wide area fields. This situation makes WSN's vulnerable to direct outside attacks or damage because of environmental parameters. In other words WSN's faces a security challenges due to both risks previously mentioned. For environmental challenges, it can be discussed as a manufacturing technology issues that affects the stability of sensor hardware. On the other hand, security issues related to data are separated into two categories. Firstly, security issues due to data compression and encoding that affected by what security algorithms installed on sensors. Secondly, security issues related to communication channels and how much it is secure against outside attacks whether it is direct human attacks or remotely by intersecting the data transmission channels [7,8,9].

CHAPTER III

WSN SECURITY AND ATTACKS

Among the most important challenges in WSN (Wireless Sensor Network) like sensors deployment, scalability, energy efficiency, computational power and QoS (Quality of Service), the security of WSN represents the most significant one. Like traditional networks (or wired one), WSN has a similar kind of security threats but it also has an extra kinds of security challenges due to the wireless nature of WSN connectivity. Wireless broadcasting of collected data lets adversaries to intercept the transmission frequencies illegally and remotely. Moreover, the deployment of sensors in wide area open lands also gives the ability for attackers to interact the sensors itself directly to take codes, ciphering keys, passwords and more things.

For that reasons securing the WSN's against adversaries especially with sensitive applications like medical or military ones. Therefore a lot of techniques proposed to mitigate the impact of attacking WSN fields. This can be done by improving security algorithms depending on the knowledge about each kind of attacks.

3.1 Security Goals

Security is a wide range concept, it has a different meaning according to the variety of what field the security involved with like military, health care, agriculture and etc.

In overall, security when it is needed in any field, there are several goals have to be achieved so the security itself achieved too. In below an illustration of these goals [12,13,15,16,17].

3.1.1 Availability

As mentioned before, WSN normally deployed in either friendly or adversary ambient so in both cases it is needed to keep the WSN services and collected data available for authorized sink nodes. In other words, keeping WSN safe from denial of service attack DOS [12,13].

3.1.2 Integrity

in WSN's data travels wirelessly from node to another one till reaches the sink node or head of cluster node. So it is very important for receiving node or next hop node to receive the data as transmitted form by sender node. Integrity protects transmitted data from any malicious modification through transmission process [12,13].

3.1.3 Confidentially

Traveling data between nodes must be understood and available for only concerned nodes. In other words, it must be guaranteed that transmitted data are hidden from adversary nodes [12,13].

3.1.4 Freshness

The main purpose of WSN is to collect data and transmit it to main station. In addition timing is also significant issue especially in sensitive applications like military or health care. In such a case, malicious adversaries cause a reply delay time. Therefore data freshness is needed as a security goal [12,13].

3.1.5 Authentication

Another goal of security in WSN is to prevent adversaries from injecting an additional illegal messages via legal WSN transmission channels. The receiver node must make sure that received data came from correct and authenticated node [12,13].

3.1.6 Access Control

Participant nodes within same WSN must have the ability of discovering and detecting adversary nodes among them. Accordingly, messages that belongs to foreign WSN's must be detected too [12,13].

3.1.7 Non-Repudiation

Also WSN nodes must prevented from neglect transmitting any received message to the next hop [12,13].

3.2 Constrains of WSN Security

Due to sensor nodes small size structure which has limitations in processing capabilities, storage, transmission bandwidth and energy resources, a related security limitation also available. So, WSN security affected by nodes computational capabilities and intermediate communications within same WSN. Security constrains can be classified into categories as illustrated below [13].

3.2.1 Limited Resources

Wireless sensor nodes designed and constructed to satisfied the variety of different environment natures. Accordingly they must be small size, self-organized, environmental factors resistant, computational capabilities, long life energy source

and RADIO communication. But due to their tiny sizes, they suffered from several resource limitations as illustrated below [13].

(i) . *Memory and storage limitation*

As mentioned previously, nodes implemented with small size. Accordingly the internal hardware are small size too. So, small memory and storage leads to memorize a short length of security management program codes which affects the quality of security services. In addition, small storage affects the efficiency of node computational power which extremely needed in encoding/decoding and ciphering/deciphering [13].

(ii) . *Power energy limitation*

Energy is the most significant factor in designing wireless sensors because it affects the working life of the node itself. In addition, internal transducers, microprocessor and RADIO communication hardware causes an exhaustive power consumption. For security field, also energy is significant due to power consumption for applying encryption and ciphering algorithms. Nowadays a rechargeable sensors available or those which uses the clean resources like solar cells that applicable in friendly and reachable environment which makes life easier but on the opposite side with adversary ambient, energy source is a real challenge.

3.2.2 Communication Unreliability

Since wireless sensors collects data from their fields and transmit it by means of wireless communication techniques like WiFi or 2G/3G services which are limited range or using satellite communication channels. In both cases, network throughput is the measurement point. Also security affects the throughput. Communication unreliability due to following categories [13].

(i) . *Unreliable data transfer*

Loosing data packets or damage them in WSN's is possible due to the huge number of sensors deployed in a certain field that tries to transfer data to each other. Another reason, the connectionless nature of WSN sensors with rapidly changeable collected data causes missing transfer some data packets. Encryption keys which is a security issue, also transferred as packets and may get dropped or lost while transmission.

(ii) . *Data transmission conflicts*

Due to congestion of nodes where they need to establish connection between them, data confliction may occur while transmitting data packets. When sensitive data especially when they are related to security conflicts, an important data will damaged or lost.

(iii) . *Synchronization issue*

Some nodes among WSN where in sleep state (Off node) can wake up because of receiving a broad casted data packets. This converts the OFF node into active state and start broad casting. Other already active nodes must synchronized immediately in order to receive new packets. Therefor synchronization is critical issue in WSN.

3.3 Attacks in WSN

WSN's faces a different types of attacks due to the variety of purposes behind attacking WSN's. So, WSN attacks classified into categories as illustrated below.

3.3.1 Passive Attacks

Some of attacks are limited in listening to transmission channels in order to analyze transmitted data and extract useful information for adversaries like knowing

which node is the head of sector. These kind of attacks are so difficult to detect because there are no activity or modification applied on original transmitted data. These kind of attacks usually occurred before starting the second category of attack which are active ones [12,13,16,17].

3.3.2 Active Attacks

In this category of attacks, the aim of attackers is to remove transmitted data, modify them, inject fake information, replying an old information, trying to mimic legal nodes and causing a denial of service in a certain WSN. In below illustration for most significant active attacks [12,13,15,16,17].

(i) . *Tampering*

WSN's that deployed in a reachable fields suffers from this kind of attacks where attackers access the nodes physically in order to get critical information like encryption keys or algorithms.

(ii) . *Black hole*

In this kind of attack, an adversary node broadcast a fake routing information to make other legal nodes changing the data traffic through the attacking node. This node acts as black hole that sinking all WSN information.

(iii) . *Selective forwarding*

Information in WSN travels from one node to another successively. Adversary nodes that enroll themselves as legal ones, simply block or drop certain packets instead of forwarding them.

(iv) . *Sybil attack*

In this attack, attacker node try to represents itself illegally with different legal ID's among certain WSN. The main purpose of this attack is to disturbing the

localization identification algorithms. Because normal nodes identify their location with respect to nearby legal ones.

(v) . *HELLO flood attack*

WSN's have the nature of self-organizing. So after sensors deployment nodes tries to discover their neighboring nodes by broadcasting a "HELLO" message and receive the neighboring acknowledgments to identify themselves to each other. An attacker may flood the network HELLO message to keep other nodes busy in responding.

(vi) . *Jamming attack*

It is an attack when an attacker disturbs the RADIO transmission channels by using same frequencies for broadcasting a useless information and jamming the channel.

(vii) . *Blackmail attack*

It is an attack when an adversary node declares another set of nodes as a malicious ones. If this happened and legal nodes been blocked and make then out of service. Such a case affects the overall performance of WSN.

(viii) . *Exhaustion attack*

This attack happened when an adversary node passes unnecessary in formation to other nodes. The main idea is to exhausting legal nodes energy with receiving useless information and making a large amount of unnecessary calculations.

(ix) . *Wormhole attack*

In this kind of attacks, adversary nodes placed at the ends of WSN area. They can receive or transmit information by parts by means of tunnels. Detecting this

attack is very difficult because it uses a combination of Selective forwarding and Sybil attacks.

(x) . Identity replication attack

Adversary nodes in this kind of attacks, clone another legal node and act as a part of WSN to collect an important traveled information. Unlike Sybil attack, legal node and malicious one sharing the same ID.

3.4 Attacks Due to WSN OSI

As in wired network, communication protocols between WSN nodes depends on the infrastructure which manages the whole activities in WSN's. Security also a significant issue that WSN protocol model should deal with. Unlike TCP/IP OSI model which consist of seven layers, WSN OSI standardization (Opining System Interconnect) [2] is responsible of communication, routing, error detection and correction and data manipulation processes. WSN OSI layers are explained in below with bottom to up manner [12,13,15].

3.4.1 Physical Layer

It is the first layer that is responsible for selection and generation of carrier frequency, signal detection, modulation and demodulation and data encryption.

3.4.2 Data Link Layer

This the second layer where it responsible for multiplexing of data stream which received from previous nodes to be sent to next hop, data frame detection, error control and point-to-point / point-to-multipoint communication.

3.4.3 Network and Routing Layer

The third layer is responsible for “node to node, node to sink, node to base station and node to cluster head & vice versa.”. Because of broadcast nature of WSN nodes, each node acts as a router.

3.4.4 Transport Layer

It is responsible for managing an end-to-end connection.

In TCP/IP based networks, each OSI layer has it's related attacks. As well as for WSN OSI layers, they also have a corresponding attacks as shown in the table below.

Table 3.1. Contains WSN OSI layers with their related attacks and defense solution

<i>Layers</i>	<i>Attack types</i>	<i>Defense</i>
Transport Layer	Flooding De-synchronization False message injected	Client puzzles, Rate limitation authentication
Network and Routing Layer	Black holes Hello Flood Sinkholes Sybil Information & selective forwarding Wormhole	Authentication, Monitoring, Redundancy verification, packet leases by using geographic and temporal information. Redundancy Authorization, monitoring Egress Filtering and authentication
Data Link Layer	Jamming & Collision, Exhaustion, Unfairness	Error correcting Rate-limit Small frames
Physical Layer	Jamming Tempering	Speed Spectrum, Priority Messages Temper –proofing, hiding

CHAPTER IV

LITERATURE REVIEW

4.1 Introduction

Most of an important attacks in WSN, is the Denial Of Service Attack (DOS). The significance of this attack came from its resistance to be detected. Therefore, a lot of efforts spent in this field to achieve a high detection efficiency. In this thesis, selected papers which concern in DOS detection and prevention separated into categories due to its similarity in their DOS detection approach. The mentioned categories are illustrated in below.

4.2 Clustering and Energy Balancing Category

The main idea of this category about creation and distribution of another kind of nodes included within cluster nodes which is Control Nodes Cnodes. Cnodes take the responsibility of monitoring the data traffic to detect malicious nodes. Electing of Cnodes algorithms has been discussed depending on random-based election, energy balancing-based election and distance from nodes to be observed. Taken in consideration the periodically timing of election and re-election against the timing of CH election. In below a figure shows the structure of WSN clustering.

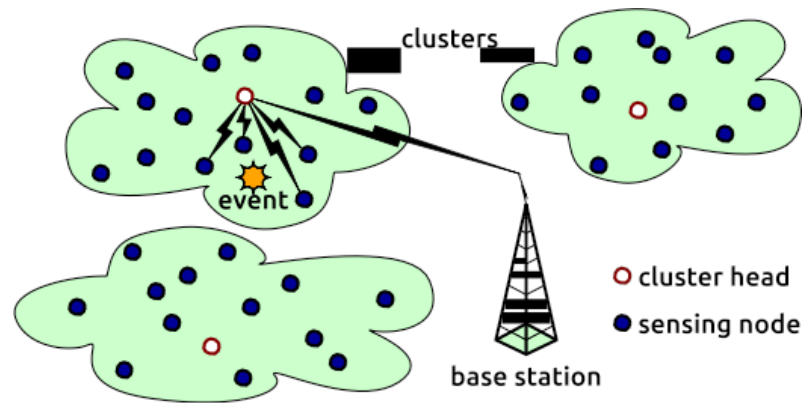


Figure 4.1. Shows the clustered WSN

In [25], authors focused on high rating detection of DOS attacks mechanisms also provides at same time a good energy-preserving solution. They considered the hierarchical topology clustering algorithms such as Low-energy Adaptive Clustering Hierarchy (LEACH) or Hybrid Energy-Efficient Distributed clustering (HEED). The detection of compromised nodes depending electing suitable cNode set which responsible for monitoring data traffic in WSN. There are three methods for election: Distributed Self-election, Cluster head-centralized election and finally the Base station-centralized election. Authors proposed a dynamic Cnode Re-elected periodically to ensure that each non-CH node has the chance to be elected which provide a good power balancing and good detecting rate under a condition of Cnode re-election period must be shorter than re-election of CH period. Two models for DOS detecting were discussed, first: the Continuous Time Markovian Chains (CTMC) which is a model for obtaining the probability for Cnode to detect DOS attacks in terms of steady-state distribution. Due to randomization of electing Cnodes, the probability result is approximated, therefore, Non-Marvovian modeling for DOS detecting is more accurate.

In [30] and [41], Authors in this paper used LEACH clustering algorithm to establish a hierarchical topology of WSN's. LEACH executed for multiple iterations to split the first level of clusters into sub clusters and so on. Node energy added to electing formula of cluster head in level-1 where the highest power were selected. Higher levels sub clusters constructed with sub CH (considered as Cnode for corresponding cluster), with number of nodes more than 2 sensor nodes. The

LEACH iterations keep generating sub of sub clusters till conditions satisfied. Cnodes generated finally, will elected to which CH belongs to depending on shortest distance. Therefore the control nodes will uniformly distributed in comparison with randomness. This achieves a higher efficiency of traffic monitoring and better DOS attack detecting. Also by considering distance. Authors claimed that less power will be consumed with their approach. But on the other hand the increasing number of Cnodes causes higher power dissipation, the issue which not discussed or mentioned. Another problem is that LEACH algorithm gives the right to nodes to self-selection whether it is Cnode or not. This issue causes un-uniform distribution of Cnodes within single cluster.

In [42], LEACH also used to achieve recursive clustering of WSN exactly as mentioned in [30] and [41] therefore same results been came out. authors improved the recursively-clustering technique by using a novel clustering algorithm, Fast and Flexible Unsupervised Clustering Algorithm (FFUCA) and compare its results with LEACH algorithm resultants. FFUCA provides an optimal solution for nodes deployment where average square distance between Cnode and sensor nodes calculated for 3 clusters, for LEACH = 136.61 but FFUCA=24.05 and also provides a better DOS detection. It is clearly shown in false negative f_n and false positive f_p results from both algorithms where LEACH has $f_n = 16\%$ and $f_p = 3\%$, but FFUCA has $f_n = 12\%$ and $f_p = 8\%$.

In [32], for achieving highest possibility to detect DOS attacks with best energy balancing, a dynamic method proposed to elect control nodes CN's by considering the remaining energy in each of it. LEACH algorithm used to construct the WSN topology which split the deployed sensor nodes into base station BS, clusters and sub clusters with cluster head CH for each, sensor nodes and control nodes. CN's responsible for motoring the traffic between nodes and nodes behavior and preventing DOS attacks. Proposed method focuses on electing control nodes CN's. The CN's elected periodically depending on highest remaining energy as a criteria. Therefore each node may elected as a CN. For electing Cnodes among a cluster, a random number generator algorithm *Multiplicative Linear- Congruential Generators (MLCG)* is used. The algorithm computed the corresponding non-CH

nodes ID's from generated random numbers as K nodes in first step. From K-nodes, another set K'-nodes will elected with heist residual energy to act as CN. In this way, WSN life time may increase and making elected CN's unpredictable from adversaries.

In [33], the problem that authors tend to solve, is the case of CN may die or CN itself may compromised by an attacking node. Since the election of Cnode depending on highest residual energy, the compromised one tries to prevent been detected by showing a high residual energy. Normally, control nodes do not declare its energy level so, it must be asked about it periodically by means of proposed type of nodes called *Verification Nodes V-node*. Which responsible for monitoring Cnodes residual energy and compare it against a mathematical model of expected power consumption. The authors considered an assumptions which are the cluster head CH's are not compromised, no cooperation between compromised nodes (attackers). In order to reduce the power consumption due to monitoring process by both of Cnode and Vnode, vnode designated to Cnode in time intervals and after collecting enough power level recordings, they will compared with a mathematical model of normal power consumption. Any abnormal expectation leads to detection of compromised Cnode and reported to base station.

4.3 Frameworks and Schemes Category

In this category, authors provides schemes and novel methods for detecting and defending DOS attacks. These method based on arranging well known DOS detecting and defending algorithms into such structures to provide high efficiency detection and defending.

In [19], the proposed framework composed of two stages: Attack detection stage and attack defense countermeasure stage. In detection stage, some of well-known and widely used algorithms for DOS detection integrated together as sub-modules to detect DOS attack in different network layers of WSN. Also in defending stage, various defending methods utilized to perform the better countermeasure against detected dos attack as shown in figure (4.2).

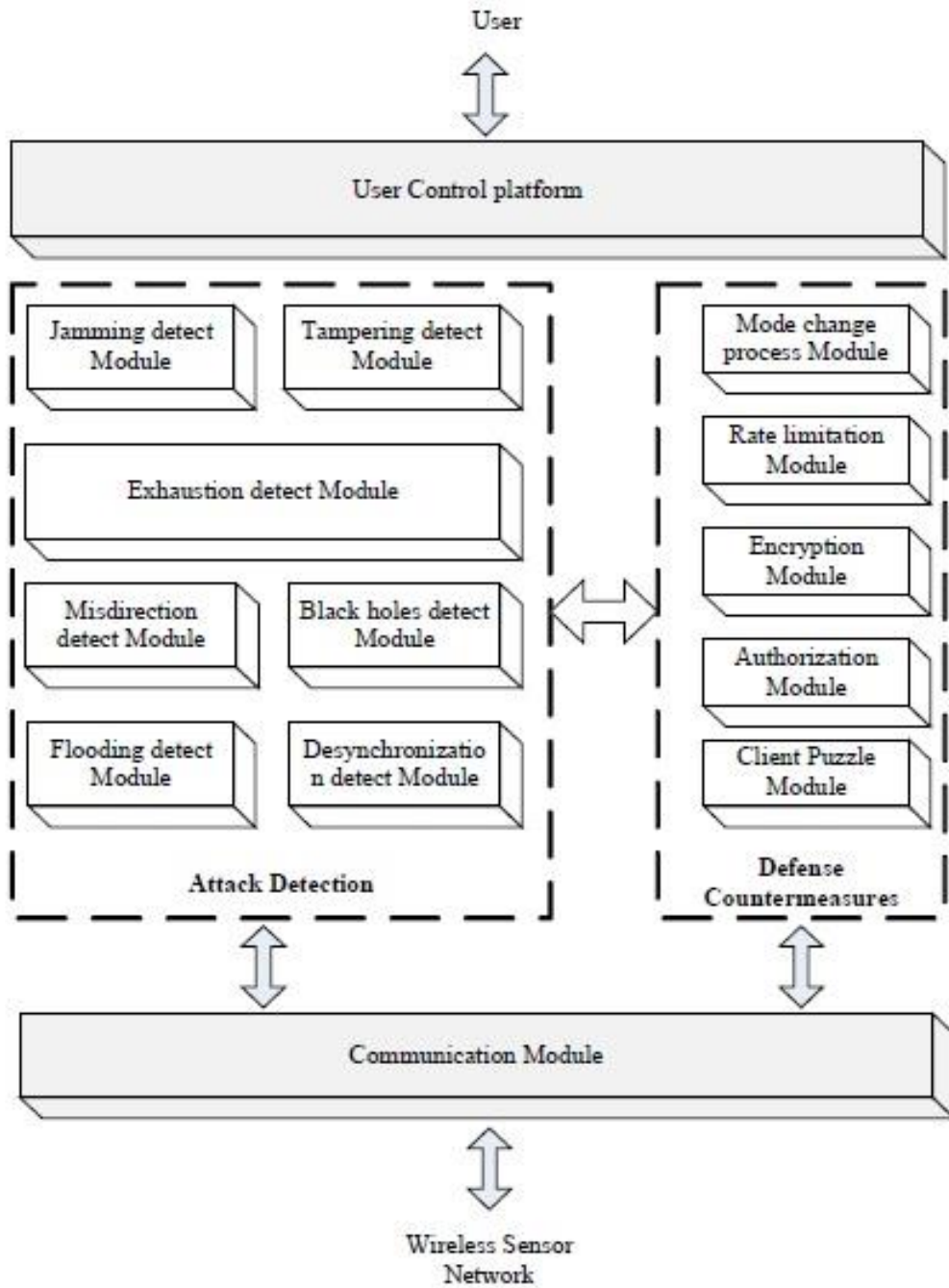


Figure 4.2. Architecture for detecting and defending system

In figure (4.2) the communication module acts as a bridge real time WSN and the attack-defense system sending and receiving packets. User control platform, it designed to let users to interact with proposed system. Attack detection component consist of sub-modules working independently and each sub-module detects specific kind of attacks where if an attack detected a corresponding Flag will setup and send it as a message to communication module. Attack defense countermeasure

component, receives the warning messages and activate the corresponding defense sub-module against certain DOS attack. The advantage of this framework, it is the ability to add more types DOS attack countermeasure sub-modules with high degree of flexibility.

In [21] and [44], Rapidly progressing in internet communication technologies and the wide use of WSN's in different fields, leads to a new concept of automation "anywhere and anytime accessible home environment " which provides users accessing home environment remotely via internet. The main challenge is publically accessible internet for both users and attackers. Then authors concentrate on DOS attacks upon WSN's in *Home Automation Systems HAS*. For that reason, authors provides a novel scheme of security works alongside the conventional of DOS defense techniques. The proposed defense scheme targeted the Low-level DOS attacks by proposing an approach consists of three parts: Virtual Home VH, Remote Home Server RHS and DDOS Defence System DDS. The idea of this approach is to create a virtual home stage to detect the DDOS attacks and prevent it from reaching real WSN as shown in figure below.

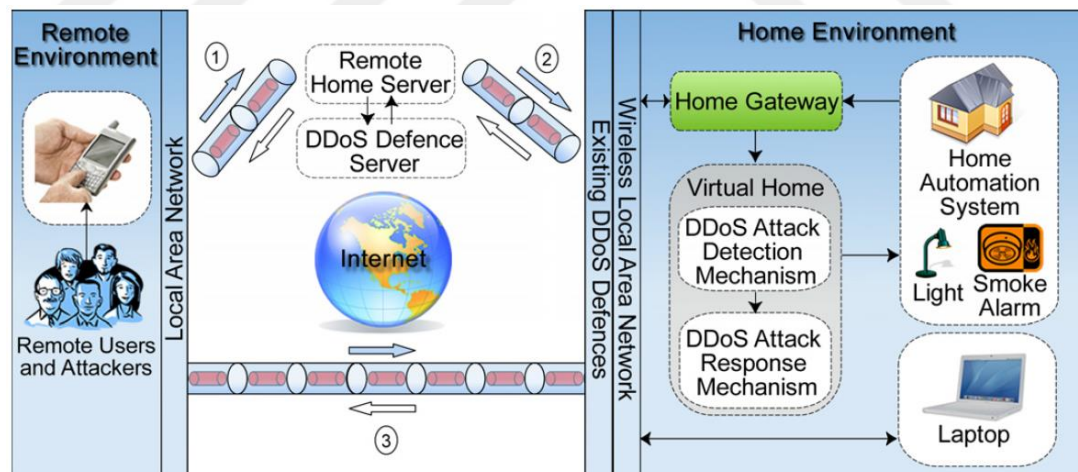


Figure 4.3. Shows the proposed defense scheme

In virtual home-DDOS attack detection mechanism the End-to-End encryption used to ensure users privacy unless an attacker captured the encryption key. If any adversary behavior detected, a corresponding flag is set and a message sent to Remote Home Server RHS to analyze the Home Gateway message. If attack

recognized, DDOS defense server will countermeasure it. But if not recognize the attack which means it is strong enough to block the communication between RHS and home gateway. In such a case, Response Mechanism overcomes the incoming Low-level attack.

In [46], Authors in this paper provides a novel method for detecting and defending a DOS attack on hierarchical WSN topology. They named the method as Message Observation Mechanism MoM. Proposed method usually installed in cluster head because of its higher computational capability and residual power than other nodes. MoM is based on monitoring the messages traveled between nodes and find the malicious node by analyzing traveled message packets. Proposed MoM consists of two lists Normal Message List NML, Abnormal Message List AML and Observation mechanism OM.

Detection mechanism depends on analyzing received messages in cluster head within certain time interval Δt . Each new message consists of parameters : $\langle msg, timestamp, counter \text{ and } ID \rangle$. new messages will compared with AML list, if it is found then it is DOS attack. If new message compared with NML and get matched but it appears more than threshold, then it is a reply DOS attack. As a defense process, when cluster head CH detects a DOS attack, CH broadcast the adversary node ID to neighboring nodes where in turn, they change the authentication key to prevent adversary node from communicating other nodes. Furthermore, to ensure that the adversary cannot copy the new key, a special function been written for that reason.

4.4 Measurements and Analysis Category

The popups of WSN is to collect date for its field whether it reachable or not, friendly area or hostile one. The significant issue is achieve highest efficiency within duty time. Therefore WSN designers and whom in concern of countermeasures of attacks, have to know information about the normal behavior for WSN and its behavior under attacks especially when talking about DOS attack where detecting it is not an easy job. For that reason, measurements and analysis is very important.

In [23], Authors focuses analyzing Sensor-Medium Access Control (S-MAC) protocol which has good energy properties, scalability and collision avoidance. A study case considered when S-MAC protocol is under DOS attack on communication. They studied the case without and with authentication and how it affects the power consumption in each activity while establishing communication channel between two nodes. The S-MAC protocol consists of four a essentials: periodic listen and sleep, collision avoidance, overhearing avoidance, and message passing.

For case of no authentication two situation considered for analyzing, first one when the adversary node B' in between of two nodes A and B (i.e. $r_1 < r$) as shown in figure below.

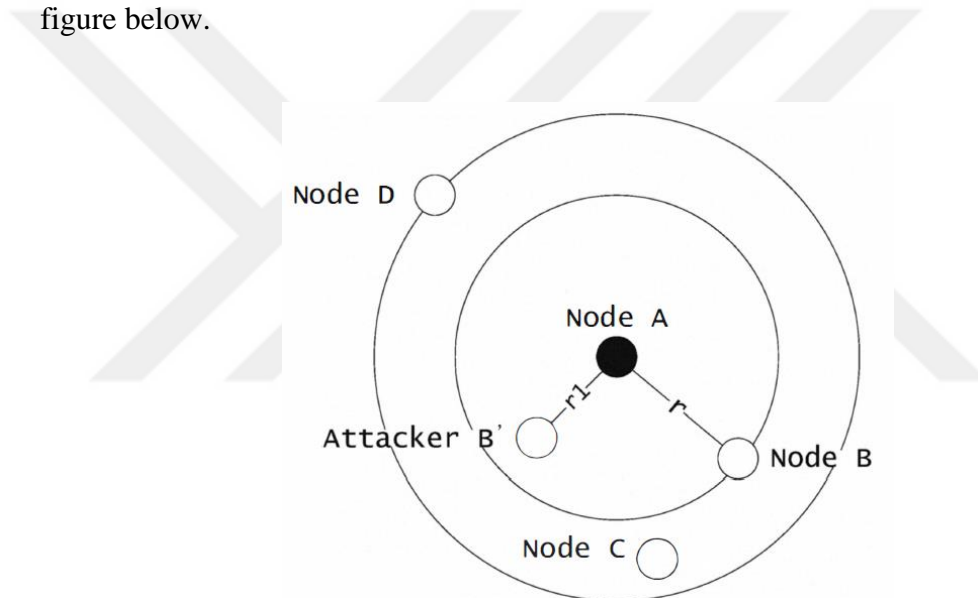


Figure 4.4. DoS attack by neighboring node in S-MAC

B' replies the clear to send packet CTS to A instead of B. the second situation with collision attack where B' keep sending fake Sync packet and request to send RTS to both of A and B and make a collision. The power consumption analyzed and compared same situation with applying an authentication algorithm. The overall result shows less power consumption if authentication used.

In [28], Authors aimed to detect flooding DOS attack which exhausted the energy of sensor nodes. Also they considered the hierarchical topology deployment

for WSN. Authors tend to achieve desired detection by deploying an Entropy estimator nodes. The entropy estimation is classification algorithm which normally used in Data mining and machine learning for distinguishing between normal and abnormal behavior.

Traditional entropy estimation is a logarithmic formula which costs higher power dissipation due to higher calculations needed, therefore, authors provides a simplification for *Bayesian entropy estimation* formula as a practical approximated method which aimed to achieve a low processing efforts, high availability, higher scalability and higher detection accuracy of DOS flooding attack.

The detection process based on simplified Entropy Estimation for key information that attached to traveling messages where in WSN, is key used for authentication and encryption of messages instead of collected information because normal collected information like temperature or light intensity could be regularly changed with respect to time. The comparison of entropy results between normal message transmission and the DOS attack transmission case leads detect which nodes floods a large amount of messages and consider it as attacker.

In [37], authors follow a systematic approach to study the impact DOS attack on WSN. They tend to find a most effective metrics for checking the behavior of WSN nodes and can decide whether nodes under attack or not and moreover, these metrics may be a base for developing an intrusion detection systems IDS. The authors focuses on jamming attack and black hole attack to test their impact on WSN. Also they considered two topologies which are *central data collection* and *mesh multi-hop* using collection tree and mesh protocol respectively. To be sure that chosen metrics are generally applicable, they vary some parameters: Topology (mesh/collect), Traffic (high/low), Transmission power (high/low) and type of Attack (jamming/black-hole/no attack).

Metrics can be divided into three categories: elementary metrics, collection tree specific metrics, and mesh network specific metrics.

Authors analyzed a 28 different metrics and they are found that The local metrics are able to detect jamming and black-hole attacks in a lightweight and most of the metrics are already calculated by the lower network layers.

Also founded that packet delivery rate is the most conclusive metric detecting attacking behavior. By analyzing the listening time and the number of neighboring nodes, both of them can detect the attack on all nodes.

In [45], DOS attack on WSN is not easy to detect. Therefor evaluation of survivability of WSN is very useful information to whom in concern of WSN designing.

Considered cluster- based WSN consists of base sink node which is safe against attacks, sensor nodes which if they are attacked or dead don not affect the cluster service therefor they neglected. So, sink node, major CH and miner CH's are in consideration as in figure below.

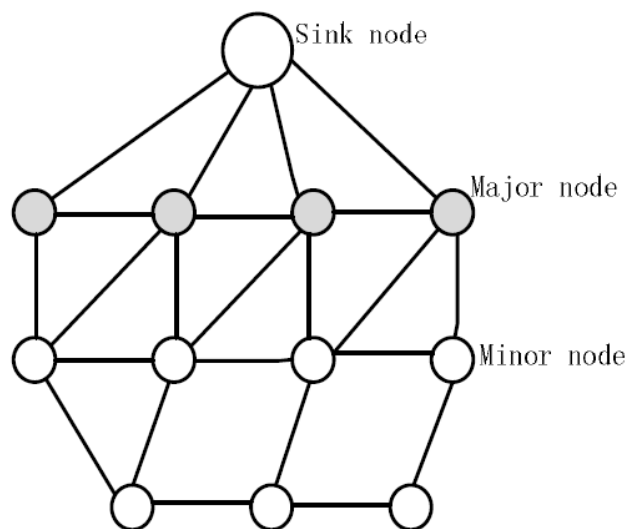


Figure 4.5. Tree structure of cluster-based WSN

Authors gave a definition for survivability as " *The ability to provide basic services after attacks or system error* " and depending on this definition, a method been followed for survivability evaluation consists of two approaches, the first one is

the *analysis of services offered by network* which is communication rate between CH's and *probability of state obtained by Markov Chain* which computes the probability of CH's failure rate especially in case of miner cluster head. The failure rate is due to exhaustive power consumption caused by DOS attack. Therefore, the authors based their evaluation upon two criteria, first one is the density of nodes and the second one is the initial power of nodes.

As a result for their evaluation, they found the survivability will increased if node density and initial power increased too.

4.5 Authentication Approach Category

Authentication is an important approach for security in WSN. Data collected from a certain field especially for hostile ones, should be protected from attackers whom try to capturing a significant information, disturb transmitted data, changing transmitted data, etc. So authentication aim to make authenticated data available for only authorized users especially for sensitive applications like military, health care or environment control.

As an advantage, making transmitted data safe and secure and accordingly, traffic monitoring will be reduced, preventing data injection attacks. On the other hand, several challenges also available. The power consumption is the most crucial factor in WSN's where power will consumed in nodes applying authentication methods. Secondly, it is applicable for a narrow range of attacks like jamming attack. In addition, multi-hop communication also a challenge which rises the probability of attacking communication paths by means of compromised nodes.

In [18], Authors proposed a DoS resilient enhanced two-factor authentication scheme in WSNs. It is based on early two-factor authentication which is simply uses two parameters that nodes in WSN utilize them for identifying the sender side to others and to verifying sender node at receipting node side. These two factors are any two elements well known for both sides for example password and digital signature.

Authors proposed two-factor authentication scheme depending on two enhancing methods. First, Lightweight pre-authentication using Merkle hash tree. A Merkle hash tree which established during initializing phase of WSN. Second, Personalized secret parameters for sensor nodes. Authors concluded that their modified Two-factor scheme has the ability to resist the *Gateway impersonation attack with node captured* and *Forgery attack with node captured* " with high efficiency even with 90% to 100% invalid login messages and adapt dynamically to DoS attacking scenarios ".

In [22], The attackers can compromise sensor nodes and inject false or fake data to perform false alarms. Also can inject a large number of messages in order to exhaust the nodes energy through multi-hop communication till data reaches the sink node. This attack is called *Path-based Denial of Service (PDoS)* attack (i.e. attacker compromised nodes along communication path). As solution for these attacks, multiple nodes can cooperate to produce an authenticated report. *False-Endorsement-Based Denial of Service (FEDoS)* is an attack when an attacker compromises one of cooperated nodes and generate a false endorsement message (MAC) which cannot verified in report generating node. Accordingly, report generating node (CH) compresses endorsements and send it to sink node. Sink node will confused between either FEDoS attack or wrong data injection attack. This issue solved by making endorsing node after a certain time, send a proof message for correct endorsement.

Mentioned solution scheme is sensitive to Jamming attack which affect the communication channel between cooperating nodes and cluster head. so authors proposed a gray-listing approach where the report generating node CH, will not excluding jammed endorsement node at once but put it in gray-list and wait for a proof within next endorsement. The problem with this approach is coasts a higher energy consumption in comparison with previous solution scheme.

In [34], Communication in WSN may suffers from a kind of DOS attacks which called *resource-draining* attack where the attacker floods the WSN with useless or fake messages leading to higher power consumption and buffer overflow.

As countermeasure against this kind of attack, authors proposed a *Hop-by-Hop Broadcast Source Authentication Protocol (H²BSAP)* which provides hop-by-hop authentication of broadcasted messages till reaching Base Station BS. In this way threats are limited to one-hop neighbors only. Proposed protocol separates into three phases which are initialization phase where BS generates Key-Chains and load them into nodes, data broadcast phase where sent data authenticated with the current key of each key-chain and buffering/verification phase where nodes in level (r-hop) buffers received data until correct authentication key appears and if buffered data were authentic then it will forwarded to next hop (r+1)-Hop neighbors.

H²BSAP reduces the time needed for data verification where nodes needs to buffer received data for short time and for one time interval. The protocol shows an extra overheads: computation, storage and transmission which are an open issue to be improved by suggesting implementation MPR-based broadcasting in order to reduce the transmission overhead on the network. Also this protocol suffers from scalability issue since it applicable for static WSN's where it can be studied for node/BS mobility as a future work.

In [38], authors discussed resource-draining DOS attack in time-asymmetry based BSAP. To countermeasure this attack they proposed to hop-by-hop authentication of broadcasted messages which leads to limiting adversary nodes to its one-hop neighbors only. There are several classes of provide broadcast source authentication is time-asymmetry based BSAPs, authors proposed one of them μ -TESLA to secure broadcast communication. Unlike other Unlike other time-asymmetry BSAPs, data will buffered in nodes then a verification process leads to forwarding decision.

Authors proposed a several independent, distinct key-disclosure delays key-chains where the number of key-chains equals to maximum number of hops. Base station BS uses the (*i*) key chain to authenticate data to its *i*_{th}-hop neighbors. Proposed μ -TESLA protocol consists of four phases which they are: initialization phase, MPR-based broadcast tree formation phase which responsible for broadcasting (forwarding) data sent by the BS, data broadcast phase and data

buffering/verification phase. Assuming fixed communication range R , static nodes and base station, well known max. number of hops (i.e. network depth) and only subset of nodes are responsible for data broadcasting.

In [43], Authors mentioned that most of anonymous authentication protocols that designed for WSN-based real-time applications are suffering from missing synchronization between participants within a WSN. This lets WSN vulnerable to DOS attack. As a result for missing synchronization, an anonymous authentication protocol may need to compromise some of the imperative security properties such as un-linkability especially when external user tends to accessing sensor nodes information. Authors proposed a system model consists of three parts: set of users U , a gateway GW and a set of sensor nodes SN where acts in real-time monitoring manner. The proposed Remedy for DOS attack consists of three phases. Firstly, User registration in GW legally, secondly, Remedy phase for DOS attack WSN based anonymous authentication protocol. Successful authentication done by user U authentication request to GW using temporary ID TID , GW responding with generating new TID for the user U . new TID lets U to access sensor nodes SN through public channel and a secret key shared between them. Due to communication upon public channel, DOS attack may occur disturbing U to GW communication where U cannot receive new TID and secret key. Therefore as solution U computes Remedy request depending on unused pair of send ID (sid_j) and emergency key (k_{em}) and send it back to GW , once GW recognize Remedy it regenerates new sid_j and k_{em} and sen it to U_i in this way synchronization will established again. Third, Re-Loading Phase where Before running out of all the shadow identity and emergency key pairs, a user needs to re-load with the new pairs within four steps mentioned in the paper. This solution can easily integrated with current protocol and reduce communication and computational efforts while re-synchronization.

CHAPTER V

OREGIONAL AND PROPOSED METHODS

5.1 Introduction

Denial of Service attack DOS to WSN takes different forms, one of these attack is node compromising. This kind of attack affects messages, which generated by means of attacked nodes. False alarms, false data injection and high power consumption are results for that type of attack especially messages needed to pass several cluster head along the path towards sink node in a certain cluster. This attack called as Path Based Denial of Service P-DOS attack. To mitigate this kind of attack, nodes which belongs to same cluster cooperate between teach other to generate endorsements for a report generated by cluster head CH about a certain phenomenon. Endorsement achieved when each node sends its Message Authentication Code MAC. Cluster head compress these messages and forward it to successor cluster head or to Sink node to be authenticated.

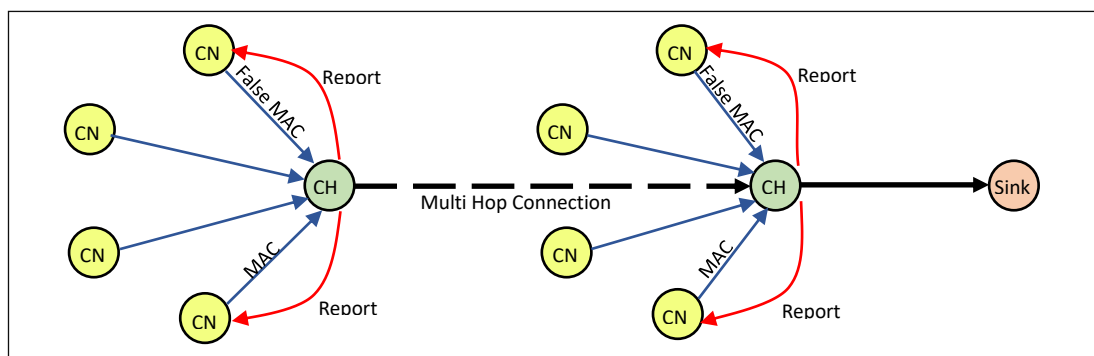


Figure 5.1. Shows False Endorsement DOS attack FEDOS

Figure (5.1) shows the case when a node compromised and receives a report from CH, it responds with false MAC message as a false endorsement. This kind of

attack called False Endorsement attack FEDOS. When final compressed message reaches sink node with false endorsements, sink cannot distinguish whether it is an FEDOS or CH itself compromised and tries to inject false data as a DOS attack. To solve this problem, FEDOS defense method must followed.

5.2 Original FEDOS Defense Method

Nodes that belongs to a certain cluster send their endorsements to cluster head CH. To mitigate FEDOS attack, cluster nodes should send the same endorsement again after a time interval as a proof for the previously sent endorsements. If proof endorsements did not reach cluster head within time interval, delayed node CN will excluded from further endorsement. Therefor Christoph Krauß, Markus Schneider and Claudia Eckert in their paper [22], considered two scenarios first, CN did not sent any endorsement. In this case, this node cannot affect the final endorsement result. Second, if cluster node sent first endorsement but proof endorsement cannot reach cluster head CH because of Jamming attack that affects the communication channel between cluster node CN and cluster head. In such a case authors previously mention proposed an enhancement by adding delayed nodes to a Grey-List instead of excluding an innocent node till node's proof of old endorsement reaches CH with new report endorsement. The method steps explained in below.

5.2.1 Initialization Phase

Initialization phase consists of two parts, before deployment, which configures the WSN nodes to by deploy as a hardware devices and after deployment immediately, which contains executing some routines for one time for security purposes. These retains like giving each WSN node its own unique ID, initial Hash chain value and a key to be use while neighboring nodes communicating between each other.

5.2.2 Report Generating Phase

Generating a report is cooperative effort between cluster head of a certain cluster and cluster nodes belong to it. First, cluster head CH initiate a list for trusted

nodes named as F-list which contains nodes ID's. In the beginning of deployment all cluster nodes will includes in that list. Second, depending on collected information about a certain phenomenon, CH generates a report about it as R and then broadcast it to all nodes belongs to its cluster. In addition, CH also broadcasts the time of generating the report, which named as T_M . Third, when cluster nodes CN's receive R and T_M , they check the T_M if it matches the time of phenomenon occurrence or not. If it is TRUE, CH's check the report R itself weather it matches the occurred phenomenon or not. If both verification pass then CH's generate their endorsements, which are Message authentication code MAC and send them to CH with their Hash values.

When CH receives nodes messages, it regenerate a new Hash value of received endorsement for each node and compare it with old (received) one. If described authentication process result is true, depending on this result, CH generates its own endorsement and send it together with compressed CN's received correct endorsements, CH ID, number of participant nodes, the regional report R and Occurrence time T_M to Sink node to be verified again as a higher level of authentication. Sink authentication not in the scope original scheme interest.

5.2.3 Considering of Jamming Attack

Christoph Krauß, Markus Schneider and Claudia Eckert mentioned in their paper [22], that jamming attack may detected via certain algorithms but it cannot prevented. Therefore, they considered the effect of jamming upon communication between endorsing node CN and cluster head CH. The considered type of jamming attack is the one that prevents or delays CN messages from reaching cluster head but not destroy the message itself.

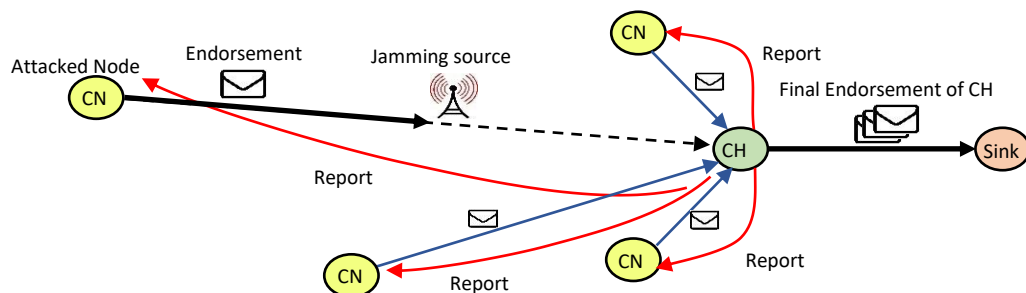


Figure 5.2. Shows Jamming attack model

Figure (5.2) represents the original method while considering jamming attack. The attacked node message prevented or delayed by more than a certain threshold time from reaching cluster head CH jamming source while other nodes messages reached correctly. As a defense solution for such attack, Grey-List enhancement considered. When a node endorsement message don't reach CH, the cluster head instead of excluding that node from further report endorsement, CH remove it from trusted list (F-list) and add it to G-list. With this method, attacked node has a chance to send unreached endorsement for last report with next report endorsement process. In next report endorsement, CH checks if the endorsing node in G-list or not, if in G-list and previous endorsement verified correctly, CH removes node from G-list and return it back to trusted list F-list. Otherwise, if node still under jamming attack or G-list filed, attacked node will excluded in further report endorsement.

5.2.4 Original Method Analysis

Original defense method was succeeded in mitigating False-Endorsement Based DOS attack because of re-computing the Hash values and compare it with received ones. But it has a serious pitfall when considering Jamming attack. If the last endorsement Hash value didn't reach CH at all or delayed more than threshold, in both cases this node will suffer from False-Exclusion while it still functioning correctly. That is mean if jamming attack continue preventing messages, more innocent nodes will excluded.

5.3 Proposed False-Exclusion Mitigation

Previously mentioned FEDOS method, has a pitfall of false-excluding nodes that their proof endorsements cannot reach CH to be authenticated because of effect of jamming attack. Therefore, an enhancement is needed to fix the problem of excluding well-functioning nodes from further report endorsement. The proposed enhancement provides a solution for multi path endorsement message delivery and do not let communication between attacked node and the cluster head be limited with direct path for transferring messages towards CH.

5.3.1 Assumptions for Proposed Method

To achieve the desired results with propose enhancement, the system model of WSN that proposed method applied on, should well-defined. Several assumption were taken in consideration while designing proposed model as following illustration:

- The cluster head is safe.
- Cluster head has higher energy, storage and computational capabilities.
- The deployed sensor nodes is not movable.
- Nodes deployed randomly.
- Cluster head has information about what nodes functioning correctly, doubtful nodes and nodes under Jamming attack.
- Jamming attack causes message delay but not destroy it.
- Node under jamming attack still alive and functioning correctly.
- Cluster head control communication between nodes.

5.3.2 Structure of Proposed Model

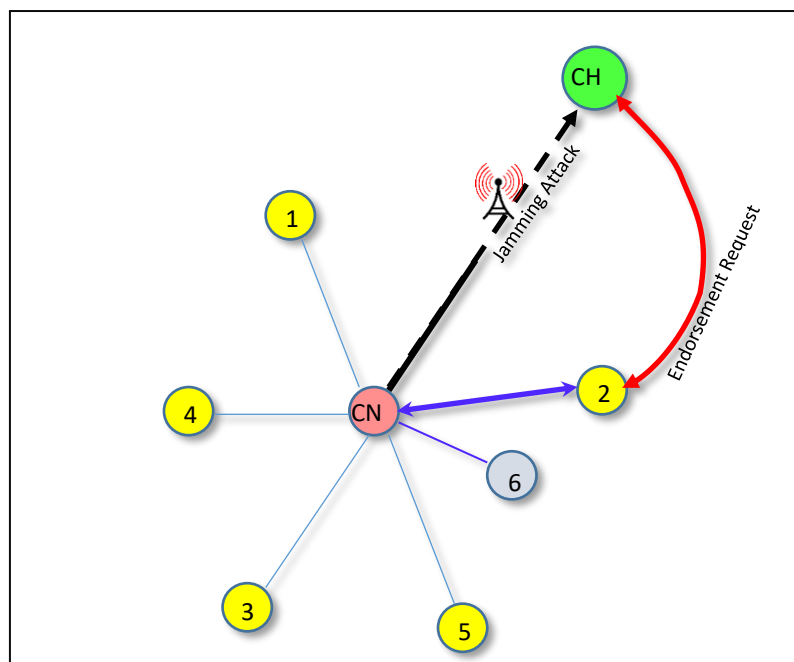


Figure 5.3. Shows the structure of a cluster

Figure (5.3) shows the structure of a cluster with its nodes and cluster head CH and their links. The link between CN and CH formed as a continuous and dotted line to represent the Jamming attack, which prevents message from reaching CH. Red arrowed line, represents communication between CH and nearest neighbor node to attacked node CN. Moreover, the blue arrowed line represents the controlled communication between attacked node CN and nearest node. The other thin blue lines represents distances from CN to each other nodes.

5.3.3 Proposed Enhancement

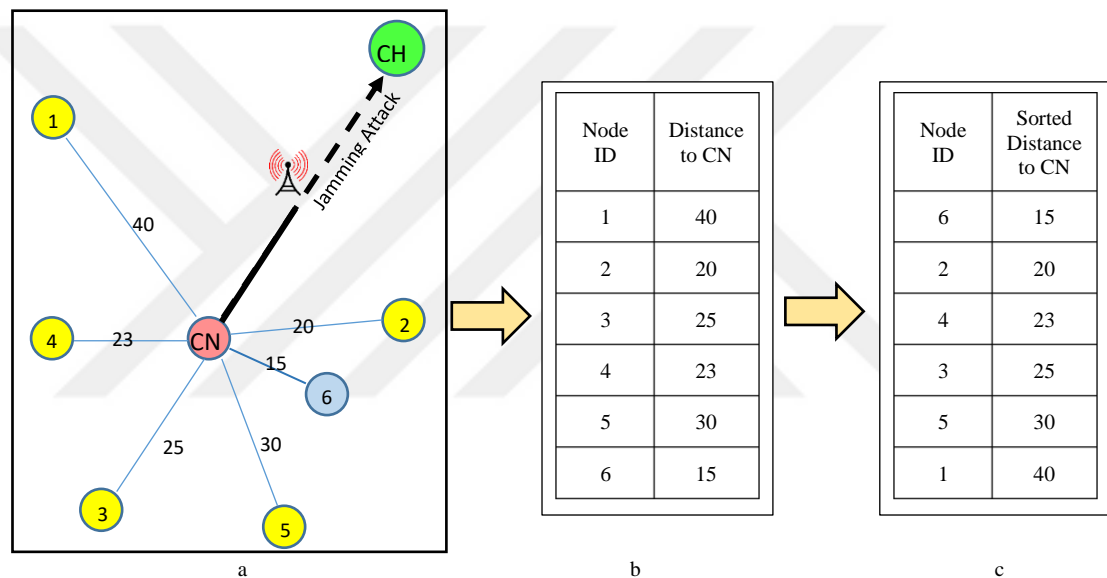


Figure 5.4. a) Nodes distribution, b) Distance table to node CN, c) Sorted Distance table to node CN

Figure (5.4), shows the cluster head behavior when node CN's second endorsement failed in reaching to it as a verification for last received endorsement. In phase, CN ID located in Gray-list and might excluded because jamming attack still acting. First, as in figure (5.4-a), cluster head CH collects the deployed nodes locations, where the locations is stored while deployment process occurred in WSN initialization phase. Second, as in figure (5.4-b), cluster head computes the distances between each node to other nodes and save results to a distance table, each node has its own distance table to others. Third, as in figure (5.4-c), CH sorts distance table in

ascending manner. The benefit of sorting is to pick the nearest neighbor to attacked node CN to communicate with between each other where real life, distance is an effective coefficient in reducing consumed energy.

Cluster head CH also collects information about the doubtful nodes and save them to a certain table. Those nodes may be compromised or acts as an adversary tries to inject false endorsement messages. As in cluster structure that represented in figure (3), node number (6) for example, represents a doubtful node. Therefore when CH selects a nearest safe neighbor node to attacked one CN, doubtful table contents (i.e. doubtful nodes) been taken in consideration. So, node (6) will be bypassed even it has nearest distance to CN. The benefit of this process is to protect CN from giving its critical information to malicious node may use them to act as legal node. In our example, node (2) will be selected as a nearest neighbor safe node to CN.

After selecting nearest safe neighbor to attacked node CN, CH send it a message with contents of (ID number of attacked node and a request for endorsement). This message tells selected nearest neighbor node (2) as in figure (9) to ask attacked node CN for its endorsement, which prevented from reaching CH because of Jamming attack and forward it back to cluster head CH. In figure (9), request message represented with a Red arrowed line. Next step, the selected neighbor communicates with the attacked node CN and send it CH's request. This communication represented as a blue arrowed line in figure (9). In this process, timing is a very important factor to check out whether the transmitted and received messages will be done in expected threshold time or not. Therefore, selected neighbor saves the time of sending request to attacked node CN.

When CN receives the request message, it responds by replaying selected neighbor node with its endorsement, endorsement hash value, node ID and time of replaying. As soon as selected neighbor node receives CN endorsement, it forwards the message to CH with the following information: **first**, selected neighbor node ID, which is an important information especially if CH manipulated multiple jamming attack cases. **Second**, attacked node ID to inform CH that this endorsement belongs to specific attacked node and to make sure that nearest node requests the correct CN.

Third, the CN endorsement message and its Hash value. **Forth**, requesting time of sent message to CN and replay time to nearest node.

When CH receives selected neighbor node message, an authentication process will start at once. First, CH checks the time difference between requesting and replay time. If it is more than threshold time then CH realize that the link between nearest node and CN also affected by jamming attack. If time difference is within acceptable range, CH will re-computes the Hash value for received endorsement and compare it with saved one. If comparison result came true the CN ID will removed from gray list and CN permitted for further endorsement. If it is not, that is mean CN suffers from another kind of attack in addition to jamming attack like compromising by another node.

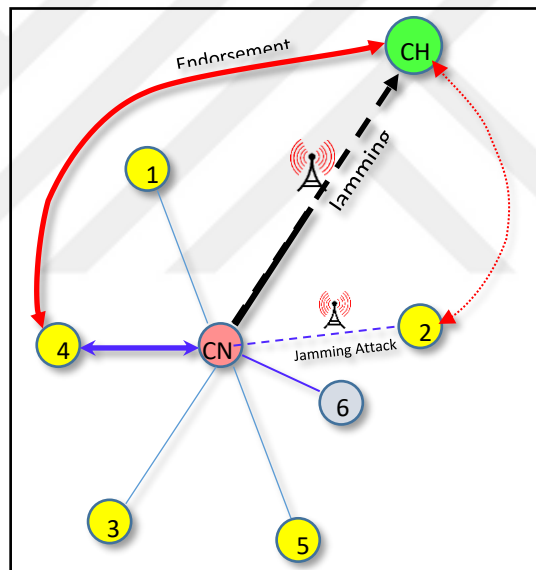


Figure 5.5. Shows case of first neighbor node failed

Figure (5.5) shows that in case of nearest neighbor node (2) fail with communicating with CN, or in other words, the authentication of CN endorsement forwarded by nearest neighbor failed. As a response of cluster head towards such a case, it selects another neighbor node from sorted distance table which belongs to attacked node CN and send the same request message previously mentioned. As in figure (11), this case happened and node (2) failed to communicate correctly with

CN, therefor next safe neighbor node in sorted distance table (node (4)) selected. The dotted arrowed line represents the failed authentication path but the solid one between CH and node (4) represent the second attempt CH to reach attacked node endorsement. The cluster head CH keep trying different neighbor nodes till first correct endorsement authentication occurs. If so, the attacked node will be trusted again for further endorsement and removed from grey-list.

5.3.4 Analysis of Enhanced Method

The main advantage of proposed method is **preventing False excluding** innocent nodes from being a participant from further report endorsement while it alive and functioning correctly. The other major advantage is detecting **double attack** on same node, as a Jamming attack prevent its message reaching CH and also may be compromised by another node. Also this proposed algorithm give the cluster head a good chance to receive the attacked node endorsement via different paths in order to mitigate the chances of excluding a node which is alive and still functioning. And CN can find at least one node of neighboring nodes can communicate with attacked one.

Delivering attacked node's endorsement under full control of CH is very important for enhanced algorithm to be success because communication prevention Jamming attack affects communication channel between CN and CH directly. Therefore attacked node do not know that it been under attack due to no acknowledgment replayed to it from CH. For example, if attacked node has acknowledged and it tends to broadcast its endorsement to neighboring nodes without CH control, the attacked node cannot make sure that whether neighboring receiving nodes were safe or not. If some of neighboring nodes were compromised, they will capture sensitive information like node ID and HASH value of endorsement and use them with injection false data via legal ID. In addition, broadcasting costs higher power consumption and node will die very soon.

The disadvantages represented by consuming more energy due to more communication activates.

5.4 Algorithm Notation

5.4.1 Algorithm for Cluster Head CH

```
If CN ∈ Grey_list then  
  CH collect nodes locations in Loc_Table  
  For each node do  
    CH calculate the distance to neighbor nodes  
    Save distances in Dist_table  
    Sort Dist_table in ascending manner (shorter distance first)  
  End  
  CH collect doubtful node ID's in a table  
  CH get attacked_node ID  
  CH extract safe and healthy nodes to Neighbor_table (sorted)  
  For each nodei in Neighbor_table do  
    CH(attacked_node_ID, endr_request) → neighbor_nodei  
    CALL Query_endorsement function  
    neighbor_nodei (CN endorsement, request_time, replay_time) → CH  
    CH do authentication  
  CH(time_difference) = CH(replay_time) – CH(request_time)  
  If CH(time_difference) <= threshold Then  
    CH(new_hash) = Hash(CH(endorsement))  
    If CH(old_hash) == CH(new_hash) then  
      Grey_list(CN_ID) = []  
      White_list ← CN_ID  
    End For loop (endorsement correct)  
  Else  
    Doubtful_list ← CN_ID  
  End  
  Else  
    CN still under Jamming attack  
    Return an apply next neighbor_nodei+1  
  (till first correct endorsement occur)  
  End  
End  
End
```

5.4.2 Algorithm for Query_Endorsement Function

Neighbor_node_i ← request time

Neighbor_node_i (Neighbor_ID, query_request) → CN

CN (CN_ID, endorsement, Hash(endorsement), replay_time) →
Neighbor_node_i

Neighbor_node_i (ID, CN_ID, endorsement, Hash (endorsement), replay_time,
request_time) → CH



CHAPTER VI

ORIGINAL AND ENHANCED ALGORITHMS IMPLEMENTATION (RUNNING AND TESTING)

6.1 Introduction

In this chapter, original and enhanced methods implementation will be discussed from a practical side of view. Also, what simulation and implementation environment has been used. After implementing models, some testing scenarios followed to ensure that the enhancement method whether achieved its purposes or not.

6.2 Simulation Environment

Among a large number of well-known simulation platforms for simulating Wireless Sensor Networks like Omnet++ or Network Simulator 2, MATLAB was chosen to implement the original and enhanced algorithms because of several reasons. First, in both models it is not needed to monitor the traffic between nodes which other simulators designed for but what is needed mostly coding capabilities that MATLAB provides especially authentication method improvements. Second, MATLAB programming language is simple code, tracking bugs and troubleshooting. MATLAB ver. R2013a was used for that purpose. It was installed on a laptop under Windows system with hardware specifications of 8 GB RAM and core i7 processor.

6.3 WSN configuration

Since the purpose behind needed implementing an authentication enhancement, the proposed WSN topology was chosen to be simple but sufficient to get

the desired results. No algorithms for clustering and self-organizing applied because they are not in the scope of problem to be solved. Therefore, sink node, sensor nodes were selected randomly. The cluster head CH chose to be in the middle of sequence of generated nodes.

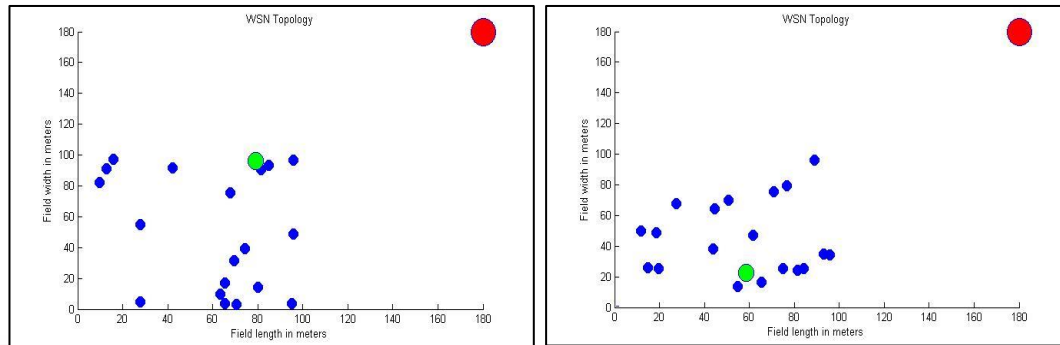


Figure 6.1. a,b shows randomly distribution of nodes

As shown in figure (6.1), the field dimensions selected as $100\text{m} \times 100\text{m}$ square shape for nodes to be randomly deployed. Figure(6.1-a,b) shows the randomness for two different execution iterations. Since cluster head node in the middle of nodes sequence, it also randomly selected. Initially, selected topology consist of 20 nodes with ID's of 1..20. the cluster head selected accordingly as node number 10. Timing also is very important variable to configure. Its importance came from its effectiveness while authenticating received messages from node CN to cluster head CH and distinguishing between delayed nodes i.e. under jamming attack and safe ones. Because of simulation environment is high speed, threshold configured as 50ms. Power consumption also considered for nodes where CH has initial energy of (1) Joule and sensor nodes as (0.5) Joule to ensure that CH has higher energy specification. Power dissipation values also configured as 5×10^{-5} Joule per message. Power configuration is for future work improvement. Previously mentioned configuration is valid for original method and its improvement.

6.4 Running Algorithms

In order to understand the overall behavior of original and enhanced methods, it is necessary to separate them and study them individually. It is also needed to

evaluate their behaviors with and without jamming attack. It is worthy of mention that with each running iteration, internal table and data structures will rebuilt to make changing variable easier to track and understand.

6.4.1 Original Method Without Jamming Attack

When no jamming attack available, program configured to run with normal entries to observe whether expected results achieved or not. It is expected from CH to generate a report and broadcast it to all nodes.

After running it is seen that report generated correctly with values:

```
'FEDOS_REPORT'  
[2017,12,12,19,56,51.870]
```

as report value and time stamp for report generating respectively. The report reaches all nodes after broadcasting process. In return, each cluster node responds by replaying its endorsement values as shown below:

```
'MAC message'  
'8edee1d50d6af0a9ef1944b416e6a92a'  
[2017,12,12,19,56,51.915]
```

Where first value is the Message Authentication code MAC, second value is the MD5 encryption Hash value for endorsement message and time stamp for endorsement replaying. In authentication phase, CH compares endorsement time stamp with report time stamp for each cluster node CN_i . If time difference more than 200ms then CH realize that corresponding node is under attack.

$$51.915 - 51.870 < 50\text{ms}$$

Therefore CH re compute endorsement and compare them to check if there is a false data injection data changing.

6.4.2 Original Method With Jamming Attack

In this case, configuration is as previously mentioned accept activating jamming attack routine which responsible for delaying endorsement replaying from certain attacked node towards CN. As a configuration, cluster node 5 been selected as attacked node. Generating report is same as in (6.4.1) so the difference will appear in endorsement replaying time stamp. The report as follows:

```
'FEDOS_REPORT'  
[2017,12,12,20,49,14.870]
```

A safe node like node (1) endorsement as follows:

```
'MAC message',  
'8edee1d50d6af0a9ef1944b416e6a92a',  
[2017,12,12,20,49,14.916]
```

Endorsement for attacked node (5)

```
'MAC message',  
'8edee1d50d6af0a9ef1944b416e6a92a',  
[2017,12,12,20,49,14.932]
```

In authentication process it is noticed that for node (1)

$$14.932 - 14.870 \leq 50\text{ms}$$

While for node (5) the comparison as follows

$$14.932 - 14.870 > 50\text{ms}$$

As a result authentication process decided to transfer node 5 to Grey-list to receive it endorsement with next report endorsement and remove it from trusted list. In below, a table shows trusted list and grey-list

Table 6.1. Authentication failure due to jamming attack

Trusted list																			
1	2	3	4	0	6	7	8	9	11	12	13	14	15	16	17	18	19	20	
Grey-list																			
0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

6.4.3 Original Method Second Endorsement

Second endorsement as a proof for last one, is very important to reallocating nodes that transferred to Grey-list due to jamming attack as a trusted nodes. To do so, grey-listed nodes should send their last endorsement with next report endorsement. Continuing same example, to simulate such a case, system configured with node (5) located at grey-list. Advisedly, set the jamming attack state as NO-Attack and run the simulation. The experimental results matches the expected one where node (5) authenticated correctly exactly as explained previously, it removed from grey-list and added to trusted list as shown in table below.

Table 6.2. Correct authentication after jamming attack

Trusted list																			
1	2	3	4	5	6	7	8	9	11	12	13	14	15	16	17	18	19	20	
Grey-list																			
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

The most important case in authentication process for original method when node (5) tend to resend its previous endorsement with new one towards cluster head CH while jamming attack still effective and prevents node (5) messages to reach CH. In this case system configured node (5) grey-listed, jamming attack is still functioning upon node (5). The obtained results came as theoretically expected as shown in table (6.3) below.

Table 6.3. Second endorsement authentication failure due to jamming attack

Trusted list																			
1	2	3	4	0	6	7	8	9	11	12	13	14	15	16	17	18	19	20	
Grey-list																			
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

As seen in table (6.3), node (5) still suffering from jamming attack while second endorsement generated. So as a reaction from authentication routine towards such situation, is to remove node (5) from both trusted list and grey list and excluded from further report endorsement.

As an analysis for this issue, it is useful to give nodes under attack a second chance to be trusted again for further endorsement processes. But on the other hand, it is a serious problem when jamming attack has continue acting on same node or region. It is wasting of effort, cost, time and monitoring capabilities to lose innocent nodes while they still well-functioning with ability of further endorsing actions.

To solve this issue, enhanced method designed for mitigating innocent nodes excluding and give a higher degree of flexibility for endorsing nodes under attack to forward their endorsements towards CH correctly via different paths without keep trying a direct path contact to cluster head.

6.4.4 Running Enhanced Method

The enhanced method starts acting from limitation point of original method which is the false excluding of an innocent nodes due to continuous jamming attack effect. The situation that enhanced method manipulate is when a node (e.g. node (5) as same as previous example) still under attack and instead of excluding it after second endorsement sending failed attempt, cluster head tries to find another path to deliver attacked node's second endorsement. The enhanced method is as follows:

As a configuration for the system, node(5) in grey-list, jamming attack still affects attacked node, odd node ID's [1,3,7,9,11,13,15,17] are untrusted nodes due to any other problem and total number of nodes are 20.

First, Cluster head collects the locations of all nodes related to same cluster and gather them in a table.

Table 6.4. Shows nodes location

Node ID	X- position	Y-position
1	81.4723686393179	90.5791937075619
2	12.6986816293506	91.3375856139019
3	63.2359246225410	9.75404049994095
4	27.8498218867048	54.6881519204984
5	95.7506835434298	96.4888535199277
6	15.7613081677548	97.0592781760616
7	95.7166948242946	48.5375648722841
8	80.0280468888800	14.1886338627215
9	42.1761282626275	91.5735525189067
CH	79.2207329559554	95.9492426392903
11	65.5740699156587	3.57116785741896
12	84.9129305868777	93.3993247757551
13	67.8735154857774	75.7740130578333
14	74.3132468124916	39.2227019534168
15	65.5477890177557	17.1186687811562
16	70.6046088019609	3.18328463774207
17	27.6922984960890	4.61713906311539
18	9.71317812358475	82.3457828327293
19	69.4828622975817	31.7099480060861
20	95.0222048838355	3.44460805029088

Second, for each node CH computes the distances from a certain node to other nodes and save results to a node related table. Table below shows from attacked node (5) to other nodes. The formula used to find distance is

$$\text{Dist} = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Table 6.5. Shows other nodes distance to attacked node

Other Node ID	Distance to other node	Description
1	15.4529723871776	
2	83.2116012523245	
3	92.6290307479009	
4	79.7359747412059	
5	0	Distance to itself
6	79.9914092717396	
7	47.9513006935438	
8	83.7885878804230	
9	53.7995646587068	
CH	16.5387558881206	Distance of node(5) to CH
11	97.6950578018999	
12	11.2695198215506	
13	34.7309820518311	
14	61.1471651741237	
15	84.9225592124714	
16	96.6346431634733	
17	114.334402926180	
18	87.1921945321538	
19	69.9021103585224	
20	93.0470971936874	

Next step, sorting distance table related to attacked node in ascending manner as table shown below.

Table 6.6. Sorted distances to attacked node

Other Node ID	Distance to other node	Description
5	0	Distance to itself
12	11.2695198215506	
1	15.4529723871776	
CH	16.5387558881206	Distance of node(5) to CH
13	34.7309820518311	
7	47.9513006935438	
9	53.7995646587068	
14	61.1471651741237	
19	69.9021103585224	
4	79.7359747412059	
6	79.9914092717396	
2	83.2116012523245	
8	83.7885878804230	
15	84.9225592124714	
18	87.1921945321538	
3	92.6290307479009	
20	93.0470971936874	
16	96.6346431634733	
11	97.6950578018999	
17	114.334402926180	

Next step, CH bypasses the untrusted node ID's [1,3,7,9,11,13,15,17] from possible communication with attacked nodes. Also attacked node distance to itself and distance to CH.

Table 6.7. Sorted nodes left to communicate with attacked node

Other Node ID	Distance to other node
12	11.2695198215506
14	61.1471651741237
19	69.9021103585224
4	79.7359747412059
6	79.9914092717396
2	83.2116012523245
8	83.7885878804230
18	87.1921945321538
20	93.0470971936874
16	96.6346431634733

Table (6.7) shows the nodes left as authorized ones to communicate with attacked node CN. The next step, is to select the nearest safe neighbor to attacked node which in our example node (12) with distance of (11.269) meters to communicate with CN.

Cluster head sends a request message to node (12) with content of attacked node ID which is (5) in order to know with which node should communicate and request message as '*Request Endorsement*'. Node (12) utilize these information and send to attacked node CN an endorsement request message to inform it that cluster head requests unreached last endorsement. The message is as following:

querying nodes is 12

querying message is '*Request Endorsement*'

querying time stamp is [2017,12,13,20,6,5.699]

cluster node has informed that its last endorsement did not reached CH and it still grey-listed. And moreover, CH requests its last endorsement via node (12). This information helps node (5) to know to which node should respond. Also attacked node informed that it requested at querying time stamp. As a response, attacked node (5) responds by replaying its last endorsement to querying node (12) with these information:

responding node is 5

responding message is '*MAC message*'

responding Hash value '8edee1d50d6af0a9ef1944b416e6a92a'

responding time stamp [2017,12,13,20,6,5.699]

as soon as node(12) received attacked node's endorsement, it forward the message to cluster head with following contents:

querying node is 12

attacked node is 5

endorsement message '*MAC message*'

endorsement Hash value '8edee1d50d6af0a9ef1944b416e6a92a'

querying time stamp [2017,12,13,20,6,5.699]

responding time stamp [2017,12,13,20,6,5.699]

cluster head compares time stamps if difference less than or equals threshold time message accepted and that is mean the path between node (12) and attacked node is clear. If so, CH recalculate a new Hash value from received one and compare theme.

If they were matched, then endorsement completed and node (5) removed from Grey-list and added to trusted list. Otherwise, CH realized that it detects a double attack on same node and add node (5) to untrusted node list.

If jamming attack also affects path between querying node and attacked node, time stamp comparison will fail. So, CH picks next node in distance table and repeat querying process till first correct endorsement received.

6.5 Test Case Scenarios

In order to proof the enhanced algorithm ability of mitigating false exclusion node DOS, several test case scenarios applied. In each scenario, some assumptions considered as an initial conditions to apply that scenario. Testing scenarios considered a variation of six different factors in order to put enhanced algorithm under wide range of testing possibilities. These factors were:

- Number of deployed nodes (size of network) and their positions selected randomly.
- Is it under attack or not. It takes values of 'YES' for active jamming attack or 'NO' for inactive jamming attack
- Number of attacked nodes as a percentage of total deployed nodes.
- Level of authentication, where level ' 1 ' means a authenticating grey listed nodes without jamming attack. While level ' 2 ' means authentication process for grey listed nodes under active jamming attack.
- Number of doubtful nodes around attacked nodes. Where these nodes under other kind of attacks making them unsafe to deliver endorsement. They were selected as a percentage of total node number.
- Number of nodes that inject false data. They are a percentage of attacked nodes where represent double attacked nodes.

These factors varied individually or combination of them to ensure false node exclusion DOS mitigation efficiency. Test case scenarios illustrated in below.

6.5.1 Scenario (1)

In this scenario it is needed to test the ability of original algorithm to authenticate various percentage (number) of attacked nodes in grey list while no jamming attack acting.

Testing scenario inputs

num_of_nodes = 100; % number of nodes to be deployed

jamming_state = 'no'; % working state of jamming attack Yes or No

attack_percentage=5; % setting of percentage (%) of attacked nodes from total nodes number

defense_level = 2; % if =(1) no nodes in G-list previously
% if =(2) previously attacked nodes in G-list

doubtful_percentage = 0; % setting of doubtful percentage (%) of total nodes around attacked nodes causes endorsement delay

fals_injecting_node_percentage = 0; % percentage of double attacked nodes among total attacked nodes causes false data injection

Testing scenario results

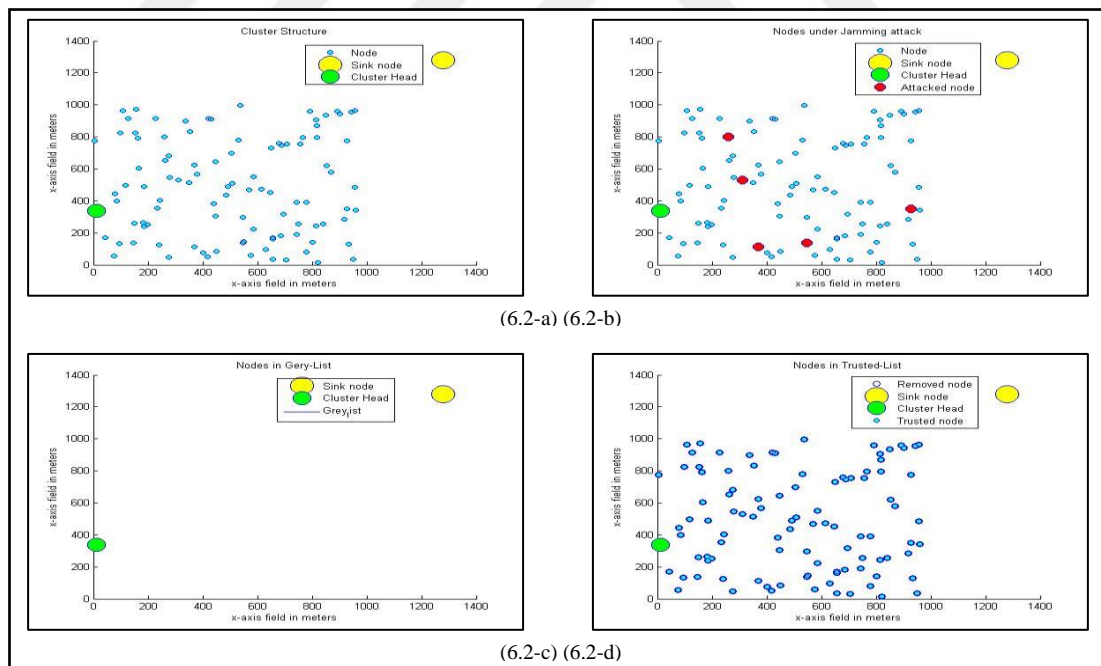


Figure 6.2. Scenario (1), shows 100 nodes and 5% attacked

Figure (6.2) shows the results for scenario (1) where (6.2-a) presented the whole assumed cluster structure with sink node, cluster head nodes. While (6.2-b)

shows in addition, attacked nodes randomly selected which they are in CH's grey-list to be authenticated. Since no active jamming attack assumed, (6.2-c) shows empty grey-list with no red circles after successful authentication and all attacked nodes removed from grey-list then added to trusted-list as in (6.2-d) where no empty circles appears. To ensure this test, new assumption will assumed with higher number of nodes and higher percentage of attacked nodes as follows:

num_of_nodes = 500 nodes
jamming_state = 'no'
attack_percentage = 10 %

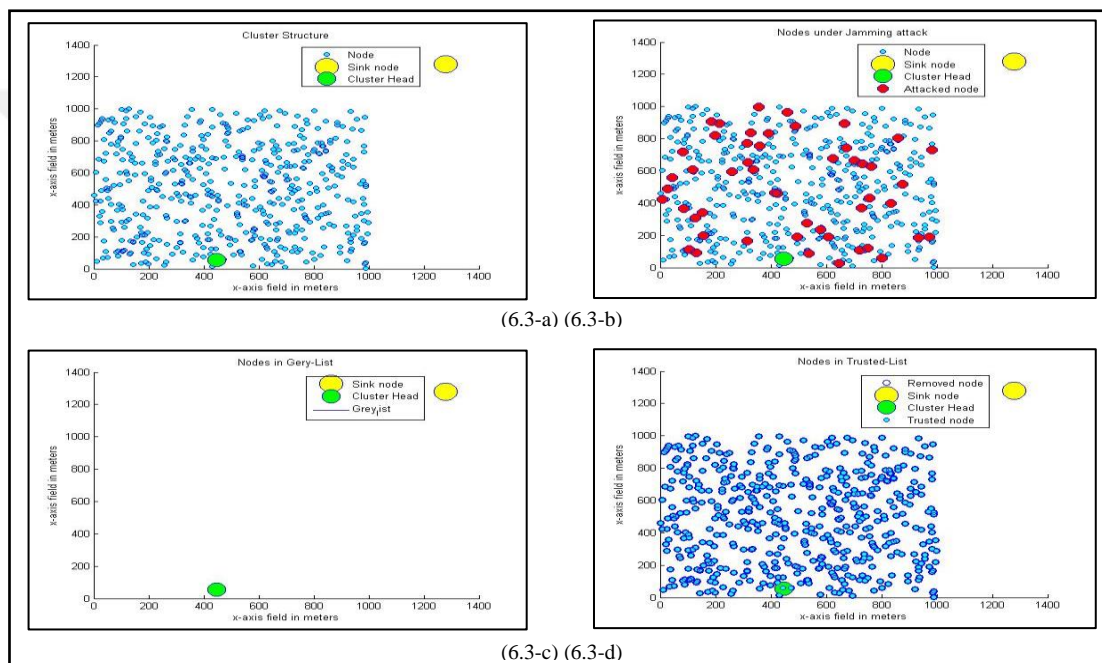


Figure 6.3. Scenario (1), shows 500 nodes and 10% attacked

Figure (6.3) shows that the original algorithm has also successfully authenticated attacked nodes even in case of increasing number of nodes in cluster and number of attacked nodes five times.

6.5.2 Scenario (2)

In this scenario it is needed to show the behavior of original algorithm when jamming attack keep acting on communication channel between attacked node and cluster head. As in input parameters below.

Testing scenario inputs

num_of_nodes = 100 nodes
jamming_state = 'Yes'
attack_percentage = 10 %
defense_level = 2

Testing scenario results

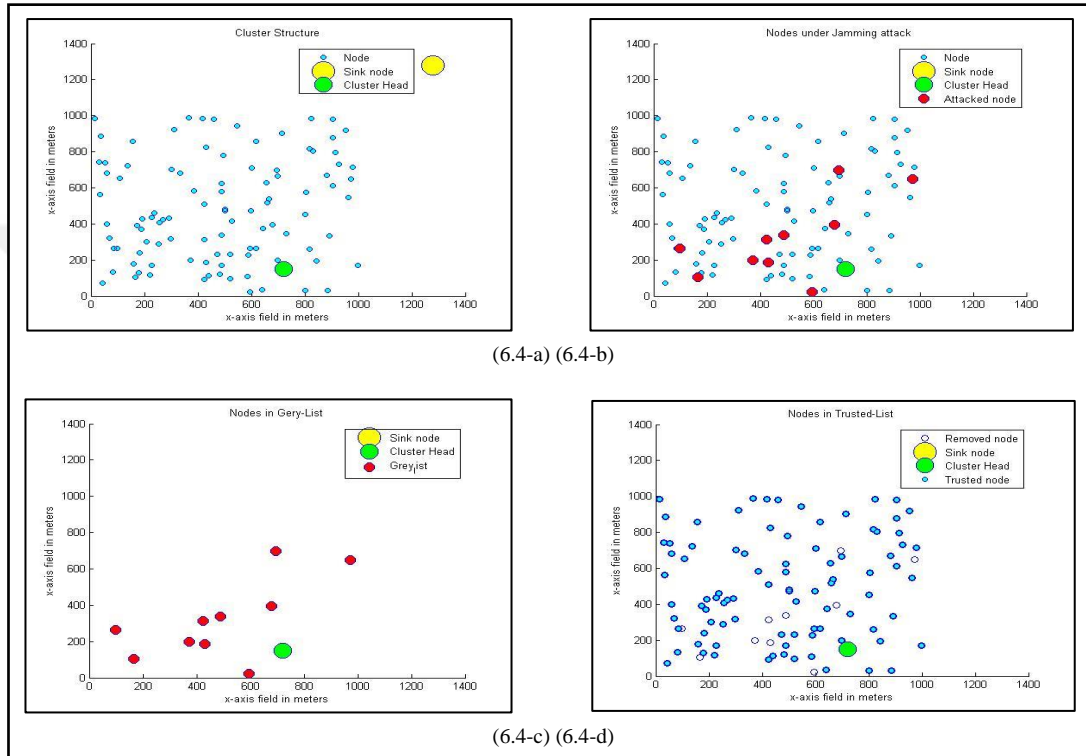


Figure 6.4. Scenario (2) attacked nodes, Jamming attack

Figure (6.4) shows that the original algorithm has no ability to authenticate attacked nodes for second proof endorsement. So, figure (6.4-a) represents assumed cluster structure and figure (6.4-b) shows attacked nodes that selected randomly and their places among the structure. Figure (6.4-c) shows grey list after authentication process where attacked nodes still in there because of jamming attack prevents their second endorsements to reach cluster head CH. Accordingly, figure (6.4-d) shows trusted node list with empty circles representing same count and location of attacked nodes in grey list that algorithm didn't authenticate.

6.5.3 Scenario (3)

In this scenario the parameter configuration will be as same as scenario (2) but it will applied on enhanced method to show the compare between both algorithms for same initial conditions.

Testing scenario inputs

num_of_nodes = 100 nodes
jamming_state = 'Yes'
attack_percentage = 10 %
defense_level = 2

Testing scenario results

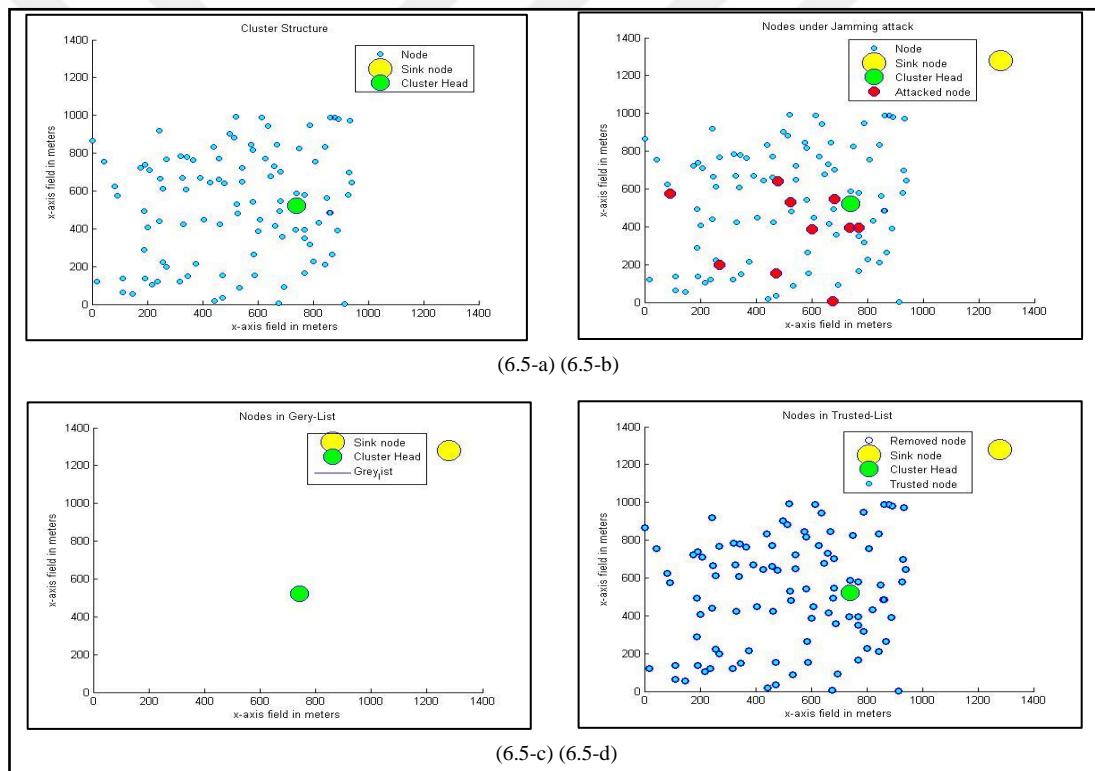


Figure 6.5. Scenario (3) Jamming attack and enhanced algorithm

Scenario (3) shows that enhanced algorithm has the ability of authenticating attacked nodes placed in grey list (6.5-c) and transferred them to trusted list as shown in (6.5-d) using neighbor nodes list to each attacked node. Therefore it is clear difference between figures (6.4-d) and (6.5-d).

6.5.4 Scenario (4)

In this scenario a further parameter added to previously mentioned ones which is doubtful node percentage parameter that represents number of neighboring nodes selected randomly as a percentage of total node number. The communication channels between attacked node and Those nodes also affected by jamming attack so, they cases a delay. The aim of scenario (4) to proof that enhanced algorithm is able to bypass those nodes if they lies in sorted neighboring list.

Testing scenario inputs

num_of_nodes = 100 nodes
jamming_state = 'Yes'
attack_percentage = 10 %
defense_level = 2
doubtful_percentage = 10 %

Testing scenario results

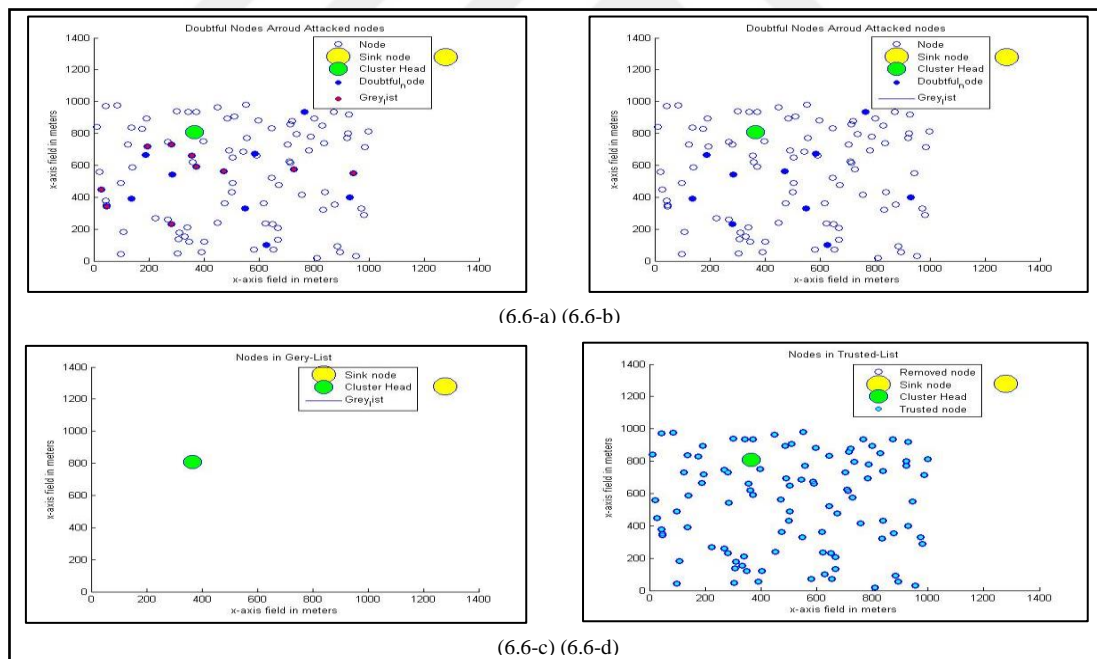


Figure 6.6. Scenario (4) Jamming attack and doubtful neighbors for enhanced algorithm

Fig (6.6-a) shows assumed cluster contents sink node, cluster head, nodes represented by empty circles, attacked nodes represented by red circles and solid blue one are the randomly selected doubtful nodes around attacked nodes. Doubtful nodes

may lie in ahead of distance lists that related to attacked nodes. If so, when CH tries to utilize nodes in distance lists, it takes first and nearest neighbor to a certain attacked node. If doubtful node selected to communicate with attacked node, proof endorsement also delayed due to active jamming attack. Therefore enhanced algorithm will bypass that doubtful node and select another one in distance list. This process keep continuing till safe and trusted node selected to complete a successful data transfer and not affected by jamming attack. As an expected result, as in fig(6.6-c), after a complete authentication phase grey list is empty and all attacked nodes been authenticated correctly for further report endorsement by transferring them to trusted list which shown in fig (6.6-d).

6.5.5 Scenario (5)

In addition to previously tested parameters, another one will added to test the ability of enhanced algorithm to detect double attacked nodes. Double attacked nodes mean that certain node is under jamming attack and while authentication process it detected as attacked with other type of DOS attack like compromised by other node and injects false endorsement. This facility gives an extra advantage to enhanced algorithm in addition to its proved and tested abilities.

Added parameter represents a percentage of attacked node considered as double attacked. These nodes changes the contents of endorsement and provides false Hash value for that endorsement.

Testing scenario inputs

```
num_of_nodes = 100 nodes
jamming_state = 'Yes'
attack_percentage = 10 %
defense_level = 2
doubtful_percentage = 10 %
fals_injecting_node_percentage = 40% (of attacked nodes)
```

Testing scenario results

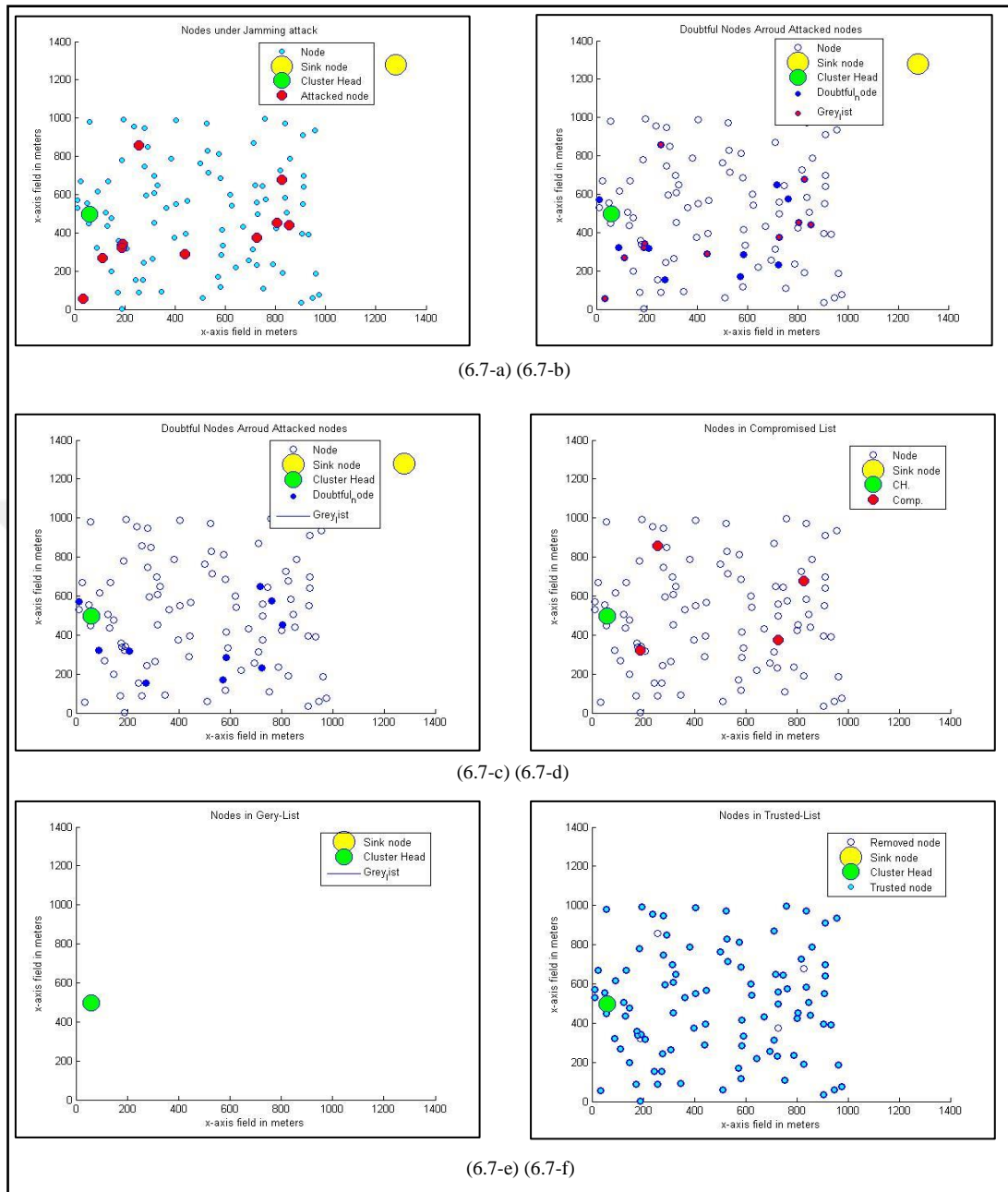


Figure 6.7. Scenario (5) Jamming attack and doubtful neighbors for enhanced algorithm

Figure (6.7) shows the behavior of enhanced algorithm against all situations that proposed in six previously mentioned input parameters. In this scenario, fig(6.7-a) shows the cluster structure with nodes under jamming attack that algorithm tries to authenticate them. Fig(6.7-b) combines between attacked nodes and doubtful nodes

around attacked ones before authentication process, while fig (6.7-c) shows the results after authentication process completed where doubtful nodes were allocated and bypassed if they were appeared in distance list of a certain attacked node.

Fig (6.7-d) shows the compromised list contents which were the nodes affected by both jamming attack and other kind of DOS attack. In this theses, injecting false Hash values considered as a second type of DOS attack. These nodes removed from grey list then added to compromised list for further attack defense techniques to be applied.

Fig (6.7-e) and fig (6.7-f) shows the final expected results where grey list should be empty and all healthy nodes are in trusted list and prepared for further report endorsements.

6.5.6 Scenario (6)

Another test to find the ability of enhanced algorithm to authenticate attacked nodes collected in a regional form with a certain radius of jamming attack effect.

Testing scenario inputs

```
num_of_nodes = 500 nodes  
jamming_state = 'Yes'  
attack_state = 'region'  
defense_level = 2  
doubtful_percentage = 0 %  
fals_injecting_node_percentage = 0% (of attacked nodes)
```

Testing scenario results

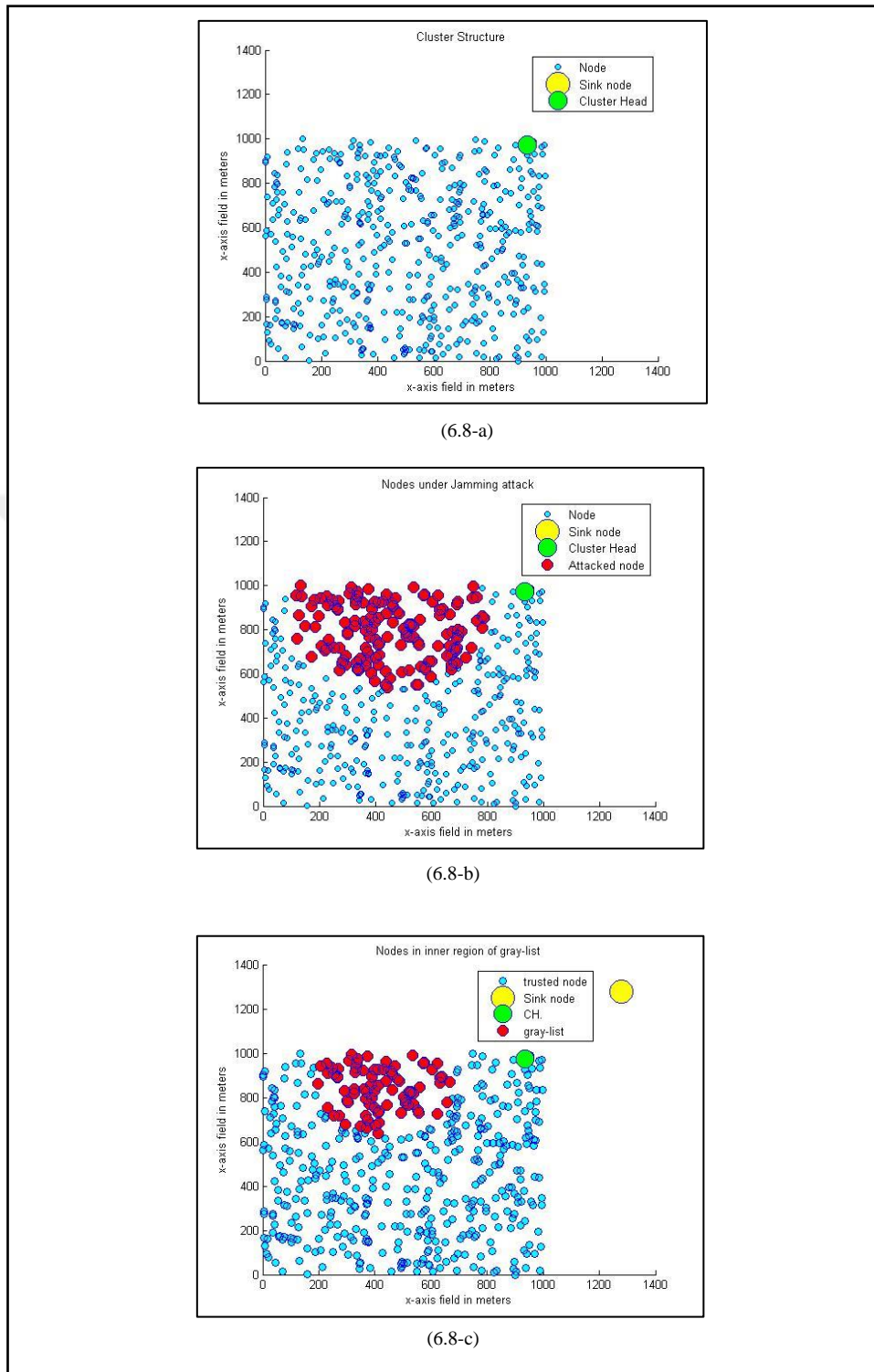


Figure 6.8. Scenario (6) Jamming attack and regionally attacked nodes

Figure (6.8) shows the behavior of enhanced algorithm against attacking form of a regional attack that makes attacked nodes collected in single region assuming that cluster head is far away from that region. In this scenario, fig(6.8-a) shows the structure of tested WSN which consist of 500 nodes.

In fig(6.8-b), a region of attacked node appears among trusted nodes. This region selected by electing a node randomly to be the center of attacked region with a certain radius of jamming attack effect.

Fig(6.8-c) shows the contents Gray-list after authentication process. It is clearly appeared that the algorithm authenticated only nodes lies on the boundary of attacked region which have safe neighbors with no barrier prevents sending proof endorsement to them. On the other hand nodes that lies inside the region did not authenticated depending on same authentication strategy.

CHAPTER VII

CONCLUSION AND FUTURE WORK

7.1 Conclusion

Among wide variety of WSN research fields like deployment techniques, construction of topologies methods, the focusing point of this thesis is upon security field of WSN. Security has also a wide range of issues to be treated. So, DOS attack selected to study it depending on several previous studies. This thesis interested in mitigating the False Node Exclusion DOS (FNEDOS) due to continues effective Jamming attack that prevents transferring messages between nodes and cluster head. The proposed enhancement method provides a solution for original False Endorsement DOS (FEDOS) method limitation which caused false excluding innocent nodes from being participant of endorsing cluster head broadcasted reports. The enhancement done by developing an algorithm helps cluster head to deliver attacked node's endorsement via safe multi path possibilities by utilizing safe nearest neighboring nodes under full control of cluster head CH. If attacked node tries to broadcast it's endorsement as alternative solution, this method is not applicable due to system assumptions by original and enhanced algorithms because attacked node do not know that it under jamming attack, broadcasting causes a sensitive data disclosure especially for other adversary nodes and this broadcasting causing higher power dissipation which leads attacked node to reach die state faster.

The obtained results of testing enhancement algorithm functionality matches the expected ones, via applying several test case scenarios to proof enhancement algorithm ability of mitigating False Exclusion of nodes under jamming attack against original one as illustrated in chapter (6). Therefore mitigation is achieved

successfully except in case of attacking a region of nodes as in testing scenario(6) which is an open issue.

7.2 Future Work

As a future work, there are several possible approaches to develop the enhanced FNEDOS algorithm. First possibility is to develop an energy balancing method which is needed to reduce power consumption due to extra communication processes to keep cluster nodes functioning as longest time as possible. Secondly, utilizing AI algorithms to develop optimum path selection between attacked nodes and cluster head especially when multi hop path considered. Third possibility is to apply the same enhanced algorithm to movable sensor nodes. To avoid the effect of regional attacking possibility, a combination of Artificial Intelligent algorithms and consideration of multi-channel communication may be taken as a future work to solve this open issue.

RESOURCES

- [1]. Delphine Christin, Andreas Reinhardt, Parag S. Mogre, Ralf Steinmetz, "***Wireless Sensor Networks and the Internet of Things: Selected Challenges***", Multimedia ommunications Lab, Technische Universit"at Darmstadt Merckstr. 25, 64283 Darmstadt,Germany,{delphine.christin,reas.reinhardt,parag.mogre,ralf.steinmetz}@kom.tu-darmstadt.de.
- [2]. Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar, Eui-Nam Huh "***Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved***", Innovative Cloud and Security Lab, Department of Computer Engineering Kyung Hee University, Suwon, South Korea. 2Dept. of Wireless Networks and Multimedia Services, Institut Minés-Télécom, Télécom SudParis, 91011 Evry Cedex, France, imran@ieee.org, {aazam1, aymen3, johnhuh4}@khu.ac.kr.
- [3]. Pengfei You, Yuxing Peng, Hang Gao," ***Providing Information Services for Wireless Sensor Networks through Cloud Computing***", National Key Laboratory for Parallel and Distributed Processing, School of Computer Science, National University of Defense Technology,Changsha, China {hbypf, pengyuxing1963, hanggao1821}@yahoo.com.cn
- [4]. A. Flammini, E. Sisinni, "***Wireless Sensor Networking in the Internet of Things and Cloud Computing Era***",*Department of Information Engineering, University of Brescia, via Branze 38, Brescia (25123), Italy*, EUROSENSORS 2014, the XXVIII edition of the conference series.
- [5]. Chiara Buratti 1; Andrea Conti 2, Davide Dardari 1 and Roberto Verdone 1, "***An Overview onWireless Sensor Networks Technology and Evolution***", Author to whom correspondence should be addressed; E-Mail: c.buratti@unibo.it; *Received: 25 July 2009; in revised form: 24 August 2009 / Accepted: 25August 2009.*

- [6]. I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, "**Wireless sensor networks: a survey**", Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA, Received 12 December 2001; accepted 20 December 2001.
- [7]. S. Prasanna, Srinivasa Rao, "**An Overview of Wireless Sensor Networks Applications and Security**", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.
- [8]. Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal, "**Issues and Challenges in Wireless Sensor Networks**", CSE & IT Department, BBSB Engineering College, Fatehgarh Sahib, India, sukhwinder.sharma@bbsbec.ac.in, Department of ECE,GZSPTU Campus, Bathinda, India, drakeshbansal@gmail.com, ECE Department, GZSPTU Campus, Bathinda, India, savina.bansal@gmail.com, International Conference on Machine Intelligence Research and Advancement 2013.
- [9]. Parli B. Hari¹, Dr. Shailendra Narayan Singh², "**Security Issues in Wireless Sensor Networks: Current Research and Challenges**", 1. Research Fellow, Department of CSE, ASET, Amity University Uttar Pradesh, INDIA, 2. Associate Professor, Department of CSE, ASET, Amity University Uttar Pradesh, INDIA.
- [10]. Anton Hergenroeder_ and Jens Hornebery, "**Facing Challenges in Evaluation of WSN Energy Efficiency with Distributed Energy Measurements**", Institute of Telematics, Karlsruhe Institute of Technology, 76128 Karlsruhe, Germany, E-mail: _hergenroeder@kit.edu, yhorneber@kit.edu
- [11]. S. Prasanna, Srinivasa Rao, "**An Overview of Wireless Sensor Networks Applications and Security**", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.
- [12]. Mohamed-Lamine Messai, "**Classification of Attacks in Wireless Sensor Networks**", International Congress on Telecommunication and Application' 14, University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014, Doctoral school in computer science, university of Bejaia, Algeria, Networks & Distributed Systems Laboratory, UFAS, Setif, Algeria, messai.amine@gmail.com.

- [13]. Parli B. Hari¹, Dr. Shailendra Narayan Singh², "***Security Issues in Wireless Sensor Networks: Current Research and Challenges***", 1. Research Fellow, Department of CSE, ASET, Amity University Uttar Pradesh, INDIA, 2. Associate Professor, Department of CSE, ASET, Amity University Uttar Pradesh, INDIA.
- [14]. Payam Porkar rezaeiye¹, Maysam gharghi², Sassan payehdar³, Jasem torfi⁴, Hamidreza hajiaghai⁵, and Pasha Porkar Rezaeiye⁶, "***Types of Attacks Penetrating Wireless Sensor Networks and Strategies to Overcome Them***", International Conference Data Mining, Civil and Mechanical Engineering (ICDMCME'2015) Feb. 1-2, 2015 Bali (Indonesia).
- [15]. Christiana Ioannou and Vasos Vassiliou, "***The Impact of Network Layer Attacks in Wireless Sensor Networks***", Department of Computer Science, University of Cyprus, 75 Kallipoleos Street, CY-1678, Nicosia, Cyprus, Email: cioannou@cs.ucy.ac.cy, vasosv@cs.ucy.ac.cy.
- [16]. Ren Junn Hwang, Yan Zhi Huang, "***Secure Data Collection Scheme for Wireless Sensor Networks***", Department of Computer Science and Information, Engineering TamKang University, New Taipei City, Taiwan, e-mail: junhwang@ms35.hinet.net, Department of Computer Science and Information, Engineering, Tam Kang University, New Taipei City, Taiwan, 2017 31st International Conference on Advanced Information Networking and Applications Workshops.
- [17]. Furrakh Shahzad¹, Maruf Pasha², Arslan Ahmad², "***A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures***", (1Department of Computer Science, Pakistan Institute of Engineering and Technology, Multan 60000, Pakistan), (2Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan), farrukhshahzad@piet.edu.pk, aruf.pasha@bzu.edu.pk, arslan_ahmad91@yahoo.com, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12, December 2016.
- [18]. Fei Wang^{1,2}, Yujun Zhang¹, Yongjun Xu¹, Lin Wu^{1,2}, Boyu Diao^{1,2}, "***DoS-Resilient Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks***", Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China, 2University of Chinese Academy of Sciences, Beijing 100049, China, Email:{ wangfei, zhunj, xyj, wulin, diaoboyu2012}@ict.ac.cn.

- [19]. Ouyang Xi^{1,2}, Tian Bin^{1,2}, Li Qi^{1,2}, Zhang Jian-yi^{1,2}, Hu Zheng-Ming¹, Xin Yang^{1,2}, "*A Novel Framework of Defense System Against DoS Attacks in Wireless Sensor Networks*", 1. Information Security Center, Beijing University of Posts and telecommunications 2. Beijing Safe-Code Technology Co.,Ltd.
- [20]. Arazil², H. Qi¹, D. Rosel, "*A Public Key Cryptographic Method for Denial of Service Mitigation in Wireless Sensor Networks*", 1-Department of Electrical and Computer Engineering University of Tennessee Knoxville, TN 37996-2100 2-Cyberspace Sciences & Information Intelligence Research Group (CSIIR) Oak Ridge National Laboratory Oak Ridge, TN 37831-6418.
- [21]. Khusvinder Gill, Shuang-Hua Yang, "*A Scheme for Preventing Denial of Service Attacks on Wireless Sensor Networks*", Department of Computer Science, Loughborough University Loughborough, Leicestershire, LE11 3TU, United Kingdom, k.gill@lboro.ac.uk, s.h.yang@lboro.ac.uk.
- [22]. Christoph Krauß, Markus Schneider, and Claudia Eckert, "*An Enhanced Scheme to Defend against False-Endorsement-Based DoS Attacks in WSNs*", Technische Universität Darmstadt, Darmstadt, Germany, {krauss, eckert}@sec.informatik.tu-darmstadt.de, Fraunhofer Institute for Secure Information Technology (SIT), Darmstadt, Germany, markus.schneider@sit.fraunhofer.de.
- [23]. Kihong Kim, linkeun Hongt, "*Analysis of Power Consumption of S-MAC Protocol According to DoS Attack*", The Attached Institute of ETRI, P. O. Box 1, Yuseong, Daejeon, 305-600, Korea, Email: hong0612@hanmir.com, tDivision of Information & Communication Engineering, Baekseok University, 115, Anseo-dong, Cheonan-si, Chungnam, 330-740, Korea, Email: jkhong@bu.ac.kr.
- [24]. Kashif Sagha, William Henderson, David Kendall, Ahmed Bouridane, "*Applying Formal modelling to detect DoS attacks in wireless medium*", School of Computing, Engineering and Information Sciences, Northumbria University, Pandon Building, Newcastle upon Tyne NE2 1XE, United Kingdom, College of Computer and Information Sciences, King Saud University, P.O.Box 51178 Riyadh 11543, Kingdom of Saudi Arabia kashif.saghar@unn.ac.uk.

- [25]. Paolo Ballarini¹, Lynda Mokdad^{2*}, Quentin Monnet², "***Modeling tools for detecting DoS attacks in WSNs***", ¹ Laboratoire MAS, École Centrale de Paris, Chatenay-Malabry, France, ² Laboratoire LACL, Université Paris-Est, Créteil, France, Published online 14 February 2013 in Wiley Online Library (wileyonlinelibrary.com).
- [26]. Rajani Muraleedharan and Lisa Ann Osadciw, "***Cross Layer Denial of Service Attacks in Wireless Sensor Network Using Swarm Intelligence***", Department of Electrical Engineering and Computer Science Syracuse University, yracuse, NY- 13244-1240, Phone: 315-443-3366/Fax: 315-443-2583, rmuralee/laosadci@syr.edu.
- [27]. Qijun Gu, Peng Liu, "***Denial of Service Attacks***", PhD. Assistant Professor Department of Computer Science Texas State University – San Marcos, San Marcos, TX, 78666, PhD. Associate Professor, School of Information Sciences and Technology Pennsylvania State University University Park, PA, 16802.
- [28]. Mihui Kim, Inshil Doh and Kijoon Chae, "***Denial-of-Service(DoS) Detection through Practical Entropy Estimation on Hierarchical Sensor Networks***", Department of Computer Science and Engineering, Ewha Womans University, 11-1 Daehyun-dong, Seodaemun-gu, Seoul, 120-750, Korea.
- [29]. David R. Raymond, Scott F. Midkiff, "***Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses***", PERVASIVE computing Published by the IEEE CS n 1536-1268/08/\$25.00 © 2008 IEEE.
- [30]. D. Mansouri, L. Mokdad, Jalel Ben-othman, M. Ioualalen, "***Detecting DoS attacks in WSN based on Clustering Technique***", Laboratoire LSI, USTHB, Algeria, mansouri.dj@gmail.com, Laboratoire LACL, University of Paris-Est, lynda.mokdad@u-pec.fr, Laboratoire L2TI, University of Paris13 jalel.ben-othman@univ-paris13.fr, Laboratoire LSI, USTHB, Algeria, mioualalen@usthb.dz.
- [31]. Heng Zhang¹, Yifei Qi², Junfeng Wu³, Lingkun Fu², and Lidong He², "***DoS Attack Energy Management Against Remote State Estimation***", IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, VOL., NO., MONTH 2016.

- [32]. Malek Guechari, Lynda Mokdad, Sovanna Tan, "*Dynamic Solution for Detecting Denial of Service Attacks in Wireless Sensor Networks*", Laboratoire LACL, University of Paris-Est, Créteil, guechari.malek@gmail.com, Lynda.mokdad@u-pec.fr, sovanna.tan@u-pec.fr, IEEE ICC 2012.
- [33]. Quentin MONNET, Lynda MOKDAD, Jalel BEN-OTHMAN, "*Energy-balancing method to detect denial of service attacks in wireless sensor networks*", Lab. LACL, Université Paris-Est, LACL (EA 4219), UPEC, F-94010 Créteil, France, quentin.monnet@lacl.fr, Lab. LACL, Université Paris-Est, LACL (EA 4219), UPEC, F-94010 Créteil, France, lynda.mokdad@u-pec.fr, Lab. L2TI, Université Paris 13, L2TI (EA 3043), P13, F-93430 Villetaneuse, France, jbo@univ-paris13.fr.
- [34]. Chakib BEKARA, Maryline LAURENT-MAKNAVICIUS, Kheira BEKARA, "*H2BSAP: A Hop-by-Hop Broadcast Source Authentication Protocol for WSN to mitigate DoS Attacks*", INSTITUT TELECOM, TELECOM&MANEGEMENT Sud-Paris, CNRS Samovar UMR 5157, 9 rue Charles Fourier, 91000 Evry, FRANCE, chakib.bekara, maryline.maknavicius, kheira.bekara}@it-sudparis.eu.
- [35]. Anthony D. Wood, John A. Stankovic, "*A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks*", Department of Computer Science, University of Virginia, fwood, stankovicg@cs.virginia.edu.
- [36]. Shahriar Mohammadi¹, Reza Ebrahimi Atani², Hossein Jadidoleslami³, "*A Comparison of Link Layer Attacks on Wireless Sensor Networks*", ¹Department of Industrial Engineering, K. N. Tossi University of Technology, Tehran, Iran, ², Department of Computer Engineering, University of Guilan, Rasht, Iran, ³Department of Information Technology, Anzali International Branch, The University of Guilan, Rasht, Iran, Email: smohammadi40@yahoo.com, rebrahimi@guilan.ac.ir, tanha.hossein@gmail.com, Journal of Information Security, 2011, 2, 69-84.
- [37]. Michael Riecker, Daniel Thies and Matthias Hollick, "*Measuring the Impact of Denial-of-Service Attacks on Wireless Sensor Networks*", Secure Mobile Networking Lab, Technische Universität Darmstadt Mornwegstr. 32, 64293 Darmstadt, Germany, fmichael.riecker,daniel.thies,matthias.hollickg@seemoo.tu-darmstadt.de.

- [38]. Chakib BEKARA, Maryline LAURENT-MAKNAVICIUS, Kheira BEKARA, "*Mitigating Resource-draining DoS attacks on Broadcast Source Authentication on Wireless Sensors Networks*", INSTITUT TELECOM, TELECOM&MANEGEMENT Sud-Paris, CNRS Samovar UMR 5157, 9 rue Charles Fourier, 91000 Evry, FRANCE, fchakib.bekara, maryline.maknavicius, kheira.bekarag@it-sudparis.eu.
- [39]. Iman Almomani, Bassam Al-Kasasbeh, "*Performance Analysis of LEACH protocol under Denial of Service Attacks*", College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia, imomani@pscw.psu.edu.sa, Computer Science Department, King Abdullah II School for Information Technology (KASIT), The University of Jordan, Amman 11942, Jordan bassamkasasbeh@yahoo.com. 2015 6th International Conference on Information and Communication Systems (ICICS).
- [40]. Lynda Mokdad, Jalel Ben-Othman, "*Performance evaluation of security routing strategies to avoid DoS attacks in WSN*", Laboratoire LACL, University of Paris-Est, Creteil, Lynda.mokdad@u-pec.fr, Laboratoire L2TI, University of Paris 13, jalel.ben-othman@univ-paris13.fr.
- [41]. Djamel Mansouri, Lynda Mokddad, Jalel Ben-othman, Malika Ioualalen, "*Preventing Denial of Service Attacks in Wireless Sensor Networks*", Laboratoire MOVEP, USTHB, Algeria, ansouri.dj@gmail.com, Laboratoire LACL, University of Paris-Est, lynda.mokdad@u-pec.fr, Laboratoire L2TI, University of Paris13, jalel.ben-othman@univ-paris13.fr, Laboratoire MOVEP, USTHB, Algeria, mioualalen@usthb.dz, IEEE ICC 2015.
- [42]. S. Fouchal¹, D. Mansouri², L. Mokdad², M. Ioualalen³, "*Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks*", 1SAF Laboratory, Paris, France, 2LACL Laboratory, Créteil, France, 3LSI Laboratory, Algiers, Algeria, INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, *Int. J. Commun. Syst.* 2015; **28**:309–324, Published online 3 October 2013 in Wiley Online Library, (wileyonlinelibrary.com). DOI: 10.1002/dac.2670.
- [43]. Prosanta Gope, Jemin Lee, Tony Q. S. Quek, "*Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks*", Member, IEEE, Senior Member, IEEE, IEEE SENSORS JOURNAL, VOL. 17, NO. 2, JANUARY 15, 2017.

- [44]. K. Gill¹ S.-H., Yang¹ W. Wang², "*Scheme for preventing low-level denial-of-service attacks on wireless sensor network-based home automation systems*", ¹Computer Science Department, Loughborough University, Loughborough, England, LE11 3TU, UK, ²College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, Peoples Republic of China.
- [45]. Jiang Zhongqiu, Yan Shu, Wang Liangmin, "*Survivability Evaluation of Cluster-Based Wireless Sensor Network under DoS Attacks*", School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China, jiangzq@ujs.edu.cn, yanshu@ujs.edu.cn, wlm.xidian@gmail.com.
- [46]. ZHANG Yi-ying^{1,2}, LI Xiang-zhen³, LIU Yuan-an¹, "*The detection and defense of DoS attack for wireless sensor network* ", 1. Beijing University of Posts and Telecommunications, Beijing 100876, China, 2. State Grid Information & Telecommunication Company Ltd., Beijing 100761, China, 3. State Grid Electric Power Research Institute, Nanjing 210003, China, October 2012, 19(Suppl. 2): 52–56, www.sciencedirect.com/science/journal/10058885.
- [47]. S.Uma maheswari, N.S.Usha E.A.,Mary Anita, K.Ramaya Devi, "*A Novel Robust Routing Protocol RAEED to Avoid DoS Attacks in WSN*", ME (CSE) student S.A Engineering College,Associate Professor, Professor, Assistant Professor, S.A Engineering College, Chennai Chennai, uthra276@gmail.com sushak3001@yahoo.co.in, drmaryanita@saec.ac.in, ramyadevik@saec.ac.in
- [48]. Munish Dhar¹, Rajeshwar Singh², "*A Review of Security Issues and Denial of Service Attacks in Wireless Sensor Networks*", ¹Dept. of ECE, DIET Kharar, Punjab, India., ²Dept. of ECE, Doaba Khalsa Trust Group of Institution Nawanshahar, Punjab, India.
- [49]. Dr. G. Padmavathi ¹, Mrs. D. Shanmugapriya ²,"*A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks*", ¹ Prof and Head, Dept. of Computer Science, Avinashilingam University for Women, Coimbatore, India, ganapathi.padmavathi@gmail.com, ² Lecturer, Dept. of Information Technology, Avinashilingam University for Women, Coimbatore, India, ds_priyaa@rediffmail.com IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

- [50]. Aditi Rani, Sanjeet Kumar, "***A Survey of security in Wireless Sensor Networks***", Aditi Rani, Sanjeet Kumar Department of Electronics and Communication Engineering BIT Mesra, Ranchi, Jharkhand, India, aditi9582@gmail.com, sanjeet@bitmesra.ac.in, 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).
- [51]. Sunil Ghildiyal, Bhupender Singh Rautela, Anupam Semwal, "***Denial of Service (DoS) Attacks at Network Layer in WSN***", Uttaranchal University Dehradun Uttarakhand, Graphic Era University Dehradun Uttarakhand, Drona College of Mgmt & Tech. Ed. Dehradun Uttarakhand, *Int. Journal of Engineering Research and Applications* www.ijera.com, ISSN: 2248-9622, Vol. 5, Issue 11, (Part - 1) November 2015, pp.86-89.
- [52]. Manju V.c, Sasi Kumar M., "***Detection of Jamming Style DoS attack in Wireless Sensor Network***", Kerala University, Trivandrum, Kerala, India, manju_tvm@yahoo.com, Kerala University, Trivandrum, Kerala, India, drmsasikumar@yahoo.com, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.
- [53]. Poonam Rolla, Manpreet Kaur, "***Dynamic Forwarding Window Technique against DoS Attack in WSN***", Department of CSE, GZS Campus College of Eng & Tech, Bathinda, India,
- [54]. poonamrolla2@gmail.com, Department of CSE, GZS Campus College of Eng & Tech, Bathinda, India
- [55]. sahez6548@gmail.com, 2016 International Conference on Micro-Electronics and Telecommunication Engineering.
- [56]. Yu Jiang¹, Jie Huang¹, Wen Jin², "***INTRUSION TOLERANCE SYSTEM AGAINST DENIAL OF SERVICE ATTACKS IN WIRELESS SENSOR NETWORK***", ¹Information Science and Engineering School Southeast University, Nanjing, China, jiangyu@seu.edu.cn, jhuang@seu.edu.cn, ²The 28th Research Institute of CETC, Nanjing, China, jinwen2046@gmail.com.
- [57]. K. Nirmal Raja & M. Marsaline Beno, "***On securing Wireless Sensor Network-Novel authentication scheme against DOS attacks***", Received: 17 October 2013 /Accepted: 6 June 2014 /Published online: 9 August 2014, # Springer Science+Business Media New York 2014.

- [58]. Xi Luo, Yi-Ying Zhang, Wen-Cheng Yang, Myong-Soon Park, "***Prevention of DoS Attacks Based on Light Weight Dynamic Key Mechanism in Hierarchical Wireless Sensor Networks***", Department of Computer Science and Engineering Korea University, Seoul, Korea, {rosa-xi, zhangyiying, wencheng, myongsp}@ilab.korea.ac.kr, 2008 Second International Conference on Future Generation Communication and Networking.
- [59]. Rajani Muraleedharan, Lisa Ann Osadciw, " ***Secure Health Monitoring Network Against Denial-Of-Service Attacks Using Cognitive Intelligence***", Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY- 13244-1240, Phone: 315-443-1319/Fax: 315-443-2583, rmuralee/laosadi@syr.edu.
- [60]. Maneesha V. Ramesh, Aswathy B. Raj and Hemalatha T., "***Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks***", Amrita Center for Wireless Networks and Applications, Amrita Vishwa Vidyapeetham, Kerala, India, maneesha@am.amrita.edu, aswathy.braj13@gmail.com, hemalatha@am.amrita.edu.
- [61]. A.Díaz, P. Sanchez J. Sancho, J. Rico, "***Wireless Sensor Network Simulation for Security and Performance Analysis***", University of Cantabria TST Sistemas {adiaz, sanchez} @teisa.unican.es, {jsancho, jrico} @tst-sistemas.es.