

A MULTI-LAYER APPROACH FOR DETECTION OF
SELECTIVE FORWARDING ATTACKS IN WIRELESS
SENSOR NETWORKS

Naser Alajmi

Under the Supervision of Dr. Khaled Elleithy

DISSERTATION

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

AND ENGINEERING

THE SCHOOL OF ENGINEERING

UNIVERSITY OF BRIDGEPORT

CONNECTICUT

November, 2016






A MULTI-LAYER APPROACH FOR DETECTION OF
SELECTIVE FORWARDING ATTACKS IN WIRELESS
SENSOR NETWORKS

Naser Alajmi

Under the Supervision of Dr. Khaled Elleithy

Approvals

Committee Members

Name	Signature	Date
Professor Dr. Khaled Elleithy		11/21/16
Professor Dr. Navarun Gupta		11/18/16
Professor Dr. Xingguo Xiong		11/18/2016
Professor Dr. Hassan Bajwa		11/18/16
Professor Dr. Mohsen Guizani		11/28/2016

Ph.D. Program Coordinator

Dr. Khaled M. Elleithy  11/30/2016

Chairman, Computer Science and Engineering Department

Dr. Ausif Mahmood  12-5-2016

Dean, School of Engineering

Dr. Tarek M. Sobh  12-5-2016

A MULTI-LAYER APPROACH FOR DETECTION OF
SELECTIVE FORWARDING ATTACKS IN WIRELESS
SENSOR NETWORKS

© Copyright by Naser Alajmi 2016

A MULTI-LAYER APPROACH FOR DETECTION OF SELECTIVE FORWARDING ATTACKS IN WIRELESS SENSOR NETWORKS

ABSTRACT

Wireless sensor networks (WSNs) are increasingly used due to their broad range of important applications in both military and civilian domains. Security is a major threat in WSNs. WSNs are prone to several types of security attacks. Sensor nodes have limited capacities and are deployed in dangerous locations; therefore, they are vulnerable to different types of attacks, including wormhole, sinkhole, and selective forwarding attacks. Security attacks are classified as data traffic and routing attacks. These security attacks could affect the most significant applications of WSNs, namely, military surveillance, traffic monitoring, and healthcare. Therefore, many approaches were suggested in literature to detect security attacks on the network layer in WSNs.

The network layer is of paramount significance to the security of WSNs to prevent exploitation of their confidentiality, privacy, availability, integrity, and authenticity. Reliability, energy efficiency, and scalability are strong constraints on sensor nodes that affect the security of WSNs. Because sensor nodes have limited

capabilities in most of these areas, selective forwarding attacks cannot be easily detected in networks.

In this dissertation, an approach to selective forwarding detection (SFD) is suggested. The approach has three layers: MAC pool IDs, rule-based processing, and anomaly detection. It maintains the safety of data transmission between a source node and base station while detecting selective forwarding attacks. Furthermore, the approach is reliable, energy efficient, and scalable.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my advisor Dr. Khaled Elleithy for the continuous support of my Ph.D. study and related research, for his patience, motivation, and immense knowledge. Prof. Elleithy's guidance helped me in all the time of research and writing of this dissertation. I could not have imagined having a better advisor and mentor for my Ph.D. study.

Beside my advisor, I would like to thank the rest of my dissertation committee: Dr. Gupta, Dr. Xiong, Dr. Bajwa, and Dr. Guizani for their insightful comments and encouragement. Also, I would like to thank all my family members. My thanks are wholly devoted to God who has helped me all the way to complete this work successfully. I owe a debt of gratitude to my family for understanding and encouragement.

I am honored that my work has been supervised by Dr. Khaled Elleithy

TABLE OF CONTENTS

ABSTRACT	iv
ACKNOWLEDGEMENTS	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	x
LIST OF FIGURES.....	xi
CHAPTER 1: INRTODUCTION	1
1.1. Research Problem and Scope	3
1.2. Motivation behind the Research.....	5
1.3. Potential Contribution of the Proposed Research.....	5
CHAPTER 2: LITERATURE SURVEY FOR SECURITY ATTACKS IN WIRELESS SENSOR NETWROKS	7
2.1. Physical Layer.....	10
2.1.1. Jamming	10
2.1.2. Tampering	11
2.2. Data Link Layer	11
2.2.1. Collision	11
2.2.2. Medium Access Control (MAC)	11
2.3. Transport Layer.....	12
2.3.1. Flooding	12
2.3.2. De-Synchronization Attack	12

2.4. Application Layer.....	13
2.5. Network Layer.....	13
2.5.1. Spoofing or Replaying Information.....	14
2.5.2. Sinkhole Attack	14
2.5.3. Sybil Attack.....	15
2.5.4. Wormhole Attack	15
2.5.5. HELLO Flood Attack	16
2.6. Selective Forwarding Detection Techniques	18
2.6.1. Selective Forwarding Scheme using Multi-Hop LWSS	18
2.6.2. Selective Forwarding Scheme using Two-Hop LWD	23
2.6.3. Selective Forwarding Scheme using Watermark Technique SDT	25
2.6.4. Selective Forwarding Scheme using Extra Monitor RSSI-EM.....	26
2.7. Selective Forwarding Detection Evaluation.....	27
CHAPTER 3: MULTI LAYER APPROACH FOR DETECTION OF SELECTIVE FORWARDING ATTACKS	33
3.1. Selective Forwarding Detection (SFD) using Multi-Layer	34
3.1.1. MAC Pool IDs Layer	36
3.1.2. Rules Processing Layer	37
3.1.3. Anomaly Detection Layer Based on Intrusion Detection System	39
3.2. Reliable, Energy efficient and Scalable (RES) Model	41
3.2.1. Reliable	41
3.2.2. Energy efficient	43
3.2.3. Scalable	46
CHAPTER 4: SIMULATION SETUP AND RESULTS	49
4.1. Simulation Setup	49

4.2. Reliable Detection	50
4.3. Energy Efficient	51
4.4. Scalability Ratio	55
4.5. Probability	57
4.6. Packet Delivery Ratio.....	61
4.7. Detection of Selective Forwarding Attack Average	63
4.8. Throughput Average	65
4.9. Accuracy Rate	67
4.10. Time Delay	67
CHAPTER 5: CONCLUSION	70
REFERENCES.....	72
APPENDIX A: PUBLICATIONS	79

LIST OF TABLES

Table 1: Selective Forwarding Attack Analysis	30
Table 2: Selective Forwarding Attack Detection Analysis.....	31
Table 3: Selective Forwarding Attack Detection Approaches Comparison	31
Table 4: Detection Approaches Analysis.....	32
Table 5: Rules Processing.....	39
Table 6: Simulation Setup.....	49

LIST OF FIGURES

Figure 1: Sensor Architecture	3
Figure 2: Taxonomy of Security Attacks.....	10
Figure 3: An example for the monitor node gets the attacker-Redrawn [32]	19
Figure 4: Suspect nodes Identification-Redrawn [33]	21
Figure 5: An example of multi-hop acknowledgement with ACK_Span=3, ACK_TTL=6. - Redrawn [33]	22
Figure 6: Illustration of monitor node-Redrawn [34]	25
Figure 7: Energy consumption.....	28
Figure 8: Average throughput.....	29
Figure 9: Reliable detection rate	29
Figure 10: Scalability ratio.....	30
Figure 11: Multi-Layer Approach.....	35
Figure 12: Selective Forwarding Detection (SFD) Flowchart.....	36
Figure 13: Selective Forwarding Detection-SFD Multi-Layers	41
Figure 14: Reliable Detection Rate of SFD Approach	43
Figure 15: Energy Consumption of SFD Approach	46
Figure 16: Scalability Ratio of SFD Approach.....	48
Figure 17: Reliable Detection Rate of Selective Forwarding Attack	50
Figure 18: Energy Consumption of Selective Forwarding Attack (No Mobility Node)	51
Figure 19: Energy Consumption of Selective Forwarding Attack (20% Mobility Node).....	52
Figure 20: Energy Consumption of Selective Forwarding Attack.....	53

Figure 21: Energy Consumption of Selective Forwarding Attack.....	54
Figure 22: Energy Consumption of Selective Forwarding Attack.....	55
Figure 23: Scalability Ratio (10% Malicious Node).....	56
Figure 24: Scalability Ratio (25% Malicious Node).....	57
Figure 25: Probability Detection of Selective Forwarding Attack (No Mobility Node)	58
Figure 26: Probability Detection of Selective Forwarding Attack (25% Mobility Node).....	59
Figure 27: Probability Detection of Selective Forwarding Attack (50% Mobility Node).....	60
Figure 28: Packet Delivery Ratio (No Mobility Node)	61
Figure 29: Packet Delivery Ratio (50% Mobility Node).....	62
Figure 30: Detection of Selective Forwarding Attack (No Mobility Node).....	63
Figure 31: Detection of Selective Forwarding Attack (25% Mobility Node)	64
Figure 32: Average Throughput.....	65
Figure 33: Average Throughput.....	66
Figure 34: Accuracy Rate	67
Figure 35: Time Delay	68
Figure 36: Time Delay	69

CHAPTER 1: INTRODUCTION

Wireless sensor networks contain numerous sensors. These sensors communicate with a vast number of small nodes via radio links. Sensor networks have a source and a base station. The base station controls the sensor networks. They have the ability to collect sensor data and send it to the base station. All data flows between the nodes and ends at the base station. Nodes are densely deployed [1]. The positions of the nodes do not need to be predetermined. Sensor nodes are deployed in high-risk areas. The majority of WSN protocols do not have the security to prevent simple attacks on the nodes [2].

The security of wireless sensor networks has been extensively investigated over the past few years. WSNs are susceptible to many types of attacks because they serve as an open network with limited resources of nodes. Therefore, the obstacles to securing a wireless sensor network comprise the main disadvantage for all devices. The sensor networks vulnerable to different types of security threats from attackers at most layers of the networks. The most conventional threats to the security of wireless sensor networks include eavesdropping, node compromised, interrupt, modify or inject malicious packets, compromised privacy and denial of service attacks [3]. Sensor node can be simply compromised in contrast with wired networks. A common attack in a WSN is a DoS attack; the primary objective of the attacker in a DoS attack is to make

WSNs unavailable for users [4]. In a DoS attack, the energy efficient protocols serve as targets in wireless sensor networks. Sensor nodes are liable to physical capture. Because the use of a sensor node as a target is inexpensive, tamper-resistant hardware is unlikely to take over. The denial of a service attack can be affected by draining the energy of sensor nodes to prevent sensor nodes from receiving authentic messages. Even with physical damage to sensor nodes, which have rendered a network inaccessible, the goal of the attacks is to disrupt the network during the transfer of data [5]. The majority of studies about WSNs can be classified as follows [6]:

- Key Management: Establishing and maintaining cryptographic keys in an energy efficient manner to enable encryption and authentication.
- Secure Routing: Discovering new protection techniques and applying them to new routing protocols without sacrificing network connectivity, coverage or scalability.
- Secure Services: Includes specialized security services such as data aggregation, localization and time synchronization.

Wireless sensor networks are emerging as a central new stage in the information technology ecosystem and an area of active research involving hardware and system design networking, distributed algorithms, programming models, data management, security and social factors [7], [8]. Wireless sensor networks are widely employed in the area that would insure a specific task.

Network layer is subjected many routing protocols for instance, Flat routing, and hierarchal routing. The simple function of the routing protocol is to find the reliability path. Data aggregation is used in flat routing. It a set of automated methods combining

the data that comes from sensor nodes into a set of relevant information and exclude the duplication [4]. LEACH is a popular hierarchy routing protocol [5]. It separates the network into clusters and randomly and selects the cluster head to do the routing function from cluster to the base station. A network layer in WSNs is subjected to many types of attacks. Furthermore, a sensor node may acquire advantages of multi-hop by simply refusing to route packets. Therefore, it could be executed all the time with the net result.

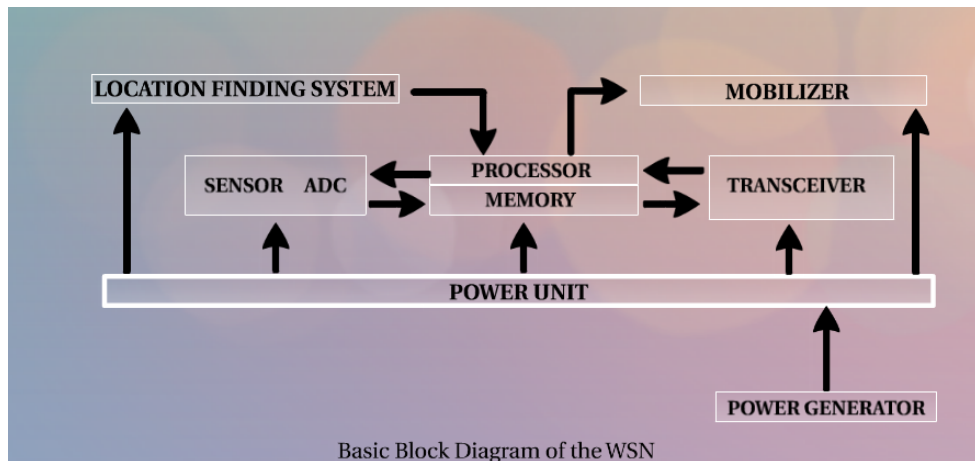


Figure 1: Sensor Architecture

1.1. Research Problem and Scope

A sensor node is a small, lightweight sensing device. It is composed of a constrained processing unit and small amount of memory for its small operating system as shown in Figure1. Additionally, a sensor node includes a limited-range transceiver and a battery unit [1]. It also includes a mobility subsystem. WSNs manage thousands of sensor nodes. In fact, these sensor nodes communicate with a huge number of small nodes via radio links. Sensor nodes in a network gather data that are necessary to

include in a smart network environment. These environments include homes, transportation systems, military installations, healthcare systems, and buildings.

Network layer is the important layer in the networks and prone many types of security attacks. The most attacks in sensor network routing are spoofing, selective forwarding, sinkhole, Sybil attack, wormhole attack, node replication attack, flooding and attack against privacy. While the communication between sensor nodes in WSNs is accomplished wirelessly by radio, adversaries can use many types of those attacks. Eavesdropping, compromising nodes, interrupting or modifying packets, and injecting malicious packets compromise privacy are threats to the security of WSNs [2]. Therefore, attackers compromise the internal sensor nodes from which they launch attacks, which are difficult to detect.

Sensor networks are vulnerable to many types of security attack. A malicious node tries to create blocks that occur while messages are being transferred between sensor nodes in the network by, for instance, forwarding a message along another path, generating an inaccurate network route, and delaying the transfer of packets between nodes. In a sensor network area, data are sent to the base station through routers. An attacker compromises the nodes by attacking the network resources. A selective forwarding attack is the one of major attacks in WSNs. It is an attack where a node send some of messages to other nodes or base station whilst drop the sensitive information. The adversary installs a malicious node in the network area, which drops packets. Once the malicious node is present in the network, it organizes routing loops that attract or refuse network traffic. In addition, malicious node can do some activities that impact to the network. These activities are such as extend or shorten source routers, generate false

messages, and attempt to drop significant messages. Packets that are dropped selectively sometime come from one node or a group of nodes. Therefore, a malicious node refuses to forward the packets. Moreover, the base station does not receive the entire message. The problem is selective forwarding attacks in network. The constraints such as reliability, energy efficient, and scalability in WSNs are challenging factors to solve. The state-of-art research in this area focuses on selective forwarding detection, reliability, energy efficient, and scalability.

1.2. Motivation behind the Research

The features of sensor nodes guarantee many applications. Therefore, applications comprise several levels of monitoring, tracking, and controlling. A group of applications is employed for specific purposes. In military applications, sensor nodes include military base, battlefield surveillance and object tracking. The military base surveillance utilized in military operations have prompted the development of WSNs. In medical applications, sensors aid in patient diagnosis and monitoring. The majority of these applications are deployed to monitor an area and react when a sensitive factor is recorded. The motives are to build a new paradigm for detecting selective forwarding attacks, extend the network lifetime by reduce the energy consumption, and the applications need to be reliable and scalable.

1.3. Potential Contribution of the Proposed Research

In this proposal, we introduce a novel data and detection protocol. The protocol's name is Selective Forwarding Detection (SFD), which contains of three multi-layers. Multi-layers framework provides longer secure surveillance for military

base, reliable path from the sender node to the base station, extends network's lifetime by reducing the energy efficient, and staying at least at the same level as the network increases larger, which is impacted to the scalable. These features enhance the network's lifetime and improve the QoS. We designed three layers including MAC pool IDs layer, rule-based processing layer, and anomaly detection layer. They maintain the safety of data transmission between a source node and base station while detecting selective forwarding attacks. Furthermore. We demonstrate the performance of the protocol by creating a military base scenario. It is simulated using Network Simulation-2 NS2. There are some assumptions to detect the selective forwarding attack within certain applications. We assume that all nodes are the same specification. All nodes in the network are having the same energy at starting point and having maximum energy. As well as, we assume that nodes are uniformly distributed in network in a random manner. Malicious nodes should not drop any packets before launching a selective forwarding attack, and an adversary cannot attack nodes during their deployment. Nodes can send data to Base station. Received Signal Strength Indicator-RSSI is the mechanism to measure the distance between the base station and node.

CHAPTER 2: LITERATURE SURVEY FOR SECURITY

ATTACKS IN WIRELESS SENSOR NETWORKS

Wireless sensor networks are very weak and susceptible to many types of security attacks on the broadcast. Security attacks are classified into two classes: passive attacks and active attacks [9]. In passive attacks, the attacker compromises data confidentiality. In active attacks, the malicious action targets data confidentiality, data integrity, and unauthorized access. In WSNs, attacks occur in two forms based on the type of hardware utilized by the attacker to compromise the network [2]: mote class attackers and laptop class attackers. Mote class attackers have access to some sensor nodes, such as regular sensor nodes. Malicious nodes are usually gained during node-compromised activities. Laptop class attackers have access to more powerful devices, such as laptops, smart phones, and workstations. The attacks can be classified into two types of attacks: outsider attacks and insider attacks. In an outsider attack, the adversary cannot gain any type of access to the network communications but the network must be pervaded before the attack can be detected. In an insider attack, the adversary gains legitimate and authorized access to the network by neighboring nodes.

A DoS attack is one of the security attacks that impacts wireless sensor networks. It is dependent on the vulnerability of each layer. A DoS attack is a multilayer attack that can launch from any layer in the network. Different types of DoS

attacks can impact sensor nodes and can also affect idle nodes or standby mode. A DoS attack comprises the main energy consumption attack in WSNs. Thus, its main focus is network resources. It can also disrupt wireless transmission and can occur either unintentionally in the form of interference, noise or collision at the receiver side or at in the context of an attack [3]. Attackers must reach certain targets, such as network access, network infrastructure, and server applications. The DoS attack attempts to drain the resources available to the victim node by transferring unnecessary data. Therefore, it prevents users from accessing services. This type of attack is intended not only for adversaries who wish to subvert, disrupt, or destroy a network but also for any event that diminishes a network's capability to provide a service [10]. Thus, a DoS attack renders a service unavailable for the users. Several types of attacks to the networks exist, such as consumption of bandwidth or processor time, disruption of service to a system or user, and disruption of physical components.

Karlof [2] noted the names of some types of DoS attacks, such as spoofed data, selective forwarding, the sinkhole attack, the Sybil attack, the wormholes attack, the hello flood attack, and acknowledgment spoofing. Therefore, DoS attacks are severe impacts on most layers of sensor networks. Because a DoS attack comprises a dangerous threat to a wireless sensor network, studies have explored various mechanisms to detect these types of attacks. The important aspect of a DoS attack is the identification of the nodes that are harmed by the adversary.

There are some methods to prevent DoS attacks such as payment for network resources, pushback, strong authentication and identification of traffic [10]. Some mechanism can be implemented to safeguard the reprogramming process, for example,

authentication flows. The choice for a DoS attack is the recreate the key request packet, which is came from the sensor node while the lifetime of the keys has expired. If the rate of recreate the key requests is frequently, the sink can conclude the occurrence of a DoS attack and drop the packet from the node for a configurable period of time [11].

Karlof and Wagner [2] have proposed a design for sensor network security and presented different types of threats in ad hoc networks that may reverse the sensor security. Arazi, Qi, and Rose have proposed a RSA based on a framework to prevent DoS attacks and ensure that malicious nodes exhaust the resources [12]. Advancements in wireless sensor networks are being achieved in several fields. Therefore, security in WSNs is an active research field [13].

Figure 2 provides denial of service for several types of attacks at different layers. At the physical layer, a DoS attack may cause jamming and tampering. At the network layer, it may cause black holes, spoofing, replying, and homing. At the link layer, it may cause collisions and unfairness. At the transport layer, it may cause flooding and de-synchronization [14].

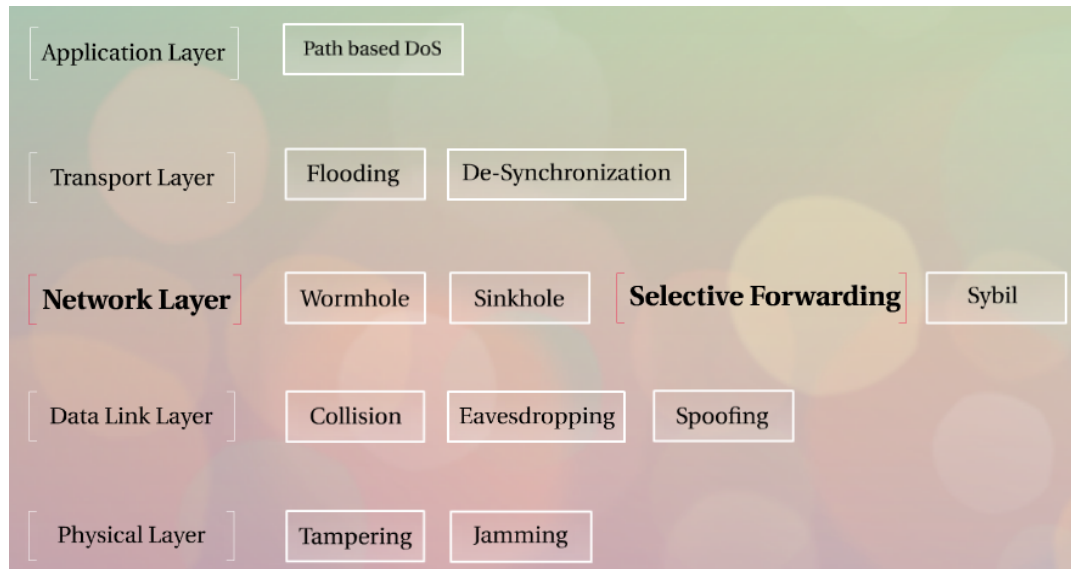


Figure 2: Taxonomy of Security Attacks

2.1. Physical Layer

The physical layer is responsible for the establishment of certain functions, such as connection, modulation, data rate, data encryption, and signal detection. In addition, a physical layer in a network may increase the reliability by reducing the path loss effect and shadowing. Attacks that affect the physical layer include jamming and tampering.

2.1.1. Jamming

Jamming is a type of DoS attack in the physical layer. Because the physical layer is responsible for frequency selection, carrier frequency generation, signal detection, and data encryption and is the lowest layer, it is the first layer to be attacked via jammers [15]. Malicious nodes use the same frequency in the network. Therefore, jamming the entire network will damage the network. An attacker attempts to transfer many packets in different paths to jam the networks. In addition, limited resources lure the adversaries to attack networks.

2.1.2. Tampering

Tampering involves circuitry or injecting fabricated code in a legitimate node. The intruder captures the node by changing its programming code. Thus, attackers may attempt to acquire sensitive information, such as the cryptography key from a node, by destroying it to gain access to a higher level of communication [16]. It affects the physical layer when the sensor nodes are unattended after deployment.

2.2. Data Link Layer

The guarantee interoperability communication between sensor nodes is the main objective of the data link layer. It is responsible for error detection, multiplexing, prevention of collision of packets and transmission. The data link layer impacts security attacks as follows:

2.2.1. Collision

A collision attack executes between two nodes during transmission in a channel. It occurs when the two nodes attempt to transmit using the same frequency. It affects all transmitted packets. The error correction code can be employed to protect the link layer from this type of attack [17].

2.2.2. Medium Access Control (MAC)

MAC layer protocols are designed for wireless sensor networks. A MAC protocol employs different algorithms to conserve battery power [18]. Using low power modes for a radio conserves the battery power when sending or receiving data. The main attack in a MAC protocol is the denial of sleep attacks. The denial of sleep attacks

is against the S-MAC protocol [19], which employ a static cycle. Sensor nodes in this protocol are organized into virtual clusters using SYNC messages. Using this protocol, radio networks will be asleep 90% of the time. The T-MAC protocol [20] is superior to the S-MAC protocol by focusing all traffic at the beginning of the period. Because it used the same SYNC technique, the technique enables nodes to transition to sleep mode. B-MAC [21] used a technique that is referred to as low-power listening (LPL). This technique is used to reduce energy consumption. G-MAC [22] is an energy efficient MAC protocol that is designed to coordinate transmissions in clusters.

2.3. Transport Layer

The main objective of the transport layer is to provide reliability and congestion. Many protocols are designed to provide these two tasks. However, they employ different techniques.

2.3.1. Flooding

Flooding attack is a problem that impacts the transport layer. The attacker establishes a connection request until resources are drained. Connection via a puzzle is a potential solution [16].

2.3.2. De-Synchronization Attack

De-synchronization is another attack in the transport layer. This attack occurs when there is connection between two endpoints. Therefore, the adversary creates inaccurate messages at the endpoints [16].

2.4. Application Layer

Collection, management and processing of the data are the main functions of the application layer. The objective of the application layer is to render the final output. Therefore, it ensures that the information flows to lower layers. The application layer consists of user data and supports many protocols, such as HTTP, FTP, SMTP, and TELNET, which provides vulnerability to attacks. The major attack in the application layer is an attack on reliability and data aggregation distortion. The adversary in this attack needs to determine the communication route to alter data using that route. In addition, the adversary creates faulty data via network connections. Therefore, sensor nodes will be harmed by the energy consumption attack when responding to the false data. Ensuring reliability acknowledgment for all received data is the main task of security to prevent attacks on reliability [23].

2.5. Network Layer

The goal of the network layer is to establish a path for efficient routing techniques. Therefore, the main function in the network layer is routing. The network layer is also responsible for some network tasks, such as routing the data between nodes, routing the data from a node to the base station, and routing data between a node and a cluster head. Several challenges at the network layer exist based on applications. These challenges include limited memory, efficiency, reliability, scalability, and energy consumption [24]. The attack of the network layer from several types of attacks impacts these challenges. Routing in the network layer may have caused one of these attacks. Consequently, most network layer attacks against sensor networks may be categorized

as one of the following attacks: spoofing or replaying information, selective forwarding, the sinkhole attack, the Sybil attack, and the wormhole attack.

2.5.1. Spoofing or Replaying Information

This type of attack directly impacts routing information. Creating routing loops, extending or shortening service routes, generating false error messages, and increasing end-to-end latency are caused by the spoofing attack [2].

2.5.2. Sinkhole Attack

One of the DoS attacks types is sinkhole attack. Sinkhole attack is a significant attack. It makes the base station to acquire the whole data and thus create a severe major threat to layer application. Sinkhole attack comprises one type of network layer attack. In addition, a compromised node sends false routing information to its neighbors to attract network traffic to itself [25]. In a sinkhole attack, the attacker's objective is to tempt the majority of the traffic from a specific location in the network via a compromised node, which generates a metaphorical sinkhole with the attacker at the center [2]. For example, when the node at the coordinator is attacked from an adversary, all other nodes follow it into the sinkhole.

The major chance in a sinkhole attack is eavesdropping. A compromised sensor node attempts to impact the information sent to it from any neighboring node. Therefore, a sensor node eavesdrops on the information is being communicated to its neighboring sensor nodes. Sinkhole attacks ordinarily function by establishing a compromised node that seems attractive to surround the nodes with regard to the routing metric. For instance, the attacker could spoof or reply to an advertisement for a

very high quality route to the base station [2]. Karlof and Wagner noted that the sensor nodes are vulnerable to the sinkhole attack based on the communication design. Some security attacks, such as selective forwarding or eavesdropping, can be started during a sinkhole attack. The malicious node or even the attacker can do anything in the network as long as the data are routed through the malicious node. WSNs are vulnerable to sinkhole attacks because many nodes transfer data to a single base station [26]. A sinkhole attack is always searching for nodes located near the base station.

2.5.3. Sybil Attack

The Sybil attack is defined as a malicious device that assumes numerous identities [27]. Malicious nodes can allege to have many identities. WSNs are vulnerable to the Sybil attack. In this a case, a node can act as more than one node using different identities of legitimate nodes. Therefore, a single node presents multiple identities to other nodes in the network [28]. The Sybil attack has attempted to degrade the integrity of data, security and resource utilization [7]. James et al. [29] developed a classification for the Sybil attack. They presented direct vs. indirect communication, fabrication vs. stolen identities, and simultaneity as three dimensions. They proposed defenses against the Sybil attack in sensor network, including radio resource testing, verification of key sets for random key pre-distribution, and registration and position verification.

2.5.4. Wormhole Attack

This type of attack is an important and also it is a dangerous attack. The attacker could record a packet at a single location in the network, tunnels them to another

location, and resends them into the network [2]. The attacker can replay messages to any part of the network. In wormhole attacks, malicious nodes can create a hidden channel between sensor nodes [30]. A wormhole attack is an important threat to a wireless sensor network because this type of attack does not require that a sensor in the network be compromised. This type of attack affects the network layer by continuously hearing and recording data [31]. It can be implemented in the initial phase when the sensor launches to discover information.

A wormhole attack is not easy to detect because an attacker uses a private band, of which the network is not aware [2]. The technique for detecting a wormhole attack was proposed by Perrig et al. [31]. It is based on packet leases, and a message includes a timestamp and the location of the sender. However, it requires strict time synchronization and is infeasible for most sensor networks. Wormhole and sinkhole attacks are sometimes combined to attack the sensor networks. These two types of attacks render the networks hard to defend against attacks [2].

2.5.5. HELLO Flood Attack

The attackers in HELLO flood attacks send or replay a routing protocol [2]. This protocol consists of HELLO packets, which transmit between sensor nodes with extra energy. HELLO packets are employed as a weapon to encourage the sensors in WSNs. The victim nodes attempt to go through the attacker because they think that the attacker is their neighbor [2].

In this chapter, the discussion of countermeasure for selective forwarding attacks is the main goal of this survey. The denial of service attack creates assortments

to attack wireless sensor networks. These assortments may temper sensor nodes and the function of networks. Consequently, some attackers target layers, such as the physical layer, the network layer, the link layer, and the transport layer, and some attackers target the routing layer. A DoS attack may occur in any layer of an OSI layer. All DoS attacks are dependent on the vulnerability of each layer in the architecture of wireless sensor networks. In a DoS attack, adversaries attempt to decipher a system but are unsuccessful. The selective forwarding attack is such an attack.

A selective forwarding attack is hard to detect due to unreliable sensor wireless communications. Karlof and Wagner [2] discussed the selective forwarding attack. In this type of attack, malicious nodes have attempted to stop the packets in a network by rejecting or refusing certain message forwarding and drop them [32]. According to [2], selective forwarding attacks can impact some multi-hop routing protocols, such as TinyOS beaconing, DSR, PSFQ, directed diffusion and its multipath variant, and geographic routing (GPSR and GEAR). During the launch of a selective forwarding attack, a compromised node has notable consequences, including itself, along the path of data. Based on previous studies, this type of attack makes the sensor network rely on the redundancy forwarding via broadcast for data to spread during the network.

Karlof et al. [2] suggested the prevention of selective forwarding attacks by counting the selective forwarding attacks using multipath routing between nodes, which has disadvantages. Communication overhead is increasing, which causes an increase in the number of paths. In addition, the security of WSNs cannot be resilient. The malicious node forwards several packets to the neighbors but drops some them, which causes a significant loss of data. The Low Energy Adaptive Clustering Hierarchy

(LEACH) protocol, which was improved by Wu, Hu, and Ni to the SS-LEACH algorithm, can prevent a selective forwarding attack using a sequence number. Thus, the cluster head is responsible for sending a packet. Jeremy Brown et al [33] described a centralized cluster based a new approach for detecting selective forwarding attack by applying Sequential Probability Ratio Test (SPRT) method [34] [35].

2.6. Selective Forwarding Detection Techniques

2.6.1. Selective Forwarding Scheme using Multi-Hop LWSS

Xin et. al., [36] proposed a lightweight defense against a selective forwarding attack. This defense is dependent on the neighboring nodes. Thus, neighboring nodes monitor the packets during packet transmission, assess the attacker's location and retransfer the packets dropped by the attackers. As a result, they suggested that this approach consumes less energy and storage. Its efficiency in detecting selective forwarding attacks ensures packet delivery to the base station. The defense scheme employs a hexagonal WSN mesh topology. According to the hexagonal mesh topology, the authors specified some processes of topology construction, such as node initialization, cell partition, active node election, and secure architecture construction. In node initialization, the node determines its location and its neighbors' locations. In cell partition, the node determines the association with the RC as shown in Figure 3. Active node selection involves contact with nodes of other RCs. The communication relation is determined between RCs to establish and construct a secure architecture.

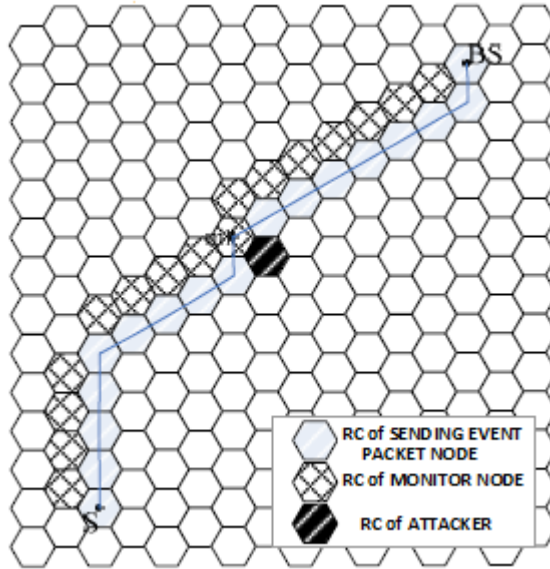


Figure 3: An example for the monitor node gets the attacker-Redrawn [36]

Xin, et.al. Discussed the two phases of a defense scheme. The first phase is routing discovery and selection. The second phase is data transmission with attack defense. Based on the network model, routing discovery and selection method are designed to prevent selective forwarding attacks. It calculates the number of hops between the source node and the destination node. According to the policy of the probability, it selects the transmission route. A method is employed to randomly create the number of continuous hops. In the discovery process, they obtain routes with a specific number of hops in each direction via probability schemes. In data transmission, a packet is sent via a source node using a selected process after an event is produced. The source node transfers the event packet to the subsequent hop node. The next hop node, which is referred to as the intermediate node, receives the event packet and neighboring node, which is referred to as the monitor node. The monitor node, which is the neighboring node responsible for detecting the possibility of a selective forwarding

attack, resends the event packet to the destination node and sends an alarm message to its neighboring nodes for the location attacker.

Yu and Xiao [37] proposed an approach based on lightweight security to detect a selective forwarding attack in the environment of sensor networks. The approach utilized a multi-hop acknowledgment to launch alarms by obtaining responses from the nodes that are located in the middle of paths. Authors assumed the approach could identify malicious sensor nodes. The aim of the detection attack is to send an alarm when a malicious node is discovered, which indicates a selective forwarding attack. Yu and Xiao employed two detection processes in the scheme: a downstream process (the direction on the way to the base station) and an upstream process (the direction on the way to the source node). In the upstream process, a report packet is created and sent to the base station hop by hop when nodes detect a malicious node. `ACK_Cnt` is set to `ACK_Span`, which is a predefined metric. The node that is referred to as the intermediate node saves the packet report as soon as it is received in its cache decreases the `ACK_Cnt` by one or resets `ACK_Cnt` to its initial value. The packet report may be sent downstream if `ACK_Cnt` is 0. Simultaneously, an ACK packet is created and the TTL in the ACK packet is set to `ACK_TTL`, which is a predefined metric. In the remaining detection process, which occurs downstream, packet loss may occur if the intermediate node receives a report packet that should have `Packet_ID` for a certain source node. In this case, the node creates an alarm packet, in which `Lost_Packet_ID_Beg` and `Lost_Packet_ID_End` describe the range of the lost `Packet_IDs`, and `Suspicious_Node_ID` is set to the upstream node, where the report with

the discontinuous Packet_ID originated. The base station will receive the alarm packet and forward multiple hops that are produced by the node.

LWSS detection accuracy is increased by a detecting selective forwarding attack scheme. Although the radio frequency status is poor, detection accuracy is guaranteed. The scheme authorizes the base station and source nodes to collect attack alarm information from the intermediate nodes. Because the sensor node requires more effort, it will impact the efficiency of scheme. The scheme cannot develop a countermeasure for other types of attacks; thus, the scalability will be decreased.

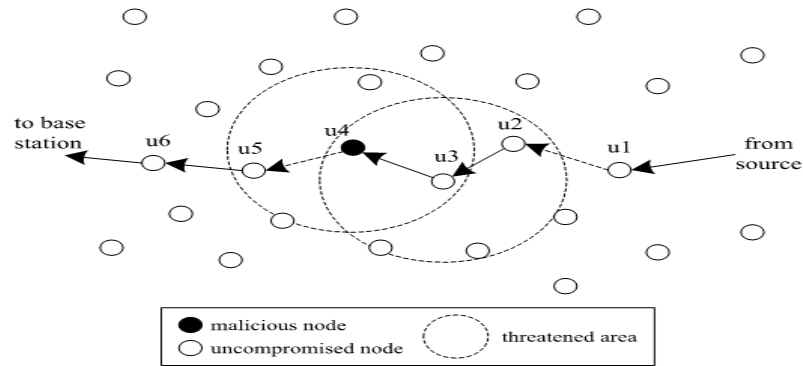


Figure 4: Suspect nodes Identification-Redrawn [37]

The identification of suspect nodes is reported via an intermediate node. Figure 4 provides an example of a node that is suspect and detected by an intermediate node. First, Xiao, Yu, and GAO [37] proposed a checkpoint-based method. In this approach, a node is randomly selected as the checkpoint to send an acknowledgement message for detecting the adversary. It is a mechanism used to identify suspect nodes in a selective forwarding attack. They have attempted to improve the technique by detecting an abnormal packet in sensor networks [36]. They assumed that any compromised nodes

could not create alert packets with the aim of maliciously prosecuting other nodes. In the previous example, node μ_3 produced an alert packet to prosecute node μ_4 . Thus, the prosecuted node is a compromised node. After collecting evidence to determine whether the node is a malicious node, the source nodes determine the position of the suspect node according to the location. However, it is no guarantee for reliable transmission of messages even though the adversary is positioned by acknowledgement.

The identification of suspect nodes is reported via an intermediate node. First, Xiao, Yu, and GAO [37] proposed a checkpoint-based method. Figure 5 illustrates the node is randomly selected as the checkpoint to send an acknowledgement message for detecting the adversary. It is a mechanism used to identify suspect nodes in a selective forwarding attack. They have attempted to improve the technique by detecting an abnormal packet in sensor networks. They assumed that any compromised nodes could not create alert packets with the aim of maliciously prosecuting other nodes. After collecting evidence to determine whether the node is a malicious node, the source nodes determine the position of the suspect node according to the location. However, it is no guarantee for reliable transmission of messages even though the adversary is positioned by acknowledgement.

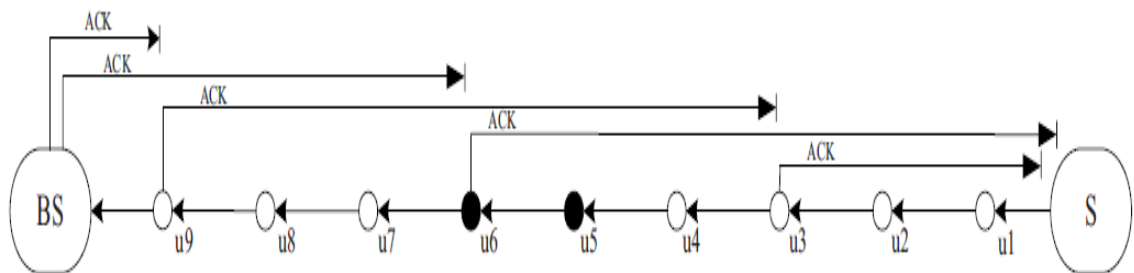


Figure 5: An example of multi-hop acknowledgement with $ACK_Span=3$, $ACK_TTL=6$. -Redrawn [37]

LWSS Drawbacks:

- Resend the packet by using another route caused energy consumption and delay during the detection.
- Transmission of the acknowledgement packet and one-way key packet are also caused energy consumed.
- The scheme is lack of scalability.
- The scheme spent much effort to detect the attack thus it is lack of efficiency.
- LWSS scheme could not detect the attack in some certain conditions.
- Sending the acknowledgment caused wasted the energy.

There is no commitment for the reliable if the packet is dropped.

2.6.2. Selective Forwarding Scheme using Two-Hop LWD

Tran Hoang and Eui-Nam [38] proposed an approach against selective forwarding attacks that consists of a lightweight detection mechanism. The detection is a centralized cluster, which utilized the two-hop neighborhood node information and overhearing technique. It is dependent on the broadcast nature of sensor communication and the high density of sensors. Each sensor node is provided with a detection module that is constructed on an application layer. Sensor node sets routing rules and two-hop neighbor knowledge to generate an alert packet. Hoang and Nam suggested that the two routing rules make the monitoring system more suitable. Thus, the first rule is to

determine if the destination node forwards the packet along the path to the sink. It generates an alert packet with the malicious factor α to the sender/source node. The second rule governs that the monitor node waits and detects the packet that was already forwarded along the path to the sink. It verifies the two-hop neighbor knowledge to assess whether the destination node is on the right path to the sink. If not, it generates an alert packet with the malicious factor β to the sender/source node.

The detection module is responsible for passively detecting a selective forwarding attack in its neighboring sensor node. The malicious counter is defined as the threshold of abnormal activity in a sensor node, which could not skip. Figure 6 provides the malicious counter crossed the threshold X , it revoked the malicious node from its neighbor list. The authors have assumed that the neighboring node should be recognized. The neighboring node must be secure and confidential in the deployment time. The network has a static topology and uses key management to prevent any outside attacks. The selection of one type of network topology prevents the scheme from working with other topologies. Some types of topology such as mesh topology could be protected by using cryptography solutions in selective forwarding attack [39].

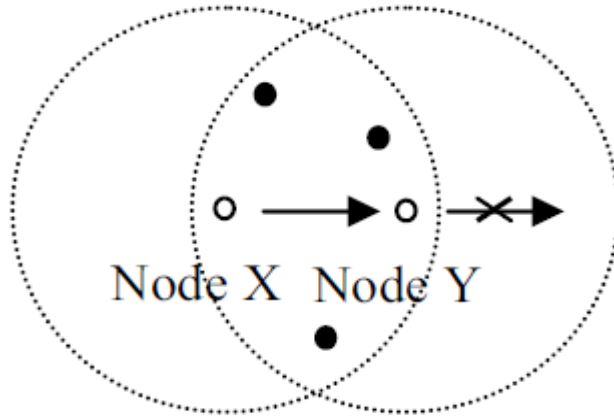


Figure 6: Illustration of monitor node-Redrawn [38]

LWD Drawbacks:

- The network has a static topology. Therefore, LWD scheme will not detect the attack if change the type of topology.
- There is no guarantee for the reliable.
- Detection scheme is not work if node is compromised.

2.6.3. Selective Forwarding Scheme using Watermark Technique SDT

Huijuan Deng et al, [40] proposed a scheme for secure data transmission and detecting a selective forwarding attack. They used watermark technology to detect malicious nodes. Prior to employing a watermark technique, they used a trust value to determine a source path for message forwarding. The trust value involves weighting the credit of each sensor node. The author notes an error rate of 10% and detection accuracy over than 90%. They assumed that the base station is always trustworthy and cannot be comprised by the adversary, which renders the scheme inappropriate for real wireless sensor networks. Every node has a trust value. At the beginning of network initializing,

all nodes should have the same trust value. Huijuan Deng et al. utilized the watermark technique to calculate the packet loss. Data transmission begins when an optimal routing path is confirmed. The base station creates a κ bits binary sequence as the original watermark message. Therefore, a watermark message is part of the packets. A base station compares the extract watermark to the original watermark to detect a selective forwarding attack. The simulation results reveal a channel error rate of 10% and detection accuracy greater than 90%.

SDT Drawbacks:

- There is no data resend method if the packet is dropped.
- SDT scheme cannot detect the malicious node if more than two.
- The scheme is not convenient for sensor caused malicious node and BS cannot compromise.

2.6.4. Selective Forwarding Scheme using Extra Monitor RSSI-EM

Chanatip et al. [41] have proposed a lightweight scheme. They referred to it as a traffic monitor-based selective forwarding attack detection scheme. They used Extra Monitor (EM) to eavesdrop and monitor all traffic when transferring data between nodes. They also employed RSSI to detect a sinkhole attack. The value of RSSI is that four EM nodes can be arranged to establish the positions of all sensor nodes, of which the base station position should be (0, 0). Chanatip et al. have assumed that the network is static when sensor nodes are deployed; thus, any change in the type of topology will immediately affect their approach. They assumed that the attackers could capture and

damage the nodes. Therefore, all sensor nodes must protect or use tamper robust hardware. These assumptions have caused the detection scheme to drain the energy of the sensor nodes and contribute to the high cost.

RSSI-EM Drawbacks:

- The topology is static thus any change of it will effect to the efficiency of the scheme.
- The accuracy of scheme is low.

2.7. Selective Forwarding Detection Evaluation

We further evaluate the performance of these approaches through simulations. We simulate a sensor network with size $800 * 800$ square meters in which 200 sensor nodes are deployed. Hence, each node has a 35 meters transmission range and sensing range of node is 30 meters. In the simulation, we pointed on energy consumption, average throughput, reliable detection rate, and scalability ratio. Details of the rules are given in Table 5.

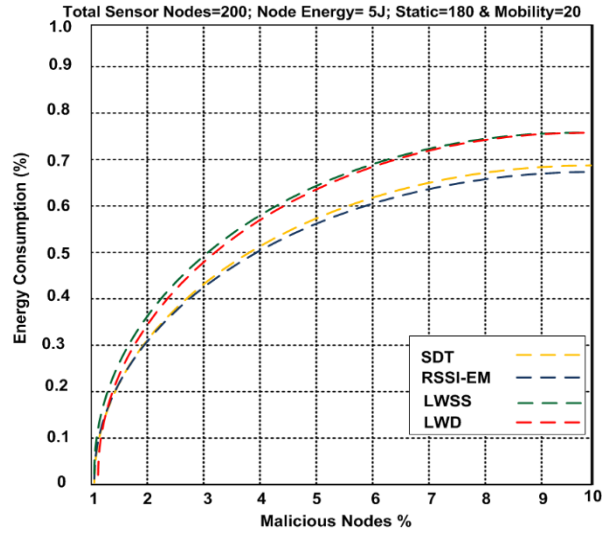


Figure 7: Energy consumption

Energy is an important factor. Figure 7 shows the performance of energy consumption for LWSS, LWD, SDT, and RSSI-EM approaches. The node cost is about 5J energy with 180 static nodes and 20 mobility nodes. As a result, we saw different percentage energy consumption for each one of these approaches. They consumed 75.1%, 81.8%, 69.1%, and 68.5% respectively. Thus, the total of malicious nodes and energy consumption are appearing.

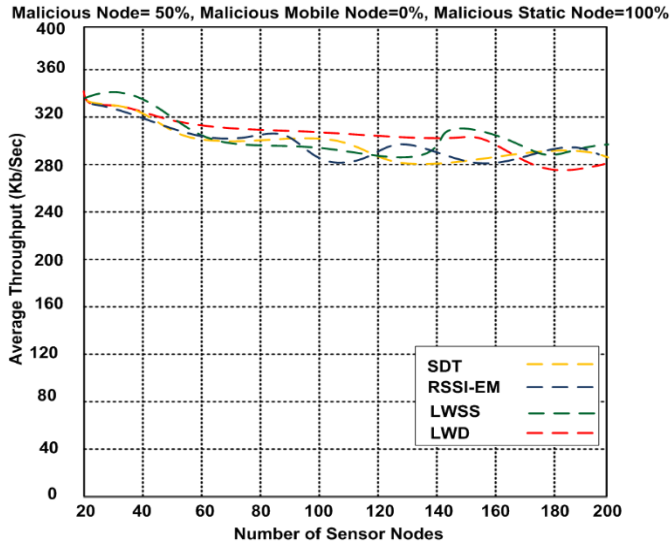


Figure 8: Average throughput

In Figure 8, the graph shows the average throughput of approaches during the attacks without mobility. The malicious node is 50%, malicious mobile node is 0%, and malicious static node is 100%. Therefore, average for each approach is 293k b/sec, 292.9k b/sec, 278.1k b/sec, and 292.8k b/sec respectively.

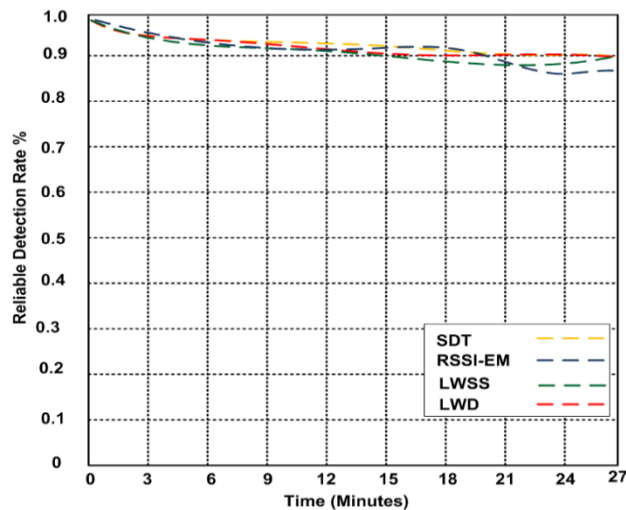


Figure 9: Reliable detection rate

As shown in Figure 9, the reliable detection rate for LWSS, LWD, SDT, and RSSI-EM approaches are not stable and go down when the time increased. The reliable rate are 88.2%, 90.6%, 89.6%, and 86.3% respectively.

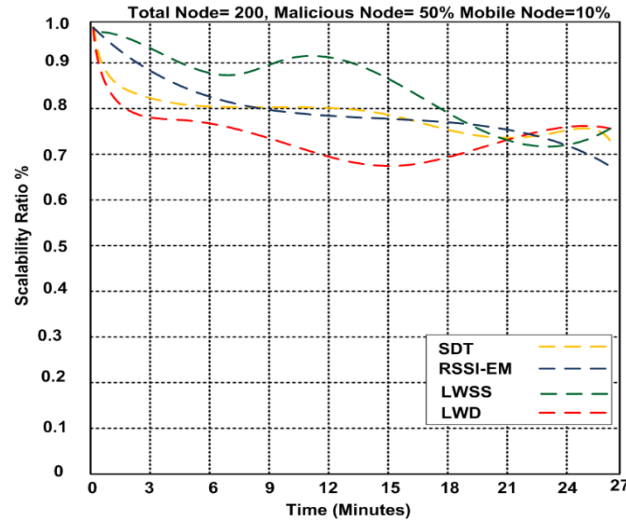


Figure 10: Scalability ratio

Figure 10 shows the scalability ratio for LWSS, LWD, SDT, and RSSI-EM approaches is not stable.

Table 1: Selective Forwarding Attack Analysis

#	Technique/Features	Detection Approach	Prevention Approach	Reliability	Scalability	Energy Consumption	Approach Accuracy	Approach Nature	Routing Protocol	Acknowledgment Based	Neighbor Monitor
1	Karlof and Wagner	X	√	√	√	High	N/A	Distributed	-	X	X
2	Yu and Xiao	√	X	88.2	88.3	75.1	88.9%	Distributed	DD, PSFQ	√	X
3	Yu and Xiao (CHEMAS)	√	X	88.2	88.3	75.1	88.9%	Distributed	DD, PSFQ	√	X
4	Hung-Min Sun et al	X	√	X	X	High	N/A	Centralized	-	X	X
5	Wang Xin-Sheng et al	√	X	√	√	High	N/A	Distributed	OPA_uvwts	X	√
6	Tran Hai and Eul Huh (Two-Hops)	√	X	90.6	95.1	81.8	90.2%	Distributed	-	X	√
7	Young Kim et al (CADE)	√	X	X	X	High	N/A	Centralized	SEEM	√	X
8	Huijuan Dong et al (Watermark)	√	X	89.6	90	69.1	90.9%	Distributed	-	X	X
9	Support Vector Machine (SVM)	√	X	√	√	High	N/A	Centralized	MTE	X	√
10	Chanatip and Ruttikorn	√	X	86.3	88.2	68.5	85.6%	Centralized	-	X	√

Table 2: Selective Forwarding Attack Detection Analysis

#	Technique/Features	Detection Approach	Prevention Approach	Reliability	Scalability	Energy Consumption	Approach Accuracy	Approach Nature	Routing Protocol	Acknowledgment Based	Neighbor Monitor
1	Karlof and Wagner	X	√	√	√	High	N/A	Distributed	-	X	X
2	Yu and Xiao	√	X	88.2	88.3	75.1	88.9%	Distributed	DD, PSFQ	√	X
3	Yu and Xiao (CHEMAS)	√	X	88.2	88.3	75.1	88.9%	Distributed	DD, PSFQ	√	X
4	Hung-Min Sun et al	X	√	X	X	High	N/A	Centralized	-	X	X
5	Wang Xin-Sheng et al	√	X	√	√	High	N/A	Distributed	OPA_uvwts	X	√
6	Tran Hai and Eui Huh (Two-Hops)	√	X	90.6	95.1	81.8	90.2%	Distributed	-	X	√
7	Young Kim et al (CADE)	√	X	X	X	High	N/A	Centralized	SEEM	√	X
8	Huijuan Dong et al (Watermark)	√	X	89.6	90	69.1	90.9%	Distributed	-	X	X
9	Support Vector Machine (SVM)	√	X	√	√	High	N/A	Centralized	MTE	X	√
10	Chanatip and Ruttikorn	√	X	86.3	88.2	68.5	85.6%	Centralized	-	X	√

Table 3: Selective Forwarding Attack Detection Approaches Comparison

Approach Name	Objective	Technique	Application	Disadvantages
LIGHTWEIGHT SECURITY SCHEME-LWSS	Detect selective forwarding attacks	Used multi hop acknowledgements	Battlefield surveillance	<ul style="list-style-type: none"> •Energy is consumed due to sending an acknowledgment. •No guaranteed for reliability.
LIGHTWEIGHT DETECTION-LWD	Detect selective forwarding attacks	2-Hops neighborhood information and over-hearing technique	Monitoring purposes	<ul style="list-style-type: none"> •In case of change in topology by any means, LWD will not work. •Energy consumption and Reliability is not assured.
SCHEME DATA TRANSMISSION-SDT	Forward the data safely and detect the selective forwarding attack	Used watermark technology	Monitoring purposes	<ul style="list-style-type: none"> •No data retransmission method is described after the packet is dropped. •Energy is consumed.
RECEIVED SIGNAL STRENGTH INDICATOR/EXTRA MONITOR , RSSI-EM	Detect selective forwarding	Used EM nodes to eavesdrop and monitor all traffics on the network	Traffic monitoring	<ul style="list-style-type: none"> •Impractical for large networks. •Any change in topology will affect the efficiency of the approach.

Table 4: Detection Approaches Analysis

Approaches	Bandwidth Consumption %	Throughput without Mobility Kb/Sec	Throughput with Mobility Kb/Sec	Scalability %	Accuracy %	Reliability %	Packet Delivery Rate %	Detection Rate %	Energy Consumption with Mobility %
LWSS	64.5	293	297.1	88.3	88.9	88.2	94.4	82.1	75.1
LWD	69.4	292.9	296.8	95.1	90.2	90.6	94.1	80.2	81.8
SDT	72.3	278.1	277.4	90	90.9	89.6	94.3	89.8	69.1
RSSI-EM	61.2	292.8	296.3	88.2	85.6	86.3	94.2	90.1	68.5

CHAPTER 3: MULTI LAYER APPROACH FOR DETECTION OF SELECTIVE FORWARDING ATTACKS

Security issues in wireless sensor networks are critical. Therefore, components that are designed without security can easily become an area for attack. In recent years, the security of WSNs has become increasingly concerning. Sensor node has limited communication and computational resources. It has a short radio range, and simply compromised by an attacker. In a selective forwarding attack, malicious nodes may refuse to forward specific messages and simply drop them or forward the message to the wrong path. Moreover, another variance of this type of attack is to delay packets passing through nodes, breaks the link between nodes, steals some sensitive information of packet. As a result, the entire packet is not transferred to the base station. The selective forwarding attack is smart attack. However, it can be detect by using multi-layer detection approach [42].

We design multi-layer framework based on IDS to detect selective forwarding attacks as well as provides surveillance for military base. The approach contains:

- MAC pool IDs layer.
- Rule-based processing layer.
- Anomaly detection layer.

The goal of our approach is to detect the malicious node, extend the network life time, maintaining the Quality of Service (QoS), and military base surveillance. The distributed approach, on the other hand, have the advantage of improved detection accuracy, low false alarm rates and also if the cluster head gets compromised or the base station gets surrounded by the malicious nodes, the other sensor nodes within the network can still detect the attack and isolate the malicious node. We assume that once the network initializes, the adversaries are not attack the network for the first period.

3.1. Selective Forwarding Detection (SFD) using Multi-Layer

Rule-based IDS is also known as signature-based IDS, which is one of the mechanisms for protecting a network from security threats. The network layer in WSNs is threatened with many types of attacks, including wormhole and sinkhole attacks. Our proposal focuses on the selective forwarding attack. As shown in Figure 11, we design a multi-layer approach to detect one type of security attack, which is selective forwarding attack that includes the three security layers. The first layer is a pool of MAC IDs. In this layer, the important information is filtered and stored. The information includes message fields (e.g., packet, destination, and source IDs) that are useful for rule-based processing. The second layer is the rule-based processing layer. In this layer, there are some rules that must be applied to the stored data. Incoming traffic is either accepted or rejected. In addition, no rules are applied to a message that fails. The third layer is the anomaly detection layer, which detects the false negative anomalies that comprise unknown attacks. The second layer (rule-based processing) and the third layer (anomaly

detection-based IDS) can identify and control selective forwarding attacks in all phases. The three layers are shown in Figure 12. They are supported with three algorithms.

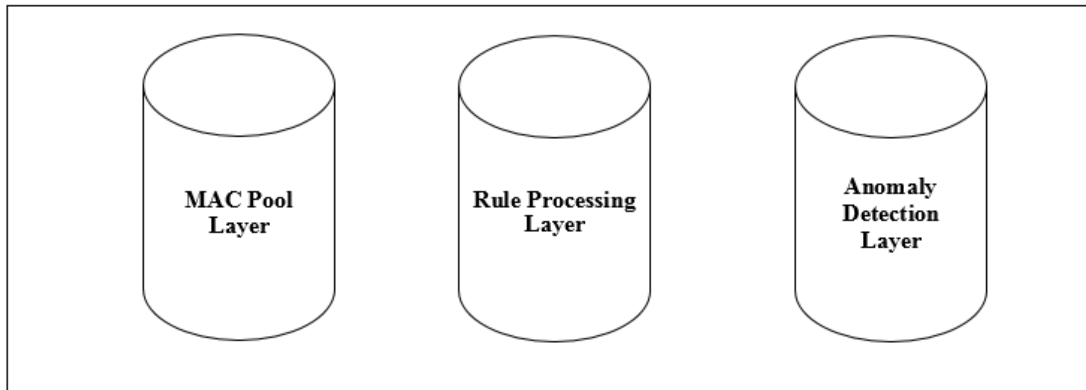


Figure 11: Multi-Layer Approach

The algorithms are used to resolve the attack on the network. An efficient algorithms appropriate for WSNs environment is required to secure communications between nodes. The detection approach saves energy by using little time and memory. It chooses a secure route along which to transfer data between the source and base station. Furthermore, SFD approach will be reliable, energy efficient, and scalable. All of these factors are important for networks of sensor nodes. Additionally, this approach has highly accuracy rate. We compared our approach with other approaches and found SFD has 98.3% accuracy rate so it is higher than other approaches [43].

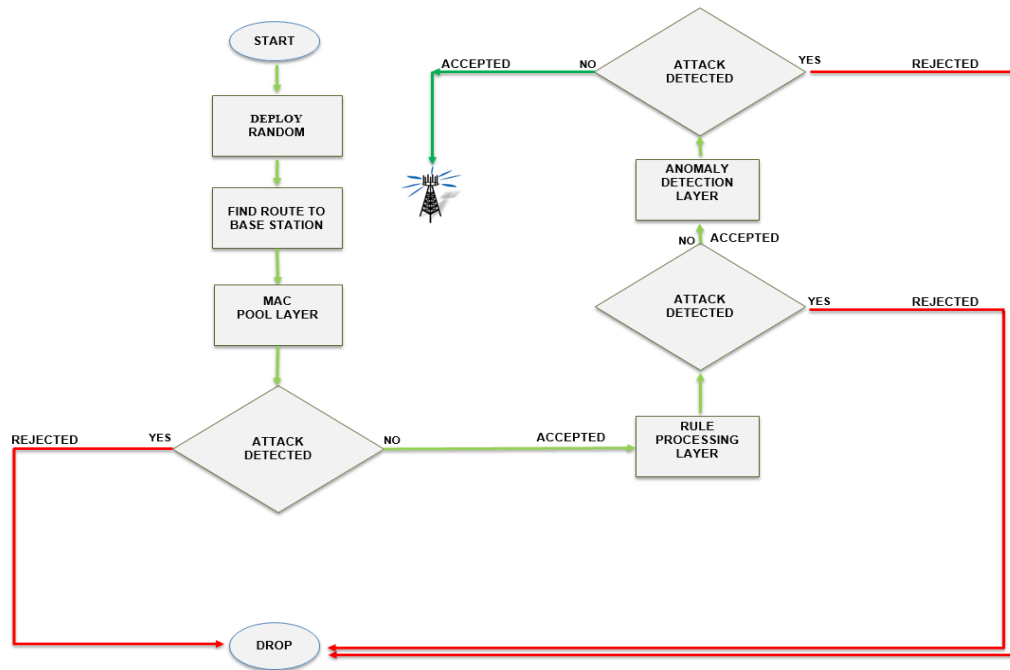


Figure 12: Selective Forwarding Detection (SFD) Flowchart

3.1.1. MAC Pool IDs Layer

The first layer consists of a pool of MAC IDs that filter and match the traffic. Each traffic packet is monitored. The packet is matched to identify malicious activity using message fields (e.g., the packet, destination, and source IDs). It checks whether a node is legitimate or malicious. Therefore, if a node is assigned a value of zero, it drops a packet and is considered malicious. Otherwise, it is accepted as a legitimate node and send it to the second layer, which is rule processing layer. In our study, we analyze the malicious nodes that are detected in the first step using an algorithm based on the pool of MAC IDs as shown in Algorithm 1.

Algorithm 1. MAC Pool of IDs Layer

1. **Input** = (MP: Mac Pool)
 2. **Network parameter** = (SN: sensor node, RT: route, TSN: Total sensor node)
 3. For (SN = 0; SN <= TSN; SN++)
 4. Set SN = SN + 1
 5. If SN \in MP then
 6. Set SN = 0 // the node is declared as malicious node not allowed for communication.
 7. Rejected
 8. Dropped
 9. Else if SN = 1 // Node is declared as a legitimate node and allowed for communication
 10. Accept
 11. Store
 12. Set SN = RT
 13. SN \rightarrow RP
 14. End if
 15. End else
 16. End for
-

3.1.2. Rules Processing Layer

The second layer involves rule-based processing. It is the middle layer. It detects known attacks using rules. These are techniques used to define and describe the normal operations for detecting selective forwarding attacks. Rules must be applied before nodes are deployed in a network area. The rule-based processing layer checks the traffic by comparing it to a list of rules. If the traffic satisfies at least 90% of the rules, the node is confirmed to be legitimate as shown in Algorithm 2. Therefore, the traffic will be accepted and send it to the third layer, which is anomaly detection layer. If the traffic

does not satisfy 90% of the rules, the node is considered doubtful and is rejected.

Details of the rules are given in Table 5.

Algorithm 2. Rules Processing Layer

```
1.   Input = (RP: Rules Process)
2.   Output = (DT: Selective Forwarding Detector, RU: Rules)
3.   Network parameter = (SN: Sensor node, RT: Route)
4.   Attacking parameter = (SFAT: Attacker)
5.   RL1 = Rules based in IDS (RL1IDS)
6.    $RP \subseteq RL1IDS$ 
7.       Set  $RL1 \geq RU$  // 90% from the rules
8.   For (SFAT = RL1; SFAT  $\leq$  RP; SFAT++)
9.       If  $SFAT \subseteq RP$  then
10.          DT  $\rightarrow$  SFAT
11.          Attack alert
12.          Rejected
13.          Dropped
14.      Else if (SFAT  $\not\subseteq$  RP) then
15.          Set SN = RT
16.          SN  $\rightarrow$  AD
17.      End if
18.      End else
19.  End for
```

Table 5: Rules Processing

Rule No.	Rule Description
Rule 1	Each node waits to see if the neighbor node has forwarded the message or not.
Rule 2	The node that receives the message has to check the transfer's identity to make sure it is not changed during transferring.
Rule 3	Each node makes sure that the next node has a shared key for negotiation.
Rule 4	Each node has a message route when it wants to transfer data to other nodes.
Rule 5	Each sensor node must have ACKs.
Rule 6	Each sensor node must have the same ACK that it uses.
Rule 7	Each node is not created a new response before the previous one transfer.
Rule 8	Each node has to send the message using the correct route.
Rule 9	Each sensor node only communicates with other sensor nodes that are located in the same topology.

3.1.3. Anomaly Detection Layer Based on Intrusion Detection System

The third layer involves anomaly detection, which is the recognition of unknown attacks. This layer checks the traffic that comes from the rule-based processing layer.

Therefore, it works to analyze the traffic. The possible results of anomaly detection are false negative, false positive, true negative, and true positive. If the algorithm determines that an unknown attack, which is a false negative, it sends an alert that is a malicious node thus it dropped. Otherwise, the traffic is returned to the pool of MAC IDs by confirming the legitimacy of the node as shown in Algorithm 3. Figure 13 shows all three layers.

Algorithm 3. Anomaly Detection Layer Based on IDS

1. Input = (AD: Anomaly Detection)
 2. Output = (DT: Selective Forwarding Detector)
 3. Network parameter = (SN: Sensor node, RT: Route)
 4. Attacking parameter = (SFAT: Attacker)
 5. RL2 = Anomaly detection based in IDS (RL2IDS)
 6. $AD \subseteq RL2IDS$
 7. For (RL2 = 0; RL2 <= AD; RL2 ++)
 8. RL2 = RL2 + 1
 9. If RL2 \in AD then
 10. Compute FN
 11. $FN = 1/N \sum FN$
 12. M = 1
 13. Set Alert
 14. Rejected
 15. Dropped
 16. Else if RL2 \notin AD then
 17. No Attack
 18. Set SN = RT
 19. Return
 20. SN \rightarrow MP
 21. Declared
 22. End if
 23. End else
 24. End for
-

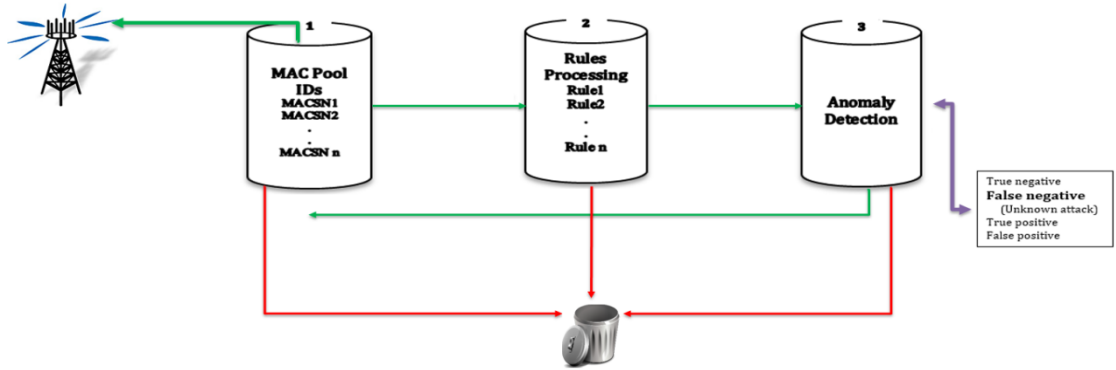


Figure 13: Selective Forwarding Detection-SFD Multi-Layers

3.2. Reliable, Energy efficient and Scalable (RES) Model

The goal of reliable energy-efficient and scalable (RES) model is to extend the network life time while maintaining the Quality of Service (QoS). The network lifetime is the most significant metrics of wireless sensor networks. RES also aims to balance the energy utilization for unevenly distributed sensor nodes to provide longer secure surveillance for military base. In the military base surveillance, there is high probability of nodes to die by forwarding heavy traffic [43, 44].

3.2.1. Reliable

In order to develop the reliable communication, we have to determine the reliable path from the sender node to the base station, as the ' $\forall K$ ' number of the sensor nodes in the reliable optimal 'RP' path is given as

$$\prod_{i=0}^{\forall K} RP_{ij} \quad (1)$$

Let us assume that WSNs are perceived as the 2D graph with vertex 'V' and edges 'E' written as G(V,E) with transmission range 'T_r' so that the maximum reliable communication can be obtained using Bellman-Ford algorithm's link measurement properties 'BF' given as:

$$BF = \frac{\theta\sigma_y^2}{T_r d_x^{-n}} \quad (2)$$

Once, we start searching the reliable path for communication then we can write as:

$$RP : RP_{max} \prod_{(i,j)}^N RP_{ij} - RP_{min} \sum_{(i,j \in RP)}^N -\log \frac{1}{RP_{ij}} \quad (3)$$

We apply Rayleigh fading model to confirm the reliable communication as:

$$RP : RP_{min} \sum_{(i,j \in RP)}^N -\log \frac{1}{RP_{ij}} - RP_{min} \sum_{(i,j \in RP)}^N -\log^2 - (BF) - \sum_{(i,j \in RP)}^N (-BF)$$

Substituting the BF, we get as

$$RP : RP_{min} \sum_{(i,j \in RP)}^N -\log \frac{1}{RP_{ij}} - RP_{min} \sum_{(i,j \in RP)}^N -\log^2 - \left(\frac{\theta\sigma_y^2}{T_r d_x^{-n}} \right) - \sum_{(i,j \in RP)}^N \left(-\frac{\theta\sigma_y^2}{T_r d_x^{-n}} \right) \quad (4)$$

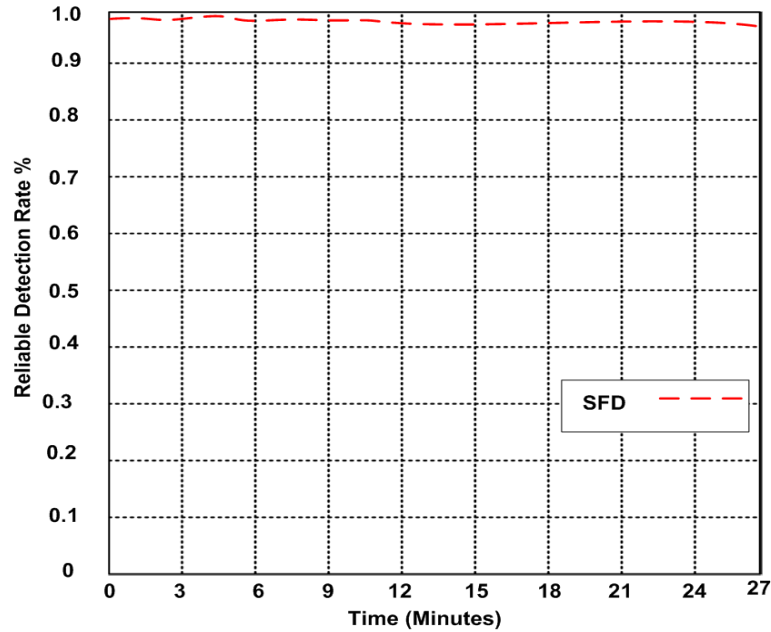


Figure 14: Reliable Detection Rate of SFD Approach

Figure 14 illustrates the rate of reliable detecting of selective forwarding attacks. The proposed approach to SFD has a perfect detection rate. This rate is greater than 98%; therefore, it is easier to detect malicious nodes when they dropped packets.

3.2.2. Energy efficient

Once we are able to find the reliable communication, then we have to balance the energy consumption. Thus, the RES also aims to balance the energy utilization for unevenly distributed sensor nodes to provide longer secure surveillance for military base. In the military base surveillance, there is highest probability of nodes to die by forwarding heavy traffic.

We defined the network lifetime when the sensor node first time drains its energy. Ideally, prolonging the network lifetime requires to satisfy the following conditions:

- Total consumed energy for all sensor nodes in the network.
- Determine the differences between the node's individual energy consumption, average energy consumption of each sensor node, and energy consumed for transmitting the packet and for receiving the packet.

Total consumed energy for all sensor nodes in the network should be considered as minimal' $\prod \Delta E_m'$. The differences between the node's individual energy consumption $\Delta E_m (1 \leq k \leq S_n)$ and an average energy consumption ' ΔE_a ' is the minimal energy. The differences can be accumulated as:

$$\rho^2 = \sum_{k=0}^n k (\Delta E_m - \Delta E_a)^2 \quad (5)$$

where ' ρ^2 ' is differences between minimal energy and an average energy of the sensor node.

After determining the differences, we focuses on an average energy ΔE_a consumption of each sensor node that can be written as:

$$\Delta E_a = \sum_{k=0}^n k (\Delta E_m) \quad (6)$$

Once, an average energy ΔE_a consumption is determined; then we substitute the minimal energy consumption ΔE_m of each sensor node

$$\Delta E_m = \Delta \beta_t \prod_{u \in S(k)} Y_{uk} + \Delta \gamma_r \prod_{v \in S(k)} Z_{vk}$$

$$\Delta E_a = \sum_{k=0}^n k \left(\Delta\beta_t \prod_{u \in S(k)} Y_{uk} + \Delta\gamma_r \prod_{v \in S(k)} Z_{vk} \right) \quad (7)$$

where ' $\Delta\beta_t$ ' is energy consumed for transmitting the packet & ' $\Delta\gamma_r$ ' energy consumed for receiving the packet.

As well as, we need to determine the number of generated packets generated by sensor node ' k '.

$$\omega_p = \left(\Delta\beta_t \prod_{u \in S(k)} Y_{uk} - \Delta\gamma_r \prod_{v \in S(k)} Z_{vk} \right) \quad (8)$$

Based on minimal energy consumption and generated packets, the total consumed energy ΔTE_m can be determined as follows:

$$\Delta TE_m = \sum_{k=0}^n k \left(\Delta\beta_t \prod_{u \in S(k)} Y_{uk} + \Delta\gamma_r \prod_{v \in S(k)} Z_{vk} \right) \times \left(\Delta\beta_t \prod_{u \in S(k)} Y_{uk} - \Delta\gamma_r \prod_{v \in S(k)} Z_{vk} \right) \quad (9)$$

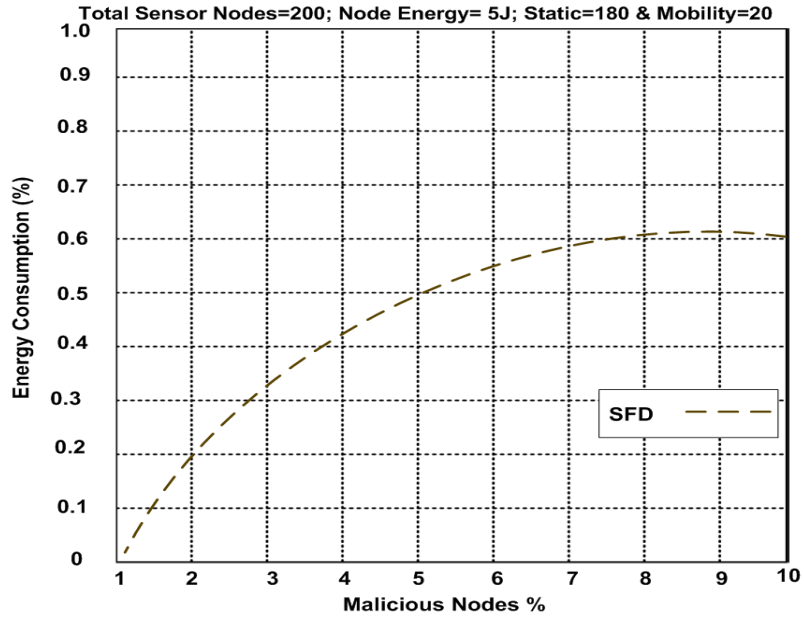


Figure 15: Energy Consumption of SFD Approach

We calculated the amount of energy consumed. Figure 15 is shown the energy consumption of our approach to SFD when 10% of the nodes were malicious and 10% were mobile. The network consumed less energy when it included mobile nodes; therefore, it was 60.4% at the highest point, and the energy cost was low. Therefore, if there are malicious nodes along the routes, this approach to SFD costed less in terms of communication overhead.

3.2.3. Scalable

Sensor network routing protocols should be scalable enough to respond to events in the environment as shown in Figure 16. Once a node joins and leaves the network, the communication performance is affected and the QoS provisioning is degraded. We address scalability in our design to overcome the performance degradation.

Let us consider the number of joining nodes ' k_j ' in the network. Size of the network is limited and it does not accept the load more than $k_j \leq 1 \leq k_t$. Given that the network will accept ' k_1 ' sensor nodes in the network. Thus, scalable probability of network can be defined as:

$$S_p^+ = \sum_{k=0}^{\infty} (k_t) + k_j \times \iint_{i=0 \& j=0}^{N+} (\Delta p)^n + (\nabla p) \quad (10)$$

Where ' $(\Delta p)^n$ ' the number of delivered packets from the sensor nodes that are already part of the network and ' ∇p ' the number of packets delivered by joining nodes in the network and ' S_p^+ ' scalable probability when sensor nodes join the networks.

Once, the sensor node wants to leave the network, then we can determine the scalable probability of network as

$$S_p^- = \sum_{k=0}^{\infty} (k_t) - k_j \times \iint_{i=0 \& j=0}^{N+} (\Delta p)^n - (\nabla p) \quad (11)$$

Where ' S_p^- ' scalable probability when sensor nodes leave the networks.

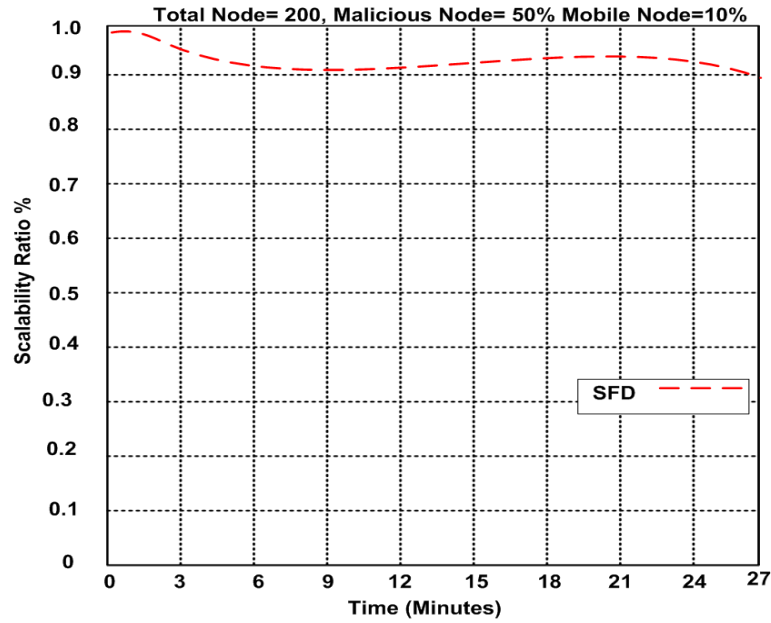


Figure 16: Scalability Ratio of SFD Approach

Based on this model, we can extend the network lifetime even malicious nodes intend to exploit the network. SFD approach designed to execute some problems in sensor network field such as detection selective forwarding attacks, increasing reliable detection rate, energy efficient, and scalable enough to respond to events in the environment.

CHAPTER 4: SIMULATION SETUP AND RESULTS

4.1. Simulation Setup

The simulation scenario consists of 200 nodes with a transmission range of 35 meters and sensing range of 30 meters. The 200 nodes divided into 120 as a legitimate sensor nodes and 80 as malicious sensor nodes. (There are 180 static and 20 mobile nodes). The nodes are randomly placed in uniform fashion in the area of 800 * 800 m² using NS2. The initial energy of the nodes is set 5 joules. The bandwidth of the node is 60 kb/sec, and maximum power consumption for each sensor is set 15.2 mW. Sensing and idle modes have 11.8 mW. Each sensor is capable of broadcasting the data at power intensity ranging from -18 dBm to 13 dBm Table 6 [45, 46].

Table 6: Simulation Setup

Parameters	Description
Transmission Range	35 meters
Sensing Range of node	30 meters
Initial energy of a node	5 Joules
Bandwidth of node	60 Kb/Sec
Number of legitimate sensors	120
Number of Malicious nodes	80
Size of network	800 * 800 square meters
Buffering capacity	45 Packets buffering capacity at each node
Data Packet size	128 bytes
Simulation time	27 minutes
Tx energy	15.2 mW
Rx energy	11.8 mW,
Power Intensity	-18 dBm to 13 dBm.

4.2. Reliable Detection

Figure 17 describes the reliable detection rate of our approach and other works. The reliable detection is an important to extend the network life time. We proved number of packet successfully implemented at the destination node. It cleared that SFD is stabled almost at the same level when the time increased from 0 minutes to 27 minutes.

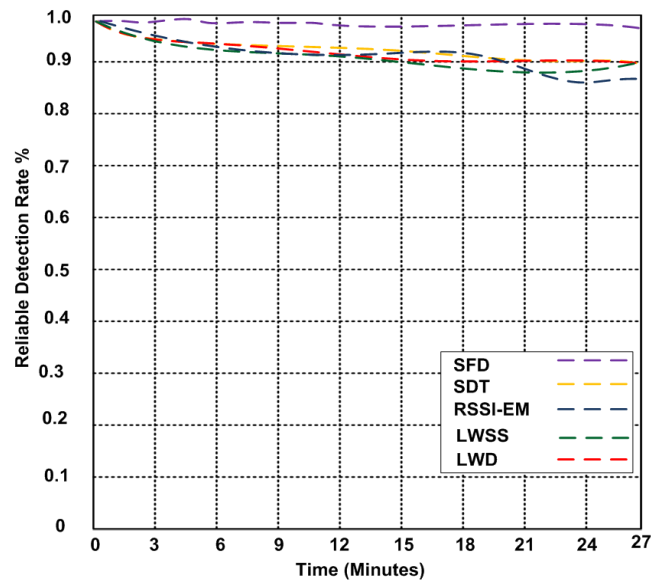


Figure 17: Reliable Detection Rate of Selective Forwarding Attack

The reliable detection rate is 98.4%. The reliable detection rate of SDT, RSSI-EM, LWSS, and LWD approaches are not stable and go down when the time increased. The reliable rates are 89.6%, 86.3%, 88.2%, and 90.6% respectively.

4.3. Energy Efficient

Energy is an important factor. Figure 18 shows the energy consumption of our approach and SDT, RSSI-EM, LWSS, and LWD approaches with 200 static nodes and no mobility nodes.

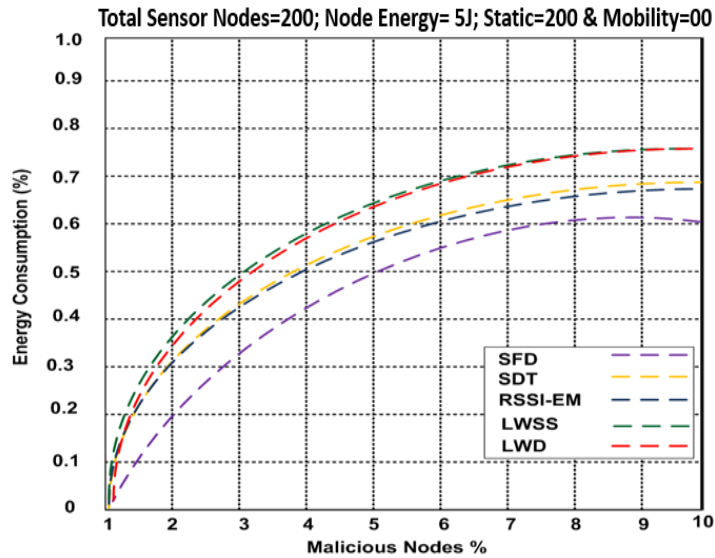


Figure 18: Energy Consumption of Selective Forwarding Attack (No Mobility Node)

Energy consumption at 10% malicious nodes. They consumed 69.1%, 68.5%, 76%, and 76% respectively. SFD is 60.4% at the highest point, and the energy cost is low. It is more efficient while node's detection is increased. Therefore, if there are malicious nodes along the routes, SFD approach able to reduce the less of communication overhead.

Figure 19 shows the performance of energy consumption SDT, RSSI-EM, LWSS, and LWD approaches with 180 static nodes and 20 mobility nodes. In

comparing SFD approach with other approaches, we assume the 10% of nodes are malicious.

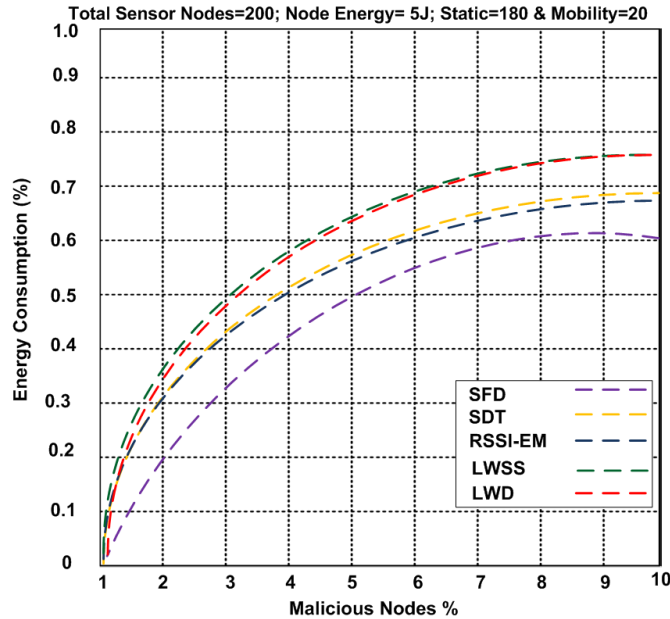


Figure 19: Energy Consumption of Selective Forwarding Attack (20% Mobility Node)

As a result, we found various percentage energy consumption for each one of all approaches. They consumed 69%, 68%, 76%, and 76% respectively. Our approach consumed 60% at the highest point. Hence, the energy cost is low and It is more efficient while node's detection is increased. Therefore, if there are malicious nodes along the routes, SFD approach able to reduce the less of communication overhead.

Figure 20 describes the rendering of energy consumption for SDT, RSSI-EM, LWSS, and LWD approaches with 160 static nodes and 40 mobility nodes. In comparing our approach with other approaches, we assume the 20% of nodes are malicious. Consequently, there were an energy consumption for each one of approaches.

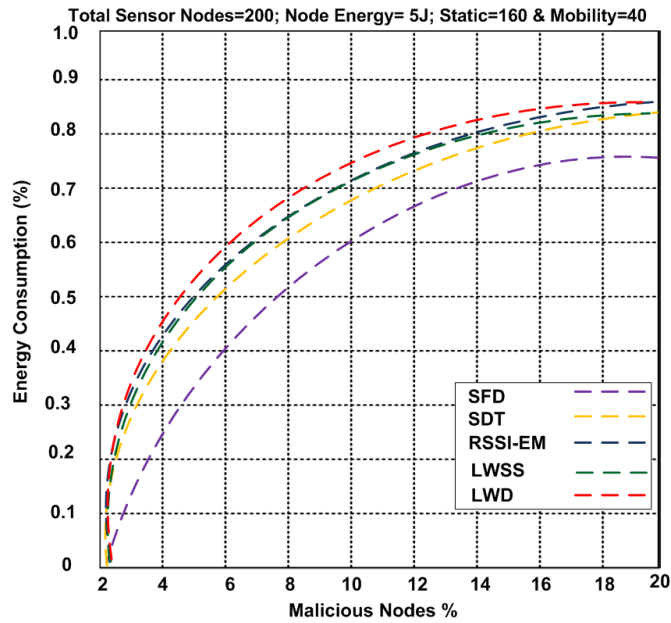


Figure 20: Energy Consumption of Selective Forwarding Attack

They consumed 84%, 86%, 87%, and 87% respectively. SFD approach consumed 76% at the highest point. as a consequence of this comparing, the energy cost is low and It is more efficient while node's detection is increased. Thus, SFD approach qualified for reducing the communication overhead.

Figure 21 shows the energy consumption of our approach and SDT, RSSI-EM, LWSS, and LWD approaches with 100 static nodes and 100 mobility nodes. We suppose the 10% nodes are malicious during the comparing between our approach and other approaches.

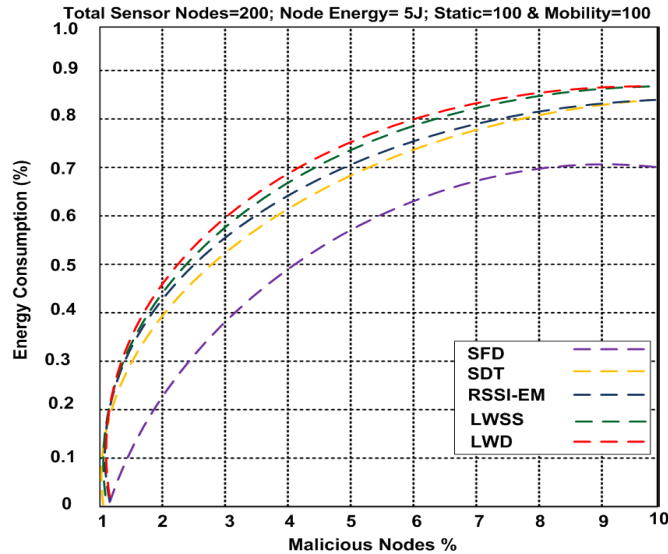


Figure 21: Energy Consumption of Selective Forwarding Attack

They consumed 83%, 83.2%, 84%, 85.1% respectively. SFD consumed 70%. Therefore, it is more efficient than other approaches. Hence, SFD approach has the ability to reduce the less of communication overhead even 50% static nodes and 50% mobility nodes.

Figure 22 shows the energy consumption of our approach and SDT, RSSI-EM, LWSS, and LWD approaches with 50% static nodes and 50% mobility nodes. Energy consumption at 50% malicious nodes.

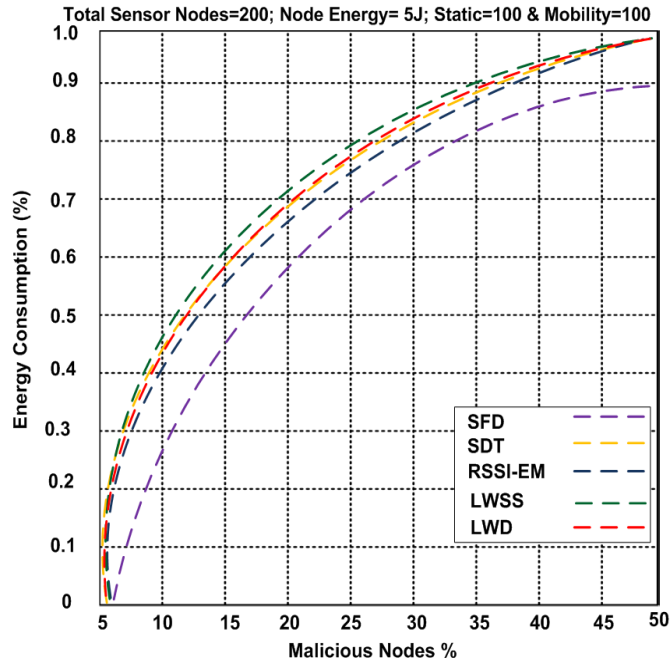


Figure 22: Energy Consumption of Selective Forwarding Attack

They consumed 98%, 98.4%, 99.1%, 99.4%, and respectively. SFD is 89.1% at the highest point. Therefore, SFD approach able to reduce the less of communication overhead even the malicious node is 50% of network.

4.4. Scalability Ratio

Figure 23 shows the scalability ratio of all approaches with 200 sensor nodes including 10% mobile nodes and 10% malicious nodes.

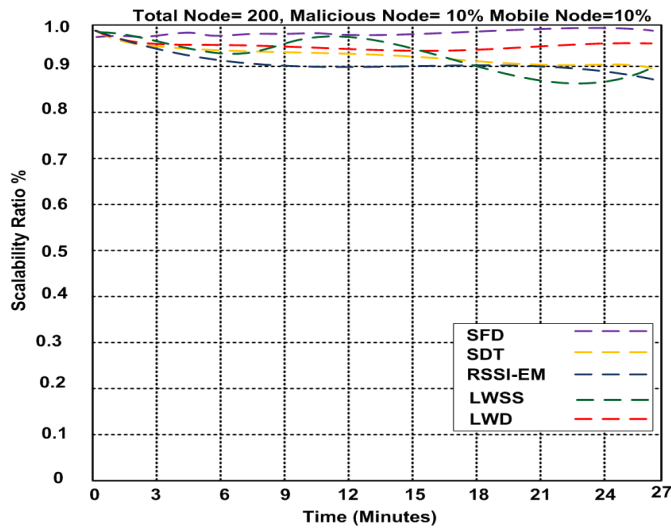


Figure 23: Scalability Ratio (10% Malicious Node)

The average of the scalability of all approaches after 12 minutes shows SFD approach is 97% and other approaches SDT, RSSI-EM, LWSS, and LWD are 93%, 90%, 96%, and 94% respectively. At 27 minutes shows SFD is 97.8 and other approaches are 90%, 88%, 90.1%, and 95%. As a result, SFD approach is scalable during selective forwarding attack than other approaches.

Figure 24 shows scalability ratio of all approaches with 200 sensor nodes including 10% mobile nodes and 25% malicious nodes.

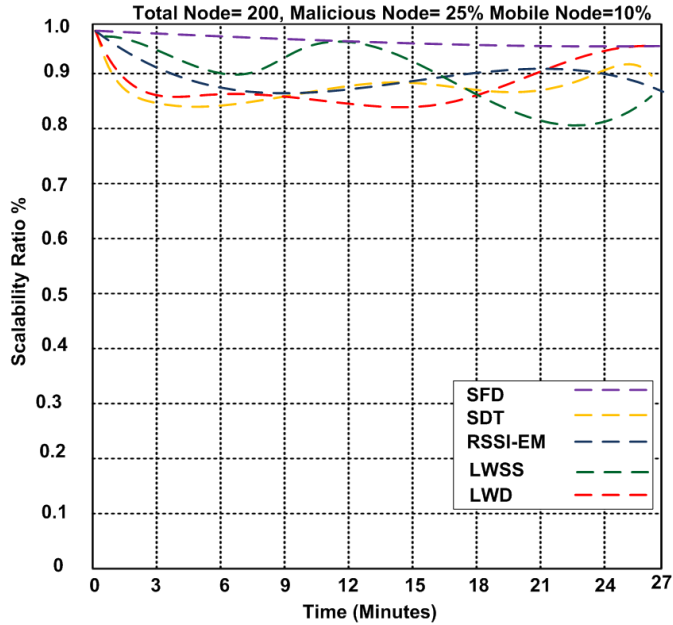


Figure 24: Scalability Ratio (25% Malicious Node)

The average of the scalability after 12 minutes, SFD approach is 97% and other approaches SDT, RSSI-EM, LWSS, and LWD are 88%, 87%, 96%, and 84% respectively. At 27 minutes, SFD is 96% and other approaches are 89.1%, 87%, 88%, and 96%. As a result of this, SFD approach is more scalable even under the attack.

4.5. Probability

Figure 25 shows the probability detection of selective forwarding attack and other competing approaches with 50% malicious nodes and 100% static nodes.

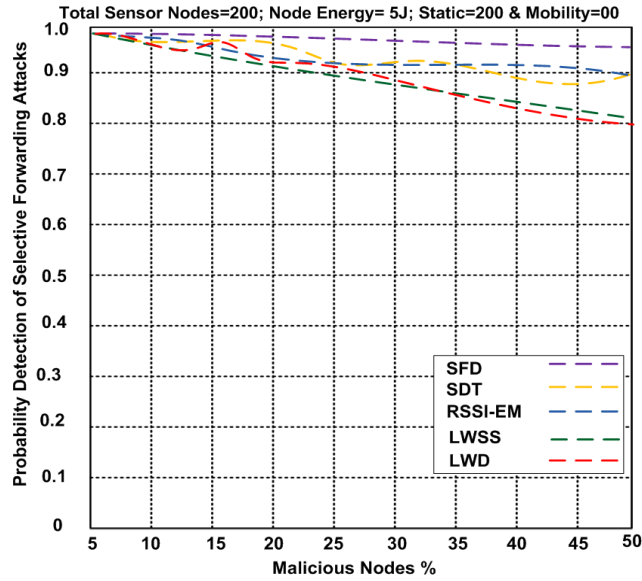


Figure 25: Probability Detection of Selective Forwarding Attack (No Mobility Node)

As a result, SFD approach probability detection between 5 % and 25% malicious nodes is 98% however, the other approaches are between 87% and 90%. Therefore, the SFD approach in probability detection of selective forwarding attacks is higher than other approaches.

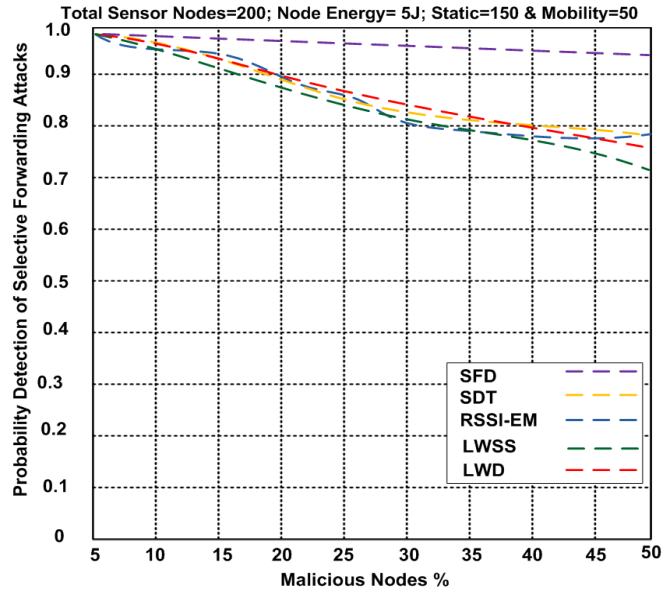


Figure 26: Probability Detection of Selective Forwarding Attack (25% Mobility Node)

Figure 26 shows the probability detection of selective forwarding attack and other competing approaches with 50% malicious nodes and 25% mobility nodes. Hence, SFD approach probability detection between 5 % and 25% malicious nodes is 95% however, the other approaches are between 83% and 86%. For this reason, the SFD approach in probability detection of selective forwarding attacks is higher than other approaches.

Figure 27 shows the probability detection of selective forwarding attack and other competing approaches with 50% malicious nodes and 50% mobility nodes.

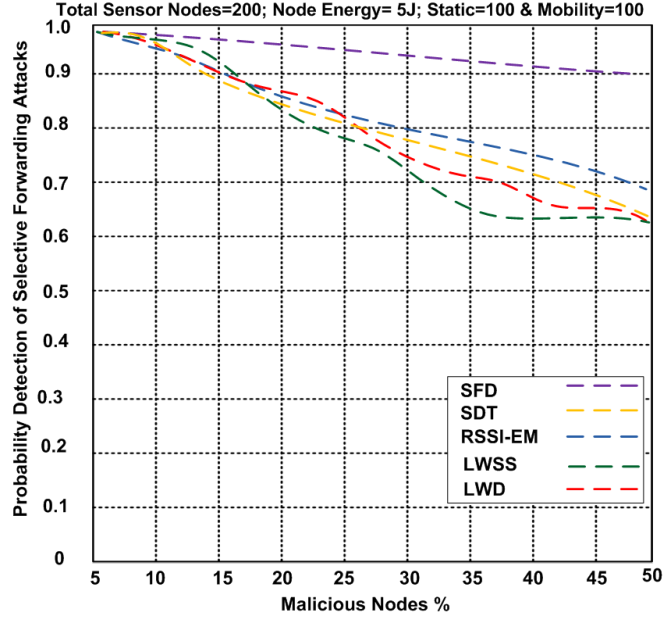


Figure 27: Probability Detection of Selective Forwarding Attack (50% Mobility Node)

As a consequence of this, SFD approach probability detection between 5 % and 50% malicious nodes is 90% however, the other approaches are between 64% and 69%. Thus, the SFD approach in probability detection of selective forwarding attacks is higher than other approaches. We used the probability detection formula as:

$$P_D = \sum_{I=0}^N \frac{e^{-s}}{i!} \times \frac{1}{(N+i-1)!} \int_x^n e^{-\mu} \beta \cdot \mu^{N+i+1} d\mu$$

4.6. Packet Delivery Ratio

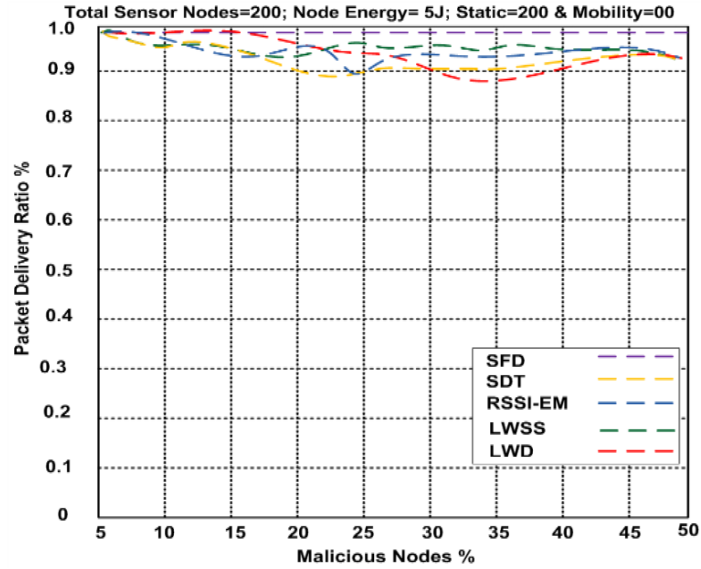


Figure 28: Packet Delivery Ratio (No Mobility Node)

Figure 28 describes packet delivery ratio with 100% static nodes and 50% malicious nodes. Between 5% and 50% malicious nodes, the average of SFD approach is 99.2% higher than other approaches that are 93.4%, 94.1%, 94.3%, and 92.2% respectively. And even malicious nodes are increased, our approach is higher to deliver packets than other approaches.

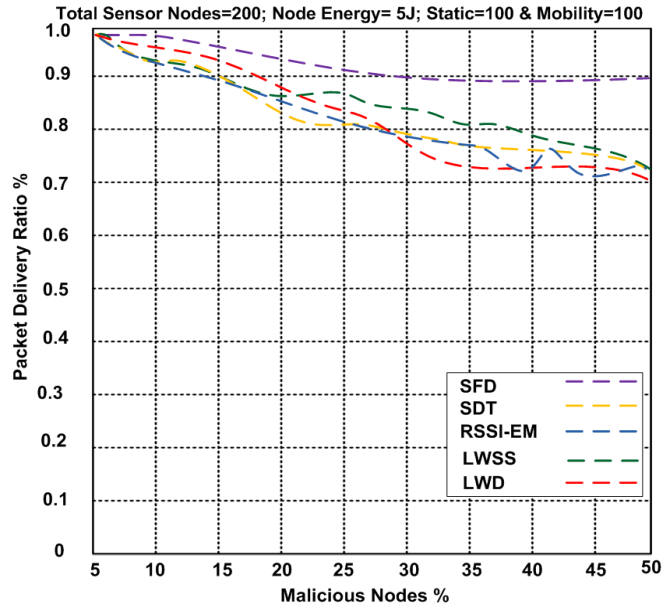


Figure 29: Packet Delivery Ratio (50% Mobility Node)

Figure 29 shows packet delivery ratio with 50% static nodes, 50% mobility nodes and 50% malicious nodes. Between 5% and 50% malicious nodes, the average of SFD approach is 94% and the other approaches are 80%, 82%, 86%, and 83% respectively. Thus, our approach is higher to deliver packets than other approaches even malicious nodes are increased.

4.7. Detection of Selective Forwarding Attack Average

Figure 30 shows detection of selective forwarding attack with 200 static nodes including 25 malicious nodes and no mobility node.

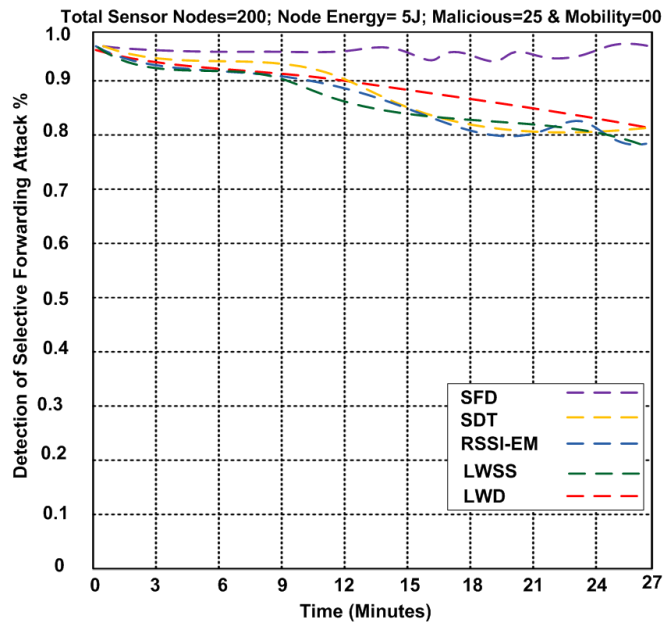


Figure 30: Detection of Selective Forwarding Attack (No Mobility Node)

The average of attack detection after 12 minutes shows SFD approach is 97% SDT, RSSI-EM, LWSS, and LWD are 90%, 88%, 86%, and 90% respectively. At 27 minutes shows SFD is 96% and other approaches are 81%, 78%, 79%, and 82%. Thus, SFD approach is better to detect the selective forwarding attack than other approaches.

Figure 31 describes detection of selective forwarding attack with 200 sensor nodes including 50% mobile nodes and 25% malicious nodes.

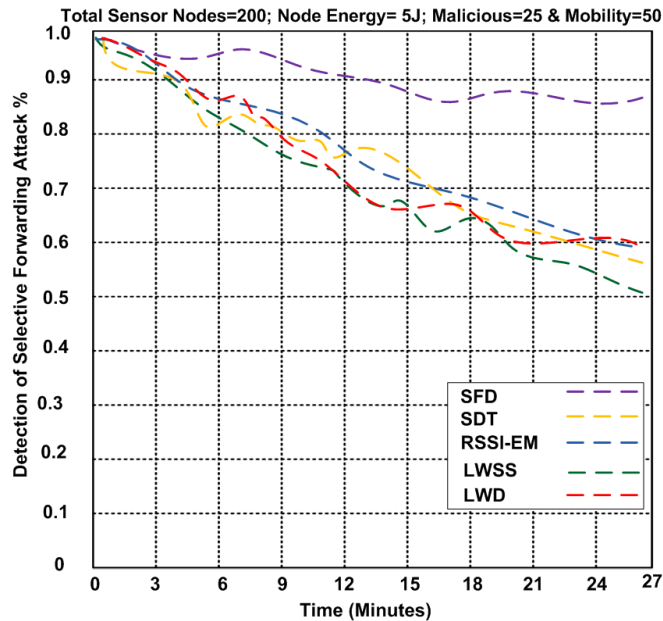


Figure 31: Detection of Selective Forwarding Attack (25% Mobility Node)

The average of attack detection after 12 minutes shows SFD approach is 90% and the other approaches SDT, RSSI-EM, LWSS, and LWD are 77%, 78%, 72%, and 70% respectively. At 27 minutes shows SFD is 87% and other approaches are 57%, 59%, 50%, and 60%. Therefore, SFD is more improved detection the attack than others.

4.8. Throughput Average

Figure 32 shows the average throughput of our approach and other approaches with 50% static nodes, 50% mobile nodes, and 50% malicious nodes.

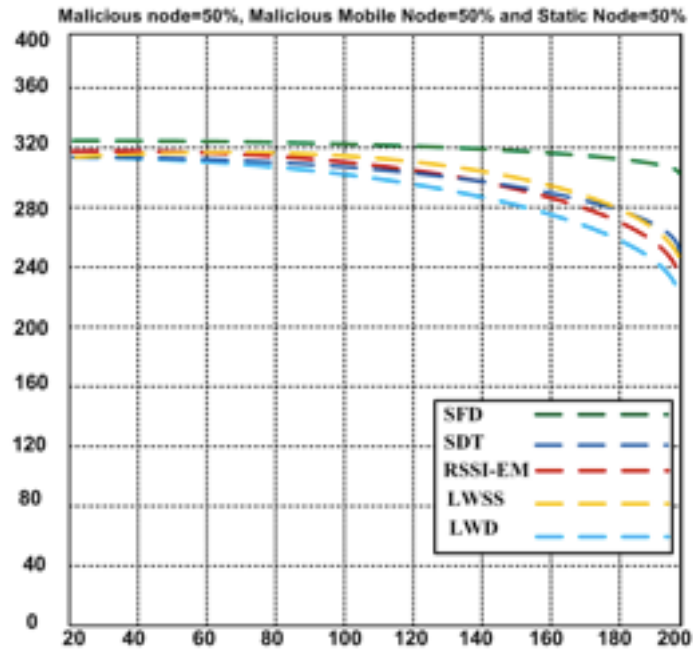


Figure 32: Average Throughput

SFD approach after 100 nodes is 320 kb/sec and others are under 320 kb/sec. At 200 nodes, SFD approach is 300 kb/sec and other approaches SDT, LWSS, RSSI-EM, and LWD are 260 kb/sec, 255 kb/sec, 240 kb/sec, and 230 kb/sec respectively.

Figure 33 shows the average throughput of our approach and other approaches with 100% static nodes and 50% malicious nodes.

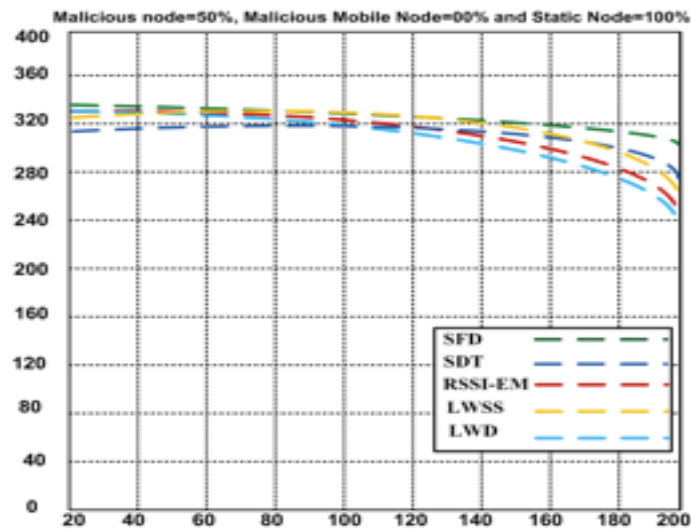


Figure 33: Average Throughput

SFD approach after 100 nodes is 340 kb/sec and other approaches are around 320 kb/sec. At 200 sensor nodes, SFD approach is 310 kb/sec and other approaches SDT, LWSS, RSSI-EM, and LWD are 270 kb/sec, 260 kb/sec, 250 kb/sec, and 240 kb/sec respectively.

4.9. Accuracy Rate

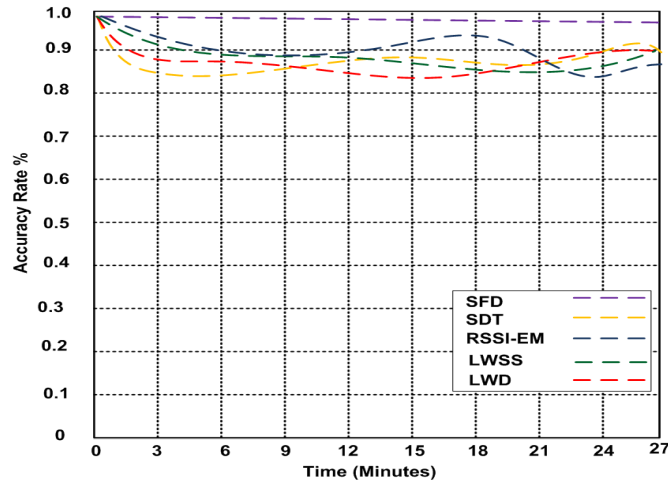


Figure 34: Accuracy Rate

Accuracy rate of SFD and other competing selective forwarding mechanisms are showed in Figure 34. So the accuracy of our approach is more than 98%.

4.10. Time Delay

Figure 35 shows average time delay in different event monitoring time with 50% malicious mobile nodes.

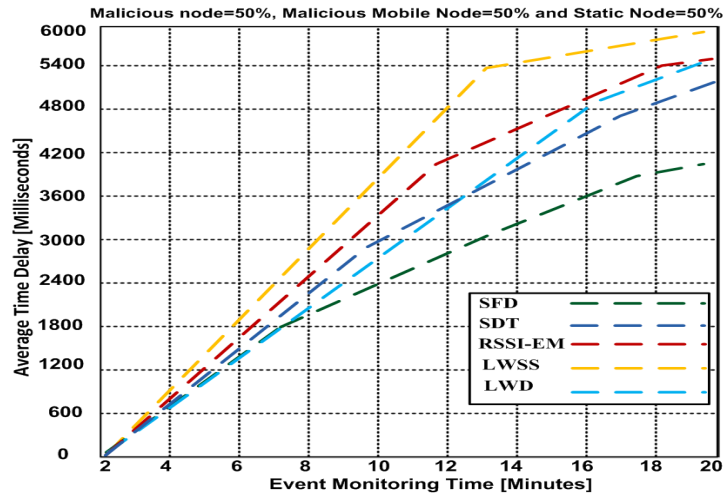


Figure 35: Time Delay

After 10 minutes, the average time delay of SFD approach is 2400 milliseconds and other approaches SDT, RSSI-EM, LWSS, and LWD are 3000, 3400, 3800, and 2800 respectively. At 20 minutes, the average time delay of SFD is 4000 milliseconds and other approaches SDT, RSSI-EM, LWSS, and LWD are 5000, 5500, 6000, and 5400 milliseconds respectively.

Figure 36 shows average time delay in different event monitoring time with 100% static nodes.

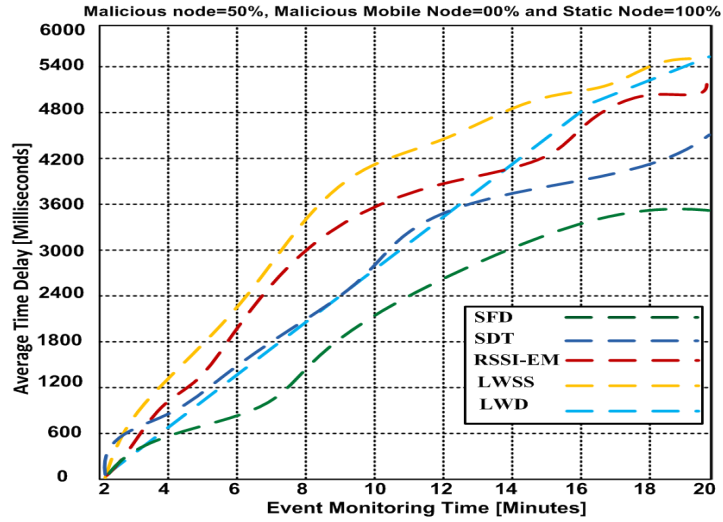


Figure 36: Time Delay

After 10 minutes, the average time delay of SFD approach is 2000 milliseconds and other approaches SDT, RSSI-EM, LWSS, and LWD are 2700, 3600, 4000, and 2700 respectively. At 20 minutes, the average time delay of SFD is 3500 milliseconds and other approaches SDT, RSSI-EM, LWSS, and LWD are 4600, 5000, 5500, and 5600 milliseconds respectively.

CHAPTER 5: CONCLUSION

This dissertation addresses the selective forwarding detection approach of network layer of wireless sensor networks. The contribution focuses on the network layer and provides a multi-layer framework for detection of selective forwarding attacks. We presented a new approach, which provides three multi-layer based on intrusion detection system. These multi-layer are MAC pool IDs layer, rules processing layer, and anomaly detection layer. Each one of these layers is supported by a different algorithm. Therefore, SFD detects malicious nodes that attempt to attack the network. In the first layer, we used an algorithm based on a pool of MAC IDs that authenticates incoming traffic to determine whether a node is legitimate or malicious. In the second layer, we used a rule-based processing algorithm, which checks the traffic by comparing it to a list of rules. In the third layer, we used an anomaly detection algorithm to identify unknown attacks, which appear as false negatives, send an alert, and reject the traffic. The approach goals are to preserve QoS of WSNs, reduce the energy waste, improve the reliable detection rate, and handle the scalability. The presented framework provides a new security model to detect the selective forwarding attacks, which validates the sensor node and then allows transfer of true information between nodes and the base station.

The network's lifetime is the most significant metrics of wireless sensor networks. Thus, we improved reliability detection, reduced the energy consumptions and developed scalability ratio. These factors aim to balance the energy utilization for

unevenly distributed sensor nodes and to provide longer secure surveillance for a military base while maintaining the Quality of Service (QoS). The remaining work for the dissertation is to show the effectiveness of our approach to detect the malicious nodes using in a mobile status. Also, we will show the performance of energy efficient and comparing with other approaches.

We compared the SFD approach with other approaches including LWSS, LWD, SDT, and RSS-EM by using NS2. Therefore, the simulation results demonstrate that SFD approach performs higher throughput than other competing selective forwarding approaches with 50% malicious nodes and 50% mobile nodes. SFD approach obtains the average of throughput between 300 Kbits and 320 Kbits whereas the other approaches are between 220 Kbits and 300 Kbits. We assumed that the SFD approach can be a perfect detection approach of selective forwarding attacks for military application.

This model is designed for detection of one type of attack in wireless sensor networks which is selective forwarding attack, but managing multi-layers to add features to detect some types of attacks in the same layer.

REFERENCES

- [1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks”
Computer Networking 2002, pp. 393-422.
- [2] Karlof, C. and Wagner, D., “Secure routing in wireless sensor networks: Attacks and
countermeasures”, Ad Hoc Networking. 2003, pp. 293-315.
- [3] A. Perrig, J. Stankovic, and D. Wagner, “Security in Wireless Sensor Networks”,
Communication. ACM 2004, pp. 53– 57.
- [4] Fengyun Li, Guiran Chang and Fuxiang GAO, Lan Yao, “A Novel Cooperation
Mechanism to Enforce Security in Wireless Sensor Networks” IEEE Fifth Interantion
Conference on Genetic and Evolutionary Computing, Aug. 29 – Sep. 1, 2011, IEE
Computer Society.
- [5] Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet S,ekercicio
glu,”Detecting Selective Forwarding Attacks in Wireless Sensor Networks using
Support Vector Machines”, In Proceedings of the 3rd International Conference on
Intelligent Sensors, Sensor Networks and Information, Melbourne, Australia, 3-6
December 2007, pp.335 – 340.
- [6] K. Loannis and T. Dimitriou, “Toward Intrusion Detection in Wireless Sensor
Networks”, 13th Euopean Wireless Conference, April 2007, pp. 1-7.
- [7] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Sean Hong, “Security in Wireless
Sensor Networks: Issues and Challenges”, Proc. ICACT 20-22 Feb 2006, vol. 1, pp.
1043-1048.

- [8] Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, June 2004, vol. 47, No. 6, pp. 30-33.
- [9] A. Blilat, A. Bouayad, N. Chaoui, and M. Elghazi, “Wireless Sensor Network: Security Challenges”, IEEE Computer Communication. 2012, pp. 68-72.
- [10] David R. Raymond and Scott F. Midkiff, (2008) “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses,” IEEE Pervasive Computing, 2008, vol. 7, no. 1, pp. 74-81.
- [11] V. Thirupathy Kesavan and S. Radhakrishnan, “Secret Key Cryptography Based Security Approach for Wireless Sensor Networks”, IEEE International Conference on Recent Advances in Computing and Software Systems, 25-27 April 2012, pp. 185-191.
- [12] O. Arazi, H. Qi, D. Rose, “A public key Cryptographic Method for DoS mitigation in wireless sensor networks”, In Sensor, Mesh and Ad Hoc Communications and Networks, June 2007, San Diego, CA, pp. 51-59 .
- [13] Asif Habib, “Sensor Network Security Issues at Network Layer”, 2nd International Conference on Advancements in Space Technologies, 2008, Islamabad, Pakistan, pp. 58-63.
- [14] G. Padmavathi and D. Shanmugapriya,”A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks” International Journal of Computer Science and Information Security, IJCSIS, 2009, vol. 4, no. 1&2, pp. 1-9.
- [15] Annie Jenniefer and John Raybin Jose,”Techniques for Identifying Denial of Service Attack in Wireless Sensor Network” International Journal of Advanced Research in

- Computer and Communication Engineering, IJARCCCE, June 2014, vol. 3, no. 6, pp. 7247-7249.
- [16] A. D. Wood and J. A. Stankovic, "Denial of Service in sensor networks," IEEE Computer, 2002, vol. 35, no. 10, pp. 54-62.
- [17] Mohit Saxena, "Security in Wireless Sensor Networks A layer based classifications", Technical Report [CERIAS TR 2007-04], Center for Education and Research in Information Assurance and Security-CERIAS, Purdue University. pages.cs.wisc.edu/~Massena/papers/2007-04-cerias.pdf.
- [18] David R. Raymond and Randy C. Marchany, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Networks MAC Protocols," IEEE Transactions on Vehicular Technology, 2009, vol. 58, no. 1, pp. 367-380.
- [19] W. Ye, J. Heidemann, and D. Estrin, "Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks," IEEE/ACM Trans. Network., June 2004, vol. 12, no. 3, pp. 493-506.
- [20] T. VanDam and K. Langendoen, "An Addaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," in Proc. 1st ACM Int. Conf. Embedded Netw. Sensor Syst., Nov. 2003, pp. 171-180.
- [21] J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," in Proc. 2nd ACM Int. Conf. Embedded Netw. Sensor Syst., Nov. 2004, pp. 95-107.
- [22] M. Brownfield, K. Mehrjoo, A. Fayez, and N. Davis, "Wireless Sensor Networks Energy Adaptive MAC Protocol," in Proc. IEEE Consume, Communication and Networking Conference, Jan. 2006, pp. 778-782.

- [23] P. Mohanty, S. Panigrahi, N. Sarma, and S. Satpathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey", *Journal of Theoretical and Applied Information Technology*, March 2010, Vol. 13, pp.14.
- [24] A. Razaque and K. M. Elleithy, "Energy-Efficient Border Node Medium Access Control Protocol for Wireless Sensor Networks," *Sensors*, 2014, vol. 14, pp. 5074-5117.
- [25] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme for power exhausting attacks in wireless sensor networks," *International Conference Ubiquitous and Future Networks (ICUFN), Third International Conference*, 2011, pp. 258-263.
- [26] Pandey, A., Tripathi, R.C., "A Survey on Wireless Sensor Networks Security", *International Journal Computing Application, IJCA*, 2010, pp.43-49.
- [27] Nagi, E. C. H., Liu, J. and Lyu, M. R., "An Efficient Intruder Detection Algorithm against Sinkhole Attacks in Wireless Sensor Networks", *Computer Communication, Elsevier*, May 6, 2007, pp. 2353-2364.
- [28] M. M. Patel and A. Aggarwal, "Security Attacks in Wireless Sensor Networks: A Survey" *IEEE International Conference on Intelligent Systems and Signal Processing (ISSP)*, 1-2 March 2013, pp. 329-333.
- [29] J. R. Douceur, "The Sybil Attack," in *1st International Workshop on Peer-to-Peer Systems, (IPTPS)*, Cambridge, MA, USA, Springer 2002, vol. 2429, pp. 251-260.
- [30] Newsome, J., Shi, E., Song, D, and Perrig, A, "The Sybil attack in sensor networks: analysis & defenses", *Proc. of the third international Symposium on Information processing in sensor networks, ACM*, 2004, pp. 259 – 268.

- [31] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless sensor networks", IEEE infocom December 2007, vol. 87, no. 12, pp. 2882-2895.
- [32] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks" IEEE, October 2009, pp. 226 –232.
- [33] J. Brown and X. Du, "Detection of selective forwarding attacks in heterogeneous sensor networks," International Conference on Communications, May 2008, pp. 1583-1587.
- [34] N. Ahmed, S. S. Kanhere, and S. Jha, "Intrusion Detection Techniques for Mobile Wireless Networks," Mobile Computing and Communications Review, 2005, Vol. 9, No. 2, pp. 418.
- [35] Guorui Li, Xiangdong Liu, and Cuirong Wang, "A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks", April 2010, pp.554-558.
- [36] Bo Yu and Bin Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks", In Proceeding of 20th International Parallel and Distributed Processing Symposium, Rhodes Island, Greece, 25-29 April 2006, pp. 1-8.
- [37] Bin Xiao, Bo Yu, and Chuanshan GAO, "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks", In Parallel and Distributed Processing Symposium, November 2007, vol. 67, pp. 1218-1230.
- [38] Tran Hoang Hai and Eui-Nam Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge" In Proceedings of

- the Seventh IEEE International Symposium on Network Computing and Applications, Cambridge, MA, USA, 10-12 July 2008, pp. 325-331.
- [39] D. M. Shila, Yu Cheng, and T. Anjali. Mitigating selective forwarding attacks with a channel-aware approach in WMNS. *Wireless Communications, IEEE Transactions*, May 2010, Vol. 9, pp. 1661 –1675.
- [40] Huijuan Deng, Xingming Sun, Baowei Wang, Yuanfu Cao, “Selective Forwarding Attack Detection using Watermark in Wireless Sensor Networks”, International Colloquium on Computing, Communications Control, and Management (ISECS), Sanya, China, 8-9 August 2009, pp. 109-113.
- [41] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth, “Detecting Sinkhole Attack and Selective Forwarding Attack in Wireless Sensor Networks”, In Proceeding of the 7th International Conference on Information, Communications and Signal Processing, (ICICS), Macau, China, 8-10 December 2009, pp. 1-5.
- [42] Naser Alajmi, Khaled Elleithy: “Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks”, *International Journal of Computer Applications (0975 – 8887)*, Volume 111 (14), pp. 1-12, February 2015.
- [43] Naser Alajmi, Khaled Elleithy: “Multi-Layer Approach for Detection Selective Forwarding Attacks”, *Sensors Journal*, Nov. 2015, Volume 15, pp. 29332-29345.
- [44] Naser Alajmi, Khaled Elleithy: “Selective Forwarding Detection (SFD) in Wireless Sensor Networks”, *IEEE Long Island Systems, Applications and Technology LISAT2015 Conference*, Long Island, NY, May 2015.

- [45] Naser Alajmi, Khaled Elleithy: “A Multi-Layer Framework for Detection Selective Forwarding Attacks in WSNs”, “The International Conference on Engineering Technologies & Entrepreneurship”, Kuala Lumpur, Malaysia, November 2015.
- [46] Naser Alajmi, Khaled Elleithy: “A New Approach for Detecting and Monitoring Selective Forwarding Attack in Wireless Sensor Networks”, IEEE Long Island Systems, Applications and Technology LISAT2016 Conference, Long Island, NY, April 2016 (Best Paper in the Technology Track).

APPENDIX A: PUBLICATIONS

Journals Publication

- Naser Alajmi, Khaled Elleithy: “Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887), Volume 111 - No 14, February 2015
- Naser Alajmi, Khaled Elleithy: “Multi-Layer Approach for Detection Selective Forwarding Attacks”, Sensors 2015, Nov., [IF 2.54], 29332-29345; doi:10.3390/s151129332

Conferences Publication

- Naser Alajmi, Khaled Elleithy: “Selective Forwarding Detection (SFD) in Wireless Sensor Networks”, IEEE Long Island Systems, Applications and Technology LISAT2015, Long Island, NY, May 2015
- Naser Alajmi, Khaled Elleithy: “A Multi-Layer Framework for Detection Selective Forwarding Attacks in WSNs”, “The International Conference on Engineering Technologies & Entrepreneurship”, Kuala Lumpur, Malaysia, November 2015
- Naser Alajmi, Khaled Elleithy: “A New Approach for Detecting and Monitoring Selective Forwarding Attack in Wireless Sensor Networks”, IEEE Long Island Systems, Applications and Technology LISAT2016, Long Island, NY, April 2016 (Best Paper in the Technology Track)

Conferences Publication

- Naser Alajmi, Khaled Elleithy: “A New Approach for Detecting and Monitoring of Selective Forwarding Attack in WSN”, UB Faculty Research Day (FRD 2016), Bridgeport, CT, April 2016
- Naser Alajmi, Khaled Elleithy: “A New Approach for Detecting of Selective Forwarding Attack in Wireless Sensor Networks”, American Society for Engineering Education (ASEE 2016), Kingston, Rhode Island, April 2016