

التاريخ: / /

نموذج رقم (18)
اقرار والتزام بالمعايير الأخلاقية والأمانة العلمية
وقوانين الجامعة الأردنية وأنظمتها وتعليماتها
لطلبة الماجستير

أنا الطالب: علاء عبد الرحيم محمد كراجة الرقم الجامعي: (8080202)
تخصص: علم الحاسوب الكلية: تكنولوجيا المعلومات

عنوان الرسالة: Securing Wireless Sensor Networks
against Denial of Service Attacks

اعلن بأنني قد التزمت بقوانين الجامعة الأردنية وأنظمتها وتعليماتها وقراراتها السارية المفعول المتعلقة بأعداد رسائل الماجستير عندما قمت شخصياً بأعداد رسالتي وذلك بما ينسجم مع الأمانة العلمية وكافة المعايير الأخلاقية المتعارف عليها في كتابة الرسائل العلمية. كما أنني أعلن بأن رسالتي هذه غير منقولة أو مستلة من رسائل أو كتب أو أبحاث أو أي منشورات علمية تم نشرها أو تخزينها في أي وسيلة اعلامية، وتأسيساً على ما تقدم فأنني أتحمل المسؤولية بأنواعها كافة فيما لو تبين غير ذلك بما فيه حق مجلس العمداء في الجامعة الأردنية بالغاء قرار منحي الدرجة العلمية التي حصلت عليها وسحب شهادة التخرج مني بعد صدورها دون أن يكون لي أي حق في التظلم أو الاعتراض أو الطعن بأي صورة كانت في القرار الصادر عن مجلس العمداء بهذا الصدد.

التاريخ: ٢٠١١ / ١٢ / ٢٠


توقيع الطالب: علاء عبد الرحيم محمد كراجة

تعتمد كلية الدراسات العليا
هذه النسخة من الرسالة
التوقيع: علاء عبد الرحيم محمد كراجة التاريخ: ٢٠١١ / ١٢ / ٢٠

The University of Jordan

Authorization Form

I, *Ola Karajeh*, authorize the University of Jordan to supply copies of my Thesis/ Dissertation to libraries or establishments or individuals on request, according to the University of Jordan regulations.

Signature: 

Date: *20/12/2010*

**SECURING WIRELESS SENSOR NETWORKS AGAINST DENIAL
OF SERVICE ATTACKS**

**By
Ola Karajeh**

**Supervisor
Dr. Iman Al-Momani**

**Co-Supervisor
Dr. Hazem Al Hiary**

**This Thesis was Submitted in Partial Fulfillment of the Requirements
for the Master's Degree of Computer Science**

**Faculty of Graduate Studies
The University of Jordan**

December, 2010

تعتمد كلية الدراسات العليا
هذه النسخة من الرسالة
التوقيع: التاريخ: ١٤/١٢/٢٠١٠

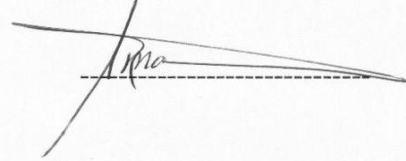
COMMITTEE DECISION

This Thesis/Dissertation (Securing Wireless Sensor Networks against Denial of Service Attacks) was successfully Defended and Approved on 6/12/2010.

Examination Committee

Dr. Iman Musa Al-Momani (Supervisor)
Assist. Prof. of Wireless Networks and Security

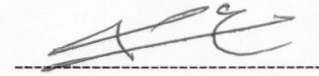
Signature



Dr. Hazem Al Hiary (Co-Supervisor)
Assist. Prof. of Image Processing, Document
Analysis and Recognition, Data Hiding



Dr. Azzam Sleit (Member)
Assoc. Prof. of Imaging Databases



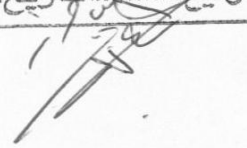
Dr. Basel Ali Mahafzah (Member)
Assist. Prof. of Parallel and Distributed Computing,
And Interconnection Networks



Dr. Hamed Saqer Al-Bdour (Member)
Assoc. Prof. of Computer Systems and Networks
Mu'tah University



تعتمد كلية الدراسات العليا
هذه النسخة من الرسالة
التوقيع..... التاريخ.....



DEDICATION

To the memory of my beloved father who has always been in my heart throughout this journey although he couldn't see this achievement in his life.

To my lovely mother for her support, patience, prayers and encouragement throughout my life.

To my dear brothers Dr. Mohammed and Dr. Mahmoud and sisters especially Nuha and Dr. Huda (and her husband Dr. Mahmoud Maqableh) as they were always there and provided me with love, support strength, patience and encouragement throughout the development of my thesis.

To my best friends, Lamyia Omar, Maryam Al-Sharief and Rawa'a Al-Jabaly whom I consider as more than sisters, for their invaluable friendship, support and encouragement throughout of my life.

ACKNOWLEDGEMENT

My marvelous thanks and appreciation are always for ALLAH the most merciful for his endless support and bless. I ask him to forgive my slackness and mistakes and allow me and my family into his mercy.

I would like to express my deepest appreciation and thanks to my supervisor Dr. Iman Al-Momani and my co-supervisor Dr. Hazem Al Hiary, to whom I am truly indebted for their generous help, continuous support, precious encouragement, enthusiasms, guidance and teaching throughout the conduction of this work. I am so grateful for their kindness, assistance and patience in reviewing, discussing and correcting the manuscript. Grateful thanks for them for providing me with confidence and constructive consultations during all my works.

Many thanks also to Maha Saadeh and Emad Mashakbeh for their help in the conduction of this work.

Precious thanks to all my friends and colleagues especially Lamyia Omar, Maryam Al-Sharief and Rawa'a Al-Jabaly for their continuous help and encouragement.

Finally, I would like to thank my mother and dear brothers and sisters, especially Dr.Mahmoud and Dr.Huda, for their support and prayers all the times that are always leading me to the right path in my life.

TABEL OF CONTENTS

COMMITTEE DECISION	ii
DEDICATION.....	iii
ACKNOWLEDGEMENT	iv
TABEL OF CONTENTS	v
LIST OF TABLES	vii
LIST OF FIGURES	viii
LIST OF ABBREVIATIONS.....	x
ABSTRACT	xi
1. INTRODUCTION	1
1.1 Research Motivation and Objectives.....	1
1.2 Problem Statement	2
1.3 Contributions.....	3
1.4 Research Methodology.....	4
1.5 Thesis Organization	5
2. Literature Review	7
2.1 Background.....	7
2.1.1 Wireless Sensor Networks.....	7
2.1.2 Denial of Service Attacks (DoS) against Wireless Sensor Networks	9
2.1.3 Broadcast Authentication Approaches.....	11
2.2 Related Works	14
2.2.1 Prevention-based Techniques	14
2.2.2 Detection-based Techniques	24
3. Methodology	30
3.1 Intrusion Prevention Detection based Scheme System Model.....	32
3.2 Intrusion Prevention Detection based Scheme (IPDS)	33
3.3 Fuzzy Logic based Intrusion Detection System (FL-IDS)	44
4. IPDS System's Evaluation.....	56
4.1 Simulation Environment.....	56
4.2 Evaluation Metrics.....	56

4.3	Parameter Values	61
4.4	Results and Evaluation.....	65
4.4.1	Energy Consumption of Faked Messages under Various DoS Attacks Intensities ...	65
4.4.2	Average Broadcast Delay for Authentic Messages under Various DoS Attacks Intensities	78
5.	Conclusions and Future Works.....	86
	References.....	88
	Abstract in Arabic	92

LIST OF TABLES

TABLE 1: DENIAL OF SERVICE AGAINST WSN: ATTACKS AND DEFENSES	10
TABLE 2: SIMPLE COMPARISON BETWEEN THE TWO MODES	18
TABLE 3: NOTATIONS AND PARAMETERS USED IN ADAPTIVE WINDOW SCHEME	22
TABLE 4: NOTATIONS AND PARAMETERS USED IN IPDS	38
TABLE 5: FUZZY IF-THEN RULES FOR FIS (1)	51
TABLE 6: FUZZY IF-THEN RULES FOR FIS (2)	54

LIST OF FIGURES

FIGURE 1: AN EXAMPLE OF ONE-WAY KEY CHAIN	12
FIGURE 2: TIME INTERVALS FOR EACH KEY	13
FIGURE 3: THE ADAPTIVE WINDOW SCHEME FLOW CHART	20
FIGURE 4: THE ADAPTIVE WINDOW SCHEME ALGORITHM DESCRIPTION (AL-MOMANI, ET AL., 2010).....	23
FIGURE 5: INTRUSION DETECTION FRAMEWORK	26
FIGURE 6: IPDS ARCHITECTURE	34
FIGURE 7: THE PROPOSED IPDS FLOW CHART	36
FIGURE 8: THE PROPOSED FLIDS ALGORITHM DESCRIPTION.....	40
FIGURE 9: TWO TIER FL-IDS.....	44
FIGURE 10: FUZZY LOGIC INFERENCE SYSTEM (1).....	47
FIGURE 11: FUZZY LOGIC INFERENCE SYSTEM (2).....	47
FIGURE 12: FUZZY MEMBERSHIP FUNCTION FOR THE ACCUMULATIVE COUNTER OF DIFFERENCE FACTOR	48
FIGURE 13: FUZZY MEMBERSHIP FUNCTION FOR THE MISMATCHING VALUE FACTOR.....	49
FIGURE 14: FUZZY MEMBERSHIP FUNCTION FOR THE REPUTATION OUTPUT PARAMETER	50
FIGURE 15: FUZZY MEMBERSHIP FUNCTION FOR REPUTATION AS INPUT PARAMETER TO FIS (2).....	52
FIGURE 16: FUZZY MEMBERSHIP FUNCTION FOR COUNTER OF FAKED MESSAGES FACTOR	53
FIGURE 17: FUZZY MEMBERSHIP FUNCTION FOR THE CONFIDENCE VALUE OUTPUT PARAMETER	54
FIGURE 18: THE PROPOSED DECISION MAKING SYSTEM PERFORMED BY BS.....	55
FIGURE 19: ENERGY CONSUMPTION: THE PERCENTAGES OF WASTED ENERGY IN RECEIVING AND FORWARDING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES IN IPDS	67
FIGURE 20: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY IN RECEIVING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES IN IPDS, ADAPTIVE WINDOW AND DYNAMIC WINDOW SCHEMES.....	69
FIGURE 21: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY IN FORWARDING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES IN IPDS, ADAPTIVE WINDOW AND DYNAMIC WINDOW SCHEMES.....	70
FIGURE 22: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY DUE TO RECEIVING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES FOR BOTH IPDS AND ADAPTIVE WINDOW SCHEMES WITH DIFFERENT A VALUES	73
FIGURE 23: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY DUE TO FORWARDING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES FOR BOTH IPDS AND ADAPTIVE WINDOW SCHEMES WITH DIFFERENT A VALUES	74
FIGURE 24: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY DUE TO RECEIVING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES FOR ADAPTIVE WINDOW SCHEME WITH DIFFERENT A VALUES (A=0.3 AND A=0.5).....	75
FIGURE 25: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY DUE TO FORWARDING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES FOR ADAPTIVE WINDOW SCHEME WITH DIFFERENT A VALUES (A=0.3 AND A=0.5).....	76
FIGURE 26: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY DUE TO RECEIVING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES FOR IPDS SCHEME WITH DIFFERENT A VALUES (A=0.3 AND A=0.5).....	77

FIGURE 27: ENERGY CONSUMPTION: THE PERCENTAGE OF WASTED ENERGY DUE TO FORWARDING FAKED MESSAGES UNDER VARIOUS DOS ATTACKS INTENSITIES FOR IPDS SCHEME WITH DIFFERENT A VALUES (A=0.3 AND A=0.5).....	78
FIGURE 28: AVERAGE BROADCAST DELAY FOR AUTHENTIC MESSAGES UNDER VARIOUS ATTACKS INTENSITIES FOR IPDS, ADAPTIVE WINDOW, DYNAMIC WINDOW AND AUTHENTICATION FIRST SCHEMES (WITH A=0.5 FOR AUTHENTIC MESSAGES AND A=0.6 FOR FAKED MESSAGES).....	81
FIGURE 29: AVERAGE BROADCAST DELAY FOR AUTHENTIC MESSAGES UNDER VARIOUS ATTACKS INTENSITIES FOR BOTH IPDS AND ADAPTIVE WINDOW SCHEMES WITH DIFFERENT A VALUES	83
FIGURE 30: AVERAGE BROADCAST DELAY FOR AUTHENTIC MESSAGES UNDER VARIOUS ATTACKS INTENSITIES FOR ADAPTIVE WINDOW SCHEME WITH DIFFERENT A VALUES (A=0.3 AND A=0.6).....	84
FIGURE 31: AVERAGE BROADCAST DELAY FOR AUTHENTIC MESSAGES UNDER VARIOUS ATTACKS INTENSITIES FOR IPDS WITH DIFFERENT A VALUES (A=0.3 AND A=0.6).....	85

LIST OF ABBREVIATIONS

Abbreviations	Expression
AIMD	Additive Increase Multiplicative Decrease
BPN	Back Propagation Network
BS	Base Station
CWSNs	Clustered-based Wireless Sensor Networks
DoS	Denial of Service
DREAM	DoS Resistant Efficient Authentication Mechanism
ECDSA	Elliptic Curve Digital Signature Algorithm
eHIDS	energy efficient Hybrid Intrusion Detection System
EW	Estimated Window size
FIS	Fuzzy Logic Inference System
FL-IDS	Fuzzy Logic based Intrusion Detection Scheme
IDS	Intrusion Detection System
IPDS	Intrusion Prevention Detection based Scheme
MANETs	Mobile Ad hoc Networks
MN	Master Node
MSP	Message Specific Puzzle
PKC	Public Key Cryptography
RH	Received Hop counter
TESLA	Timed Efficient Stream Loss-tolerant Authentication
WSNs	Wireless Sensor Networks

SECURING WIRELESS SENSOR NETWORKS AGAINST DENIAL OF SERVICE ATTACKS

By
Ola Karajeh

Supervisor
Dr. Iman Al-Momani

Co-Supervisor
Dr. Hazem Al Hiary

ABSTRACT

Broadcast authentication is an important process that is used to secure network's applications from different kinds of attacks including Denial of Service (DoS) attacks. Timed Efficient Stream Loss-tolerant Authentication (TESLA) and digital signature are used in Wireless Sensor Networks (WSNs) to provide broadcast authentication, but both are still vulnerable to DoS attacks. Attackers keep broadcasting huge number of forged messages that will exhaust such resource-constraint networks, shortening their expected lifetime. Many schemes were proposed in the literature to secure this broadcast authentication. Some of them tried to contain the effect of DoS attacks to involve only a small portion of the network and others tried to prevent them from happening.

This research proposes a hybrid solution that can prevent and detect the DoS attacks that are launching against broadcast authentication in WSN. The proposed scheme is named Intrusion Prevention Detection based Scheme (IPDS). It consists of two main parts; prevention and detection. The prevention part is based on the adaptive window scheme which is installed at each sensor node. In the detection part, a Fuzzy Logic based Intrusion Detection Scheme (FL-IDS) is proposed and installed at monitor nodes only. This part uses the information available from the prevention part and utilizes Fuzzy Logic Inference System (FIS) in order to make the final decision about the attacker. By utilizing the fuzzy logic, the proposed system achieves a high detection rate by considering factors such as: the total number of received faked messages, accumulative counter of the difference between Estimated Window size (EW) and the Received Hop counter (RH), and the mismatching value in the Estimated Window size (EW) and the received window size (W). The introduced detection part uses specification-based detection policy that depends on defining a set of rules for the attackers, and then checking the behavior of nodes against these rules in order to detect the abnormal behavior.

The proposed scheme in this research (IPDS) is evaluated by comparing its behavior with other schemes (adaptive window, dynamic window and authentication first schemes) in terms of the average broadcast delay of authentic messages and the energy consumption. The performance evaluation of the proposed scheme showed that the IPDS outperforms the other schemes by reducing the average broadcast delay of authentic messages by up to 55% compared to adaptive window scheme, up to 65% compared to dynamic window scheme and by up to 90% compared to authentication first scheme. The IPDS is also found to minimize the wasted energy consumed in receiving faked messages by up to 90% and that in forwarding them by up to 73% when compared to adaptive window scheme. On the other hand, the wasted energy consumed in receiving faked messages is found to be minimized up to 98% and that in forwarding them up to 98% when compared to dynamic window scheme.

1. INTRODUCTION

This chapter starts with the motivations and objectives behind this research followed by the problem statement. It also briefly mentions the contributions and the research methodologies used in this study. Finally, the chapter ends with thesis organization.

1.1 Research Motivation and Objectives

Wireless Sensor Networks (WSNs) are currently deployed in many variant applications such as military, medical, emergency and civilian areas. The sensors used in such networks are usually resource-constraint regarding the power, transmission rate, available bandwidth and computation ability. The usual communication approach in WSNs is broadcasting request/command from the Base Station (BS) to sensor nodes, and then the sensor nodes respond to these requests. As this communication process is vulnerable to attackers, such broadcast orders must be authenticated to make sure that they are really sent from BS and not from intruders. The WSNs are usually deployed in wide geographical areas, therefore, the broadcast operation is often performed in relay fashion; the intermediate node will participate in forwarding messages to farther nodes that do not have direct connection with the BS.

Many broadcast authentication approaches have been suggested in the literature. All these approaches must satisfy the asymmetry property to check the identity of the BS. The most well known approaches are the digital signature and Timed Efficient Stream Loss-tolerant Authentication (TESLA). In digital signature the asymmetry property is implicitly provided by Public Key Cryptography (PKC). In which, the real time-broadcast authentication can be achieved for time sensitive applications. But these operations are

expensive in terms of energy consumption and processing time. TESLA is a very important broadcast authentication approach that depends on one-way hash chain. Although TESLA is classified as symmetry approach, it provides asymmetry property by delaying the disclosure of authentication (symmetric) keys; i.e. it uses the uniqueness of key per time-interval. This property is undesirable in case the message is time sensitive broadcast message.

Although these authentication approaches are used to secure WSN from different kinds of attackers, and even with the suggested schemes in literature to secure these approaches, Denial of Service (DoS) attacks still form a great challenge. This challenge forms a great motivation to maximize the security of such resource-constraint networks.

1.2 Problem Statement

Despite the great technical advancement that network security had witnessed during the last few years, and in parallel with the increased deployment of WSN in variant sensitive applications; DoS attacks can still form a great challenge. They can deplete the energy of sensor nodes by forcing them to perform unnecessary huge number of false verifications and huge number of forwarding and receiving faked messages. They can also prevent authentic messages from being received by sensor nodes and thus delay the response from them back to the BS.

When digital signature authentication approach is used, attackers can keep injecting huge number of faked messages to enforce sensor nodes to perform huge number of signature verifications. On the other hand, when TESLA authentication approach is used, attackers can enforce sensor nodes to forward huge number of faked messages. Such actions will

allow the spread of faked messages throughout the network, targeting huge computation and communication overhead, depleting the battery power of sensor nodes, ending with the violation of the availability of WSNs.

Upon receiving faked messages, when digital signature broadcast authentication approach is used, if the sensor nodes forward them immediately to their neighbors before the authentication process (sensor nodes are in forwarding first mode), then faked messages will spread across the network. This will consume more sensor's energy. Even though the sensors will finally drop the message after the verification process, at that time the WSN will have already-depleted resources.

On the other hand, if the sensor nodes verify every message before forwarding it (sensor nodes are in authentication first mode), then faked messages will be filtered out by the first hop neighbors of the attacker, so farther nodes will not be affected. Therefore, this mode is very good in filtering out faked messages, but it introduces a significant amount of delay on authentic messages.

1.3 Contributions

Many solutions had been proposed in the literature to secure broadcast authentication in order to avoid unnecessary verification or forwarding of broadcast messages. Some of them aimed at containing the effect of DoS attacks to involve a small portion of the network, and others tried to prevent such attacks from launching against broadcast authentication approaches in WSNs. But, till this moment, there is no absolute solution that can detect and exclude DoS attacks from exploiting the broadcast authentication process.

Therefore, this research aims at proposing a hybrid solution that can prevent and detect DoS attacks that launching against broadcast authentication in WSN.

The proposed scheme in this research is named Intrusion Prevention Detection based Scheme (IPDS). It is planned to be based on two parts: prevention and detection parts. In the prevention part, the adaptive window scheme proposed by (Al-Momani, et al., 2010) is used as first line of defense that can reduce the damage of DoS attacks to involve only a small portion of the network. This part is installed in each sensor node. In the detection part and per each monitor node, a proposed Fuzzy Logic based Intrusion Detection Scheme (FL-IDS) is used as second line of defense. This second defense mechanism depends on the available information produced by the adaptive window scheme (the prevention part used in this research) and utilizes the Fuzzy Logic Inference System (FIS) in order to make decision about the attacker.

In terms of the average broadcast delay and energy consumption, the IPDS was found to reduce the average broadcast delay of authentic messages by a percentage that reached up to 55%, 65% and 90%, compared to the adaptive window, dynamic window and authentication first schemes, respectively. Furthermore, the IPDS reduced the energy wasted in receiving faked messages by up to 90%, 98%, as well as the energy wasted in forwarding them by up to 73%, 98%, compared to the both adaptive window and dynamic window schemes, respectively.

1.4 Research Methodology

In this research, the following research methodology steps are followed:

1. Building a strong background about WSNs.

2. Studying the needs to secure these networks against different type of attackers (such as DoS attackers).
3. Collecting related information about the problem and organize them in a scientific manner.
4. Reviewing the related works which tried to prevent and detect the effect of DoS attacks in WSNs.
5. Defining the shortcomings existed in the current mechanisms that tried to prevent and detect DoS attacks in WSNs.
6. Proposing a secure mechanism that can protect WSNs form different kinds of DoS attacks.
7. Implementing and executing the proposed mechanism. This simulation is performed using Matlab.
8. Studying and evaluation the results and comparing them with related works.
9. Writing and documenting this research including the entire previous steps combined with the results.

1.5 Thesis Organization

The rest of this thesis is organized as follows:

Chapter 2 presents the main characteristics of WSNs and its applications, challenges and its vulnerability to different kind of attacks. It also describes how DoS attacks threaten the WSN. It also introduces the two main broadcast authentication approaches (digital signature and TESLA). It also reviews some of the proposed techniques in the literature that tried to prevent or detect the DoS attacks in WSNs.

Chapter 3 presents the proposed scheme (IPDS) in this research. This chapter starts by describing the system model of the proposed scheme, and then it explains the two main parts of this scheme; the prevention part and the detection part. Finally, it describes the system proposed in the detection part (FL-IDS) in details.

Chapter 4 presents the proposed IPDS system evaluation. It starts by describing the simulation environment and the evaluation metrics used in this research which are the degree of energy consumption in sensor networks and the average broadcast delay that introduced on authentic messages. Then, it describes the parameter values used in simulation such as the network size, the monitor nodes percentage and the maximum window size. Finally, this chapter analyzes the behavior of the proposed scheme (IPDS) by comparing its behavior with that of other schemes such as the adaptive window scheme and dynamic window scheme in terms of energy consumption and average broadcast delay on authentic messages.

Chapter 5 summarizes the work presented in this research by highlighting the contribution, together with the discussion of future works.

2. Literature Review

In this chapter, we present two main sections, the first one is the background and the second one is the related works in which we review many related techniques in the literature that tried to prevent and detect DoS attacks.

2.1 Background

In this section, the WSNs characteristics and applications are discussed, and then the threat of DoS attacks against WSNs is illustrated clearly. The section ends with a brief introduction about the most well known broadcast authentication approaches (digital signature and TESLA).

2.1.1 Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are type of wireless networks that consist mainly of resource-constraint devices (sensors) and a small number of powerful devices called BS. WSNs Medium Access Control specifications are defined in IEEE 802.15.4. Sensors are resource-constraint devices; they have limited resources such as limited processing capabilities, memory and power supply (work on battery) that results in low transmission range (small number of nodes will receive the message from a particular node as they usually communicate through low-power wireless links). Generally, the power consumption depends on the nature of the operation that is performed by the sensor. For example, while receiving a packet consumes more power than being in the sleep mode, verifying authenticity consumes much more than receiving process. This means that heavy operations exhaust the battery of the nodes, so that the unnecessary operations must be avoided, as the few light operations lengthen the lifetime of the network, i.e. increasing the

network's lifetime could be achieved by keeping the nodes in sleep mode, when they are not performing any necessary operations (Raymond and Midkiff, 2008), (Wood and Stankovic, 2002) and (Sabbah and Kang, 2009).

Sensors usually perform few operations such as reading the surrounding environment (sensing), and then transfer data to the BS which in turn takes the data as input for specific larger process. On the other hand, BS usually performs a huge processing for the main application (Raymond and Midkiff, 2008) and (Wood and Stankovic, 2002).

The dominant communication type in a standard WSN is the broadcast communication, the BS broadcasts messages to all nodes (either flooding or probabilistic broadcasting), so that broadcast messages must be authenticated before taking the data in consideration (Ning, et al., 2008).

WSNs have been used in wide different critical areas such as: medical monitoring, homeland security, industrial automation, military applications (ex: battlefield surveillance, monitoring critical infrastructure), monitor environmental infrastructure and resources, and tracking (Raymond and Midkiff, 2008), (Wood and Stankovic, 2002) and (Akyildiz, et al., 2002).

The inherent limited resources and weaknesses of WSNs make them vulnerable to different kinds of attacks. To explain, the inability to secure the medium (shared with all wireless networks), makes it possible for the network to be deployed in insecure or even hostile area so that it can be easily tampered and destructed. In addition, it is easy to be targeted by resource consumption. Moreover the attackers are not necessary resource-constraint, so that they are easy target to the DoS attacks. Due to the sensitivity of the WSNs'

applications and their vulnerabilities, they need to be secured from different types of security attacks.

2.1.2 Denial of Service Attacks (DoS) against Wireless Sensor Networks

The main aim of the DoS attacks is to hit the availability security requirement defined by the ITU-T Security Architecture (ITU-T X.800, X.805). DoS attack targets the network and seeks to disturb network survivability. An attacker can send a large amount of data to a sensor node causing it to deplete its energy and make it down. Although DoS attack could threaten all kinds of networks, the wireless networks are specifically vulnerable due to the open nature of the wireless media. Therefore, WSN is considered an easy target for DoS attacks because of their resource constraints.

Various types of DoS attacks can be launched at different layers of the TCP/IP stack, for each layer there is a different mechanism to defend against the DoS attacks (Raymond and Midkiff, 2008). Table 1 summarizes the possible DoS attacks in WSN and proper defending mechanisms. As indicated in this table, most of the defense mechanisms depend on the authentication process.

DoS attacks can affect the network in many ways and they are easily accomplished against the WSN, as simple as possible. But the most serious threat that may damage the network can be performed by exploiting the authentication process. Broadcast authentication is a vital process that is used to secure the applications from different kinds of attacks including DoS attacks. TESLA and digital signature are used in WSNs to provide broadcast authentication, but both are still vulnerable to DoS attacks; attackers keep broadcasting forged messages which will cause extra cost on the network due to the power

consumption. This will exhaust the node's energy, which consequently shorten the network's lifetime (Ning, et al., 2008).

Table 1: Denial of Service against WSN: Attacks and Defenses

Layer	Attacks	Defenses
physical	Jamming	Detect and sleep Route around jamming region
	Node tampering or destruction	Hide or camouflage nodes Tamper-proof packaging
Link/MAC	Interrogation	Authentication and antireplay protection
	Denial of sleep	Authentication and antireplay protection Detect and sleep Broadcast attack protection
Network	Spoofing, replaying, or altering routing control traffic or clustering msgs	Authentication and antireplay protection Secure cluster formation
	Hello floods	Pair wise authentication Geographic routing
	homing	Header encryption Dummy packets
Transport	SYN(Synchronize) flood	SYN cookies
	Desynchronization attack	Packet authentication
Application	Overwhelming sensors	Sensor tuning Data aggregation
	Path-based DoS	Authentication and antireplay protection
	Deluge (reprogramming)attack	Authentication and antireplay protection Authentication streams

2.1.3 Broadcast Authentication Approaches

This section presents a brief overview about the two most useful authentication approaches in Wireless Sensor Network which are Digital Signature and μ TESLA.

2.1.3.1 Digital Signature Approach

Initially, the digital signature that is based on PKC is considered an impractical operation in WSNs due to the high computations needed to perform it on resource-constraint resources (Revest, et al., 1978) and (Stanliings, 2007). However, recently with more optimized digital signature techniques and more modern devices being developed, studies show that it is possible to perform PKC on resource-constraint sensors (Ning, et al., 2008). For example, the verification of Elliptic Curve Digital Signature Algorithm (ECDSA) using 160-bit elliptic curve on Atmega 128 processor (which is used in many sensor networks) will take only 1.62 seconds (Gura, et al., 2004).

In this approach the sender (BS) signs the message with its private key before the sending operation, and then the receivers (sensor nodes) verify the signature with BS's public key (assuming that the keys are distributed previously). There are several advantages of this approach such as: it allows immediate verification as the packet arrives, it provides no additional authentication delay and increases the response time to broadcast message. On the other hand, the disadvantage of this approach is that it is a heavy operation for both sender and receiver, and so it requires expensive energy consumption and running time (Ning, et al., 2008).

2.1.3.2 Timed Efficient Stream Loss-tolerant Authentication (TESLA) Approach

TESLA or any of its variations such μ TESLA uses one-way key chain. Although μ TESLA approach is based on symmetric cryptography, it provides asymmetric property by delaying the disclosure of authentication (symmetric) keys (Perrig, et al., 2002). This approach uses one-way key chains to generate set of keys. The sender generates this chain by choosing a random value K_n which will be the last value in the key chain, and then the sender repeatedly applies the hash function F , which is one way hash function, to compute the remaining keys in the chain, as shown in Figure 1.



Figure 1: An example of one-way key chain

Note that K_0 , which is called the seed of the chain, is previously distributed to all possible receivers, thus the seed is known to all sensor nodes before communication started. With the hash function F , it is easy to compute all the previous keys (of K_i for example), but it is computationally infeasible to compute any of later ones. So the receiver can authenticate any key in the chain by repeatedly applying the hash function. In the sender side, μ TESLA partitions the broadcast time into multiple time intervals and gives every time interval a unique key from the chain. All broadcast messages in a specific time interval are authenticated with the same key specified to that time interval. As we see in Figure 2, P_1 (packet₁) and P_2 (packet₂) are sent in the intervals (I_1) and (I_2), so they are authenticated with keys K_1 and K_2 , respectively, (have not yet disclosed).

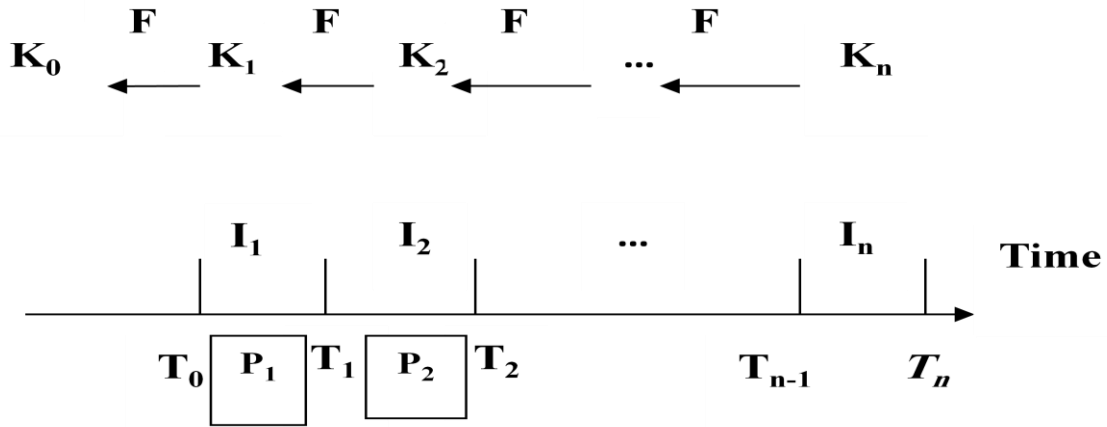


Figure 2: Time intervals for each key

In the receiver side, when the receiver receives a packet in the i -th time interval (I_i); it firstly checks its security condition (if the sender has not disclosed the K_i). When this condition is satisfied, then the receiver accepts and buffers this packet and will authenticate the packet later when it receives the disclosed authentication key. If the security condition is not satisfied, the receiver drops the packet. The main drawback of μ TESLA is the delaying of the authentication process. So the sensor nodes have to forward the packets without authenticating them, which in turn forms a big chance for an attacker to forge large number of packets and force the sensor nodes to forward them and this will consequently deplete their battery power (Ning, et al., 2008).

Compared with digital signature approach, TESLA-based approaches are more conservative (consumes less resources) because they are based on symmetric cryptography, much more efficient and less power consuming. The disadvantages of this approach are the requirement of synchronization between sender and receiver before beginning transmission, the delaying of the authentication process, the inefficiency for real

time applications and the requirement for buffer in the sender to hold the chain (Ning, et al., 2008).

As mentioned before, both approaches (the digital signature and TESLA) are vulnerable to DoS attacks; attacker can send huge number of bogus messages to force nodes to perform signature verification (in case of using digital signature) or packet forwarding (in case of using TESLA). So we still need to protect WSNs against DoS attacks.

2.2 Related Works

Generally, network security mechanisms can be classified into two categories: prevention-based techniques and detection-based techniques. The prevention-based techniques (including authentication and encryption) are usually used as the first line of protection against attackers; they are specialized to prevent the outside attacker. On the contrary, the detection-based techniques are used as a second defense mechanism to identify and exclude the inside attackers (Onat and Miri, 2005).

The sensitivity of WSN applications necessitate the need to optimize the security mechanisms that are used in such resource-constraint networks. These mechanisms must protect the networks against multivariant attacks, including DoS attacks which target the network availability by overloading or crashing the target sensor node with a huge number of messages, and causing it to go down. So WSNs need a mechanism that provides a strong protection and takes into account the limited resources that WSNs suffer from.

2.2.1 Prevention-based Techniques

Many solutions have been proposed to prevent, resist or contain DoS attacks against broadcast authentication in WSNs, thus preventing unnecessary authentication verification

which consumes the sensor nodes resources. They differ in assumptions and purposes, in addition to many various criteria. Thus they can be distinguished as hop-by-hop schemes proposed by (Dong, et al., 2008), (Du, et al., 2008) and (Huang, et al., 2008), and not hop-by-hop schemes proposed by (Ning, et al., 2008). With hop-by-hop, intermediate nodes are participating in DoS resistance, whereas with not hop-by-hop only the BS affords the DoS resistance mechanism.

Luk, et al. (2006) summarized seven properties that are cardinal for any accepted broadcast authentication scheme in WSN. These are: resistant to compromised nodes, low communication overhead, low computation overhead, robustness to packet loss, immediate authentication, message are at irregular time and high message entropy. Most current schemes can satisfy at most six of them. The digital signature for example, satisfies all of the cardinal properties except low computation overhead.

Ning, et al. (2008) proposed Message Specific Puzzle (MSP) which is used to mitigate DoS attacks. This technique adds a weak authenticator to every broadcast message. This weak authenticator is not a replacement of the broadcast authentication approaches (digital signature and TESLA); instead, it is used as filter to differentiate the forged broadcast messages. When a sensor node receives a broadcast message, it first checks the weak authenticator, and only when it is valid, the sensor node performs the signature verification or packet forwarding – either using digital signature or TESLA. This approach has two limitations: It requires computationally powerful sender in order to compute the puzzle solution, and it introduces a delay on the sender before sending the packet.

Dong, et al. (2008) suggested to use pre-authentication filters to provide first line of authentication before the main broadcast authenticator (such as digital signature) is applied. Using group-based or key chain-based pre-authentication filters requires keys distribution mechanism between nodes in addition to the re-grouping. The group-based ones, which is needed due to the possibility of compromised nodes within the group, result in a communication overhead due to additional key management mechanisms.

Tan, et al. (2009) illustrated a solution that seeks to provide both confidentiality and authentication to resist possible DoS attacks, for code dissemination process specifically, which is the process of distributing new programs images over WSN in order to update programs' versions. Their approach depends on the idea of chaining, then rely on finding a cipher puzzle to avoid DoS attacks. Compared to MSP proposed by (Ning, et al., 2008), they argue that this approach is better than MSP due to the chaining of hash results of the previous packets.

Huang, et al. (2008) proposed a broadcast authentication scheme, called DREAM, stands for DoS Resistant Efficient Authentication Mechanisms. It contains false packets by frequent use of the "authentication first" mode, in which nodes must verify authenticity of the message before forwarding it and at the same time it allows a small number of packets to be forwarded without verification and thus reducing end-to-end delay. So the remote nodes get the message more quickly. In this solution the sensors periodically exchange hello messages with one hop neighbors, and the one hop neighborhood size is included in each hello message, then these messages must be signed and verified that introduces an extra overhead. DREAM is used in Mobile Ad hoc Networks (MANETs).

The proposed techniques by (Ren, et al., 2009), (Gan and Li, 2009) and (Du, et al., 2008) focused on environment in which nodes know each other in the network or at least the set of its neighbors. Ren, et al. (2009) used the bloom filter to allow nodes to ensure that a certain receiver is part of the network, but bloom filter may result in a false positive, which provides additional security concern. Furthermore, the distribution of new filters to denote changes in the network affords additional communication overhead, thus increasing resource consumption. Similarly, the research proposed by (Du, et al., 2008) depends on nodes to be verifiable by each node of the neighbor set, using a sender-specific one-way chain. Keys in the chain are unique for each node, then each receiver must verify the key according to whom the message been received from. By the issue of distributing nodes identities and corresponding K_0 (commitment value) securely, which would be either public solution or pair wise shared key, they produce computationally and communication overhead, respectively.

Wang, et al. (2007) proposed a hop-by-hop scheme that focuses on the two categories of how nodes acts with the broadcast message; either forward it immediately and then check its authenticity, or check the authenticity first and then forward only if the message is authentic. These modes are called forwarding first mode and authentication first mode, respectively (as shown in Table 2).

The idea behind this solution is to conduct using both schemes, authentication-first with faked message and forwarding-first with authentic messages in order to trade-off delay and power consumption. The sensor nodes shift to authenticate first mode only if they start receiving many faked messages, but will remain in forwarding first mode if the majority of the received messages are authentic. Every sensor node maintains an authentication

window size, on the other hand, every broadcast message saves the number of hops it passed from the last authentication. The sensor decides which mode to use according to a comparative window size-hop count relationship; if the window is larger than the hop count, then it uses forwarding first mode, otherwise, authentication first mode is used.

Table 2: Simple comparison between the two modes

Forwarding First Mode <i>Forwarding message before verifying</i>	Authentication First Mode <i>Verifying then forward the authentic message</i>
<ul style="list-style-type: none"> • Faked message will spread across the network. • A large number of sensors will verify the faked message and eventually will drop it. • In case of authentic message being broadcasting it suffers no delay 	<ul style="list-style-type: none"> • Only first hop nodes will receive the faked message, which will not spread. • Only first hop nodes will verify the message and drop it • in case of broadcasting of authentic message, much delay (increase the response time of the broadcast message), specifically for farther nodes

The updating function of the window size in this scheme is based on Additive Increase Multiplicative Decrease (AIMD) approach. AIMD is a feedback control approach used to control the traffic in the network. The most important application of AIMD is the congestion control, in which AIMD combines the linear increasing for the congestion window and the exponential decreasing when the congestion occurs. For example, (Kesselman and Mansour, 2003) proposed an adaptive AIMD congestion control algorithm that provides high utilization of the bandwidth and achieve fairness between connections. So, when detecting a faked message the window must rapidly decrease, and when authentic message is received increase slowly, so the node is able to tolerate the swapping

between faked messages and good messages. The updating function is as follows: $W = \text{ceiling}(W/2)$ in case of faked message, and $W = W+1$ in case of authentic message.

This solution took into consideration all possible kinds of DoS attacks models, such as all consecutive authentic messages, non-consecutive authentic messages and the mix authentic messages. In the latter, faked messages are not sent after each other, in order to deceive the receiver and make the widow get larger, but even though, the proposed solution can contain the damage of the DoS attack to involve only a small portion of nodes.

Al-Momani, et al. (2010) proposed a new scheme that allows the receiver sensor node to recognize forged message before verifying its authenticity in order to avoid performing many unnecessary operations. This prevents DoS from damaging the availability of the network and additionally reduces the delay that results from the verification itself. The proposed scheme protects nodes by using adaptive window that is based on the scheme proposed by (Wang, et al., 2007).

The adaptive window scheme checks the probability of the message M if it is faked, so that it is needed to be authenticated first, or if it is probably authentic and thus can be forwarded to other nodes first without verification to minimize the broadcast delay. Similar to dynamic window scheme suggested by (Wang, et al., 2007), each sensor node has a parameter (W) that represents the maximum number of hops (H) with which the broadcast message can be forwarded without being verified (the broadcast authentication approach used in both schemes is the digital signature).

As shown in Figure 3, hops counter (H) on each message must be verified against the locally stored window (W), if $H \geq W$ then the node should verify the authentication of the

message. After that, if the message is positively authenticated, then it will be forwarded after setting the message's hops counter $H=0$, indicating that the message has just been authenticated, and the window size updated increasingly. On the contrary, if the message is negatively verified, then the message will be dropped and the window size updated decreasingly. Window size update will be as the following equation:

$$cw = \alpha cw + (1 - \alpha)AIMD_W$$

Then,

$$W = round(cw) \quad (1)$$

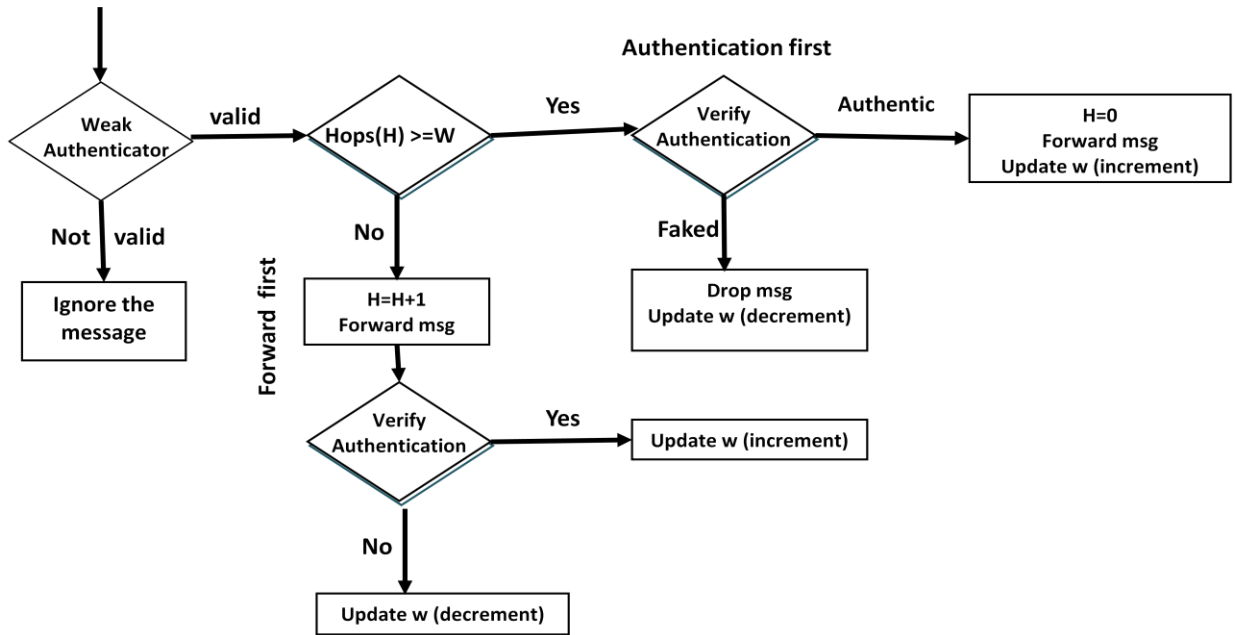


Figure 3: The adaptive window scheme flow chart

Where cw is the current window that is calculated by the proposed algorithm, $AIMD_W$ is the window size that is computed according to AIMD approach, in which $W = \text{ceiling}(W/2)$ in case of faked message, and $W = W+1$ in case of authentic message; (W) is the final value that is compared to Hops.

The value (α) is recommended to differentiate authentic from faked message as follows:

$$\alpha = \begin{cases} 0.6, & \text{if } msg \text{ is faked} \\ 0.5, & \text{if } msg \text{ is authentic} \end{cases} \quad (2)$$

Figure 4 shows the adaptive window scheme algorithm, in which (α) is chosen to be (0.6) with faked messages so that the AIMD_W, upon receiving faked message, takes higher ratio than when receiving an authentic one. These ratios can be changed according to the broadcast nature of the application and the network. Heavy broadcast and more physically secured network such in sensors in a secured homeland area; will use lower α in order to be highly affected by the hops.

As equation (1) indicates, receiving two consecutive authentic messages will affect the window to be increased by (1). The ratio must be chosen carefully to guarantee that the window is not decreased dramatically as the case in the dynamic window scheme which causes more delay. Table 3 demonstrates the notations and parameters used in adaptive window scheme.

Table 3: Notations and Parameters used in adaptive window scheme

Item	Attributes
M	Broadcast message
BA	Broadcast Authenticator
i	Index from the chain
K_i	Key i, from the one-way chain
W	The window to be compared against the hops
cw	The current window, could be decimal
AIMD_W	The window size that is computed according to AIMD approach
H	Hop counter on the broadcast message
α	$0 < \text{Ratio} < 1$
Hash(K_i)	Hash function used in the key chain

Algorithm: adaptive window-based scheme on receiving broadcast message, in a sensor node.

```

Input: msg ( i, M, BAi, Ki, H)
1: msg = ( i, M, BAi, Ki, H)
2: if Hash(Ki) = Ki-1 Then
3:   if H >= W Then //Authentication first mode
4:     Validity=Check_Broadcast_Authenticator (BAi);
5:     if Validity is true Then
6:       H = 0; msg = ( i, M, BAi, Ki, H);
7:       forward msg;
8:       AIMD_W = cw + 1;
9:       α = 0.5;
10:    else // Validity is false
11:      drop msg;
12:      AIMD_W = cw / 2;
13:      α = 0.6;
14:    end if;
15:  else // H < W
16:    H = H + 1;
17:    forward msg;
18:    Validity=Check_Broadcast_Authenticator (BAi);
19:    if Validity is true Then
20:      AIMD_W = cw + 1;
21:      α = 0.5;
22:    else // Validity is false
23:      drop msg;
24:      AIMD_W = cw / 2;
25:      α = 0.6;
26:    end if;
27:  end if;
28:  Update w :
29:    cw = α*cw + (1- α)*AIMD_W;
30:    W = round (cw);
31: else // the Ki is not valid in the chain
32:   drop msg;
33: end if;
34: Return W;

```

Figure 4: The adaptive window scheme algorithm description (Al-Momani, et al., 2010)

2.2.2 Detection-based Techniques

Intrusion Detection System (IDS) is a security mechanism used to protect WSNs by collecting a sufficient amount of network data in order to detect the abnormal activities of sensor nodes and takes the appropriate action. The IDSs suggested for the other networks types (such as ad hoc network) cannot be applied to WSNs due to the resource-constraint (Farooqi and Khan, 2009).

Initially, IDS approaches are considered impractical in WSNs due to high computations required to apply such systems. WSNs are usually used for military applications such as battlefield environment and tracking the movements of the enemy. Therefore, it is worthy to use IDS approaches even they are computationally expensive. However, recently with the more modern sensor devices being developed with their high capabilities (in terms of memory, battery and processor), studies show that it is feasible to apply IDS on these sensor nodes (Farooqi and Khan, 2009).

The part of the IDS that is responsible for analyzing the collected data and detecting the intrusion is called the IDS agent. There are three phases of the IDS agent as shown in Figure 5. The first phase is collecting the needed data. The second phase is detecting the intrusion using the selected detection policy. The third one is taking the appropriate actions. There are different approaches to install the IDS agent in WSN (also shown in Figure 5). The first approach is purely distributed IDS in which the IDS agent is installed in each node, it collects and analyzes the data from its neighbors locally. Then the decision about the abnormal behaviors can be performed as individualized or cooperative operation. In the former operation, any node that detects any abnormal behavior of another sensor sends an alarm to the BS. In the latter one, an alarm must be sent to the BS after voting for

the abnormal behavior from a group of nodes. The second approach is to install the IDS agent in the BS. This approach requires an additional routing protocol that collects the network data and analyzes the abnormal behavior of the sensors. The final approach is distributed-centralized IDS in which the agent is installed in monitor nodes only. This approach minimize the overhead that introduced by purely distributed approach (Farooqi and Khan, 2009).

The most important phase in the IDS is the detection process. There are three distinct intrusion detection policies. The first one is the misuse detection policy which is sometimes called signature-based detection policy. The idea behind this method is that some attackers follow the same sequence of steps to do the attacking; this sequence can be used to detect these attackers. This policy has high accuracy but low detection rate, and it can detect most of known attackers, but cannot detect the unknown attackers (Farooqi and Khan, 2009) and (Yan, et al., 2009).

The second policy is the anomaly detection policy that builds a model of normal behavior, and then any unusual deviation from the normal model is declared as attacking. This model can detect the novel attackers and has high detection rate but the false positive rate is high. The final policy is the specification-based detection policy which depends on defining set of rules for the attacker. Each sensor node behavior is verified against these rules. For each node, there is a failure degree; if the node does not satisfy any rule, the failure degree is incremented. After a time interval, if the degree reaches a predefined threshold then an alarm must be generated (Farooqi and Khan, 2009) and (Yan, et al., 2009).

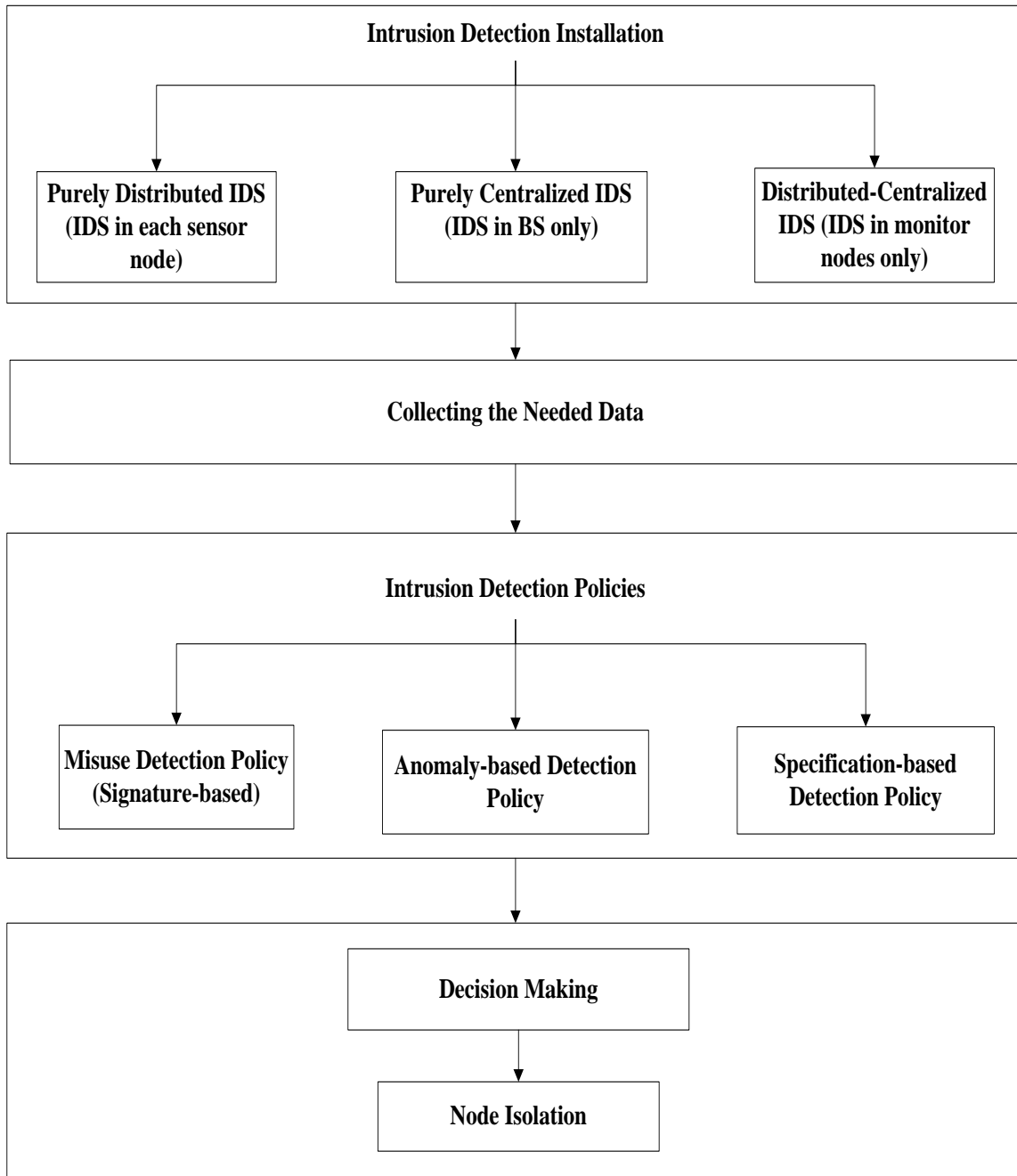


Figure 5: Intrusion Detection Framework

Abduvaliyev, et al. (2010), Hai, et al. (2007) and Yan, et al. (2009) used both anomaly and misuse detection in order to build a hybrid model. The purpose of using this combined version of detection was to achieve the goals of high accuracy and high detection rate. Also, they depend on using Clustered-based Wireless Sensor Networks (CWSNs) as network architecture in order to reduce the communication overhead and energy consumption. (Abduvaliyev, et al., 2010) proposed an architecture of energy efficient Hybrid Intrusion Detection System (eHIDS) for WSNs. eHIDS consists of three models: anomaly detection, misuse detection and decision making models. Firstly, the anomaly detection model checks the packet to find out the abnormal activities. If the intrusion was detected, then the packet is sent to misuse detection model which compares the received information with predefined normal behaviors. After all, the results of both models are sent to the decision making model to make the final decision (Farooqi and Khan, 2009).

Hai, et al. (2007) presented a hybrid and lightweight intrusion detection system. This system depends on a collaborating global agent and a local agent located in the application layer of sensor nodes. The simulation results show that the system performs well even the network is dense.

Yan, et al. (2009) suggested a hybrid intrusion detection system (HIDS) that detects the intrusion efficiently, and avoids wasting the resources of the WSN. Like the system proposed by (Abduvaliyev, et al., 2010), HIDS consists of three models: the first one is the anomaly detection model that uses rule based method in order to analyze packets and determine which packets are abnormal. The second one is the misuse detection model that based on Back Propagation Network (BPN) in order to achieve high accuracy through training the data. The last model is the decision making model that combines the

information resulted from both models in order to make decision about attacking occurrence and classify the type of the attacker. In this model, they used rule based method in building the rules.

Onat and Miri (2005) introduced a novel anomaly based IDS for WSNs. They exploited the properties of WSN such as the lack of mobility of sensor nodes and the stable neighborhood communication in the detection process. This IDS is distributed in each sensor node, but the decision about the attacker is determined in a cooperative manner. The authors assumed that each sensor node has the ability to compute some statistics about its neighboring nodes which can be used later in order to detect the changes on them. The monitoring process is performed through measuring two parameters; the power level of the received packet and the arrival rate in order to make the decision about the attacker.

Martynov, et al. (2007) designed and implemented a preliminary IDS for WSNs which protects these networks against DoS attacks. In order to detect the potential DoS attacks, this IDS used anomaly detection pattern. The main goal of this system is to determine the DoS attackers, thus stopping the communication with the adversary nodes as well as continuing the communication with non-adversary nodes. The system draws a baseline level of network traffic and determines if the DoS attacks exist or not by comparing all coming traffic against the baseline.

Many intrusion detection systems that are proposed in the literature are based on artificial intelligence techniques such as fuzzy logic (Chi and Cho, 2006), neural networks (Tian and Gao, 2009) and clustering algorithm (Jian-hua and Chuan-Xiang, 2008).

Chi and Cho (2006) suggested an anomaly intrusion detection scheme that secures the directed diffusion protocol in WSNs against DoS attacks. In the proposed scheme, each sensor node monitors the behavior of neighboring nodes within its transmission range. Sensors used four criteria to monitor the nodes behavior. These are: node energy level, neighbor node list, message transmission rate and error rate in the transmission. In order to detect the intrusion, a Master Node (MN) or the BS collects the needed information (four criteria) and uses the fuzzy logic in the determination of the detection value. The simulation results show that by using the fuzzy logic, the intrusion detection rate is high.

3. Methodology

The broadcast authentication is an important process that is used to secure the applications from different kinds of attacks including DoS attacks. TESLA and digital signature are used in WSNs to provide broadcast authentication, but both are still vulnerable to DoS attacks. Hence, attackers can inject many forged messages enforcing sensors to perform unnecessary verifications if the digital signature is used as broadcast authentication approach, or to forward the forged messages in case of using TESLA as authentication approach. Consequently, the faked messages can spread throughout the entire network, targeting huge computations, depleting the battery power of sensor nodes, which affects the availability of WSNs.

In order to avoid unnecessary authentication verification of broadcast messages, thus reducing the damage of possible DoS without introducing additional overhead, faked messages must be dropped out before being verified. Therefore, an indicator to such messages is needed. Using authenticating first mode or forwarding first mode approaches alone yields serious problems to the network; each mode is vulnerable to specific attack. Whereas authenticating first results in a long broadcast delay as network gets larger, forwarding first allows spread of faked messages, thus more unnecessary network-wide computation power consumption. That means DoS will affect the availability of the whole network.

Many solutions had been proposed in the literature to secure broadcast authentication in order to avoid unnecessary verification or forwarding of broadcast messages. Some of them aimed at containing the effect of DoS attacks to involve a small portion of the

network, and others tried to prevent such attacks from launching against broadcast authentication approaches in WSNs. But, according to our knowledge there is no absolute solution that can detect and exclude DoS attacks from exploiting the broadcast authentication process. Therefore, this research aims at proposing a hybrid solution that can prevent and detect DoS attacks that are launched against broadcast authentication in WSN.

The proposed scheme in this research is named Intrusion Prevention Detection based Scheme (IPDS). It is planned to be based on two parts: prevention and detection parts. In the prevention part, the adaptive window scheme proposed by (Al-Momani, et al., 2010) is used as first line of defense that can reduce the damage of DoS attacks to involve only a small portion of the network. In the detection part and per each monitor node, a proposed Fuzzy Logic based Intrusion Detection Scheme (FL-IDS) is used as second line of defense. This second defense mechanism depends on the available information produced by the adaptive window scheme (the prevention part used in this research) and utilizes the FIS in order to make decision about the attacker. Therefore, maximizing the security of the broadcast authentication process.

By exploiting the fuzzy logic, the proposed system achieves a high detection rate by considering factors such as: the total number of received faked message, accumulative counter of the difference between estimated window size (EW) and the received hop counter (RH) and the mismatching value in the estimated window size (EW) and the received window size (W). The introduced detection part uses specification-based

detection policy that depends on defining set of rules for the attackers, and checking the behavior of nodes against these rules in order to detect the abnormal behavior.

3.1 Intrusion Prevention Detection based Scheme System Model

This section describes the system model to which the proposed scheme in this research is applied. The sensor nodes used in this research assumed to be identical entities (using the same hardware and run the same protocol stack) and have limited resources such as energy, computational capabilities and transmission range. Broadcast messages are sent from the BS to the entire sensor nodes via the multi-hop forwarding, thus some sensors will forward messages to others. The broadcast messages could be requests or commands. The digital signature is used in this research as broadcast authentication approach. The BS signs the message before sending it, and then the sensor nodes can perform PKC verification to make sure that this message is really sent by the BS. Each node has: public and private keys (signing with the private key and verifying with the public).

For each group of sensor nodes (neighbors), a monitor node is deployed in the area that lies in the transmission range of all nodes in that group. These monitors assumed to be static and trusted as BS, and they have more energy, computational capabilities and longer transmission range than ordinary sensor, so they can monitor everything sent and received by the neighbor sensors (Moon and Cho, 2009) and (Islam, et al., 2010).

Each monitor node has a local database that is used to collect data about its neighbors. Initial windows sizes that are identical to specific windows sizes of the neighbors are stored at their monitor node. This is computed according to the adaptive window scheme.

The architecture of the WSN under which the proposed technique is evaluated is flat. Clustering techniques were used only for IDS (Roman, et al., 2006).

We assume that attacker can launch DoS attacks in a wide range; an attacker can inject faked broadcast messages to fool sensor nodes to verify the broadcast authenticator. We also assume that the attacker can exploit the larger network diameter to isolate farther nodes by fooling them to perform unnecessary computations using the time of broadcast delay.

3.2 Intrusion Prevention Detection based Scheme (IPDS)

As mentioned earlier, the proposed IPDS consists of the prevention part and the detection part. The prevention part is installed at each sensor node while the detection part is installed at the monitor nodes only as shown in Figure 6. The proposed detection system (FL-IDS) in this research could be categorized as distributed-centralized IDS (Farooqi and Khan, 2009). It does not cost the sensors any additional overhead, because its main functionalities are performed only by the monitoring system.

FL-IDS (used in the detection part) uses two Fuzzy Inference Systems that are deployed into two tiers. It is based on three factors to build reputation about its neighbors. It starts by collecting the needed information about the abnormal behaviors of its neighbors, and then takes decision regarding the suspected attackers.

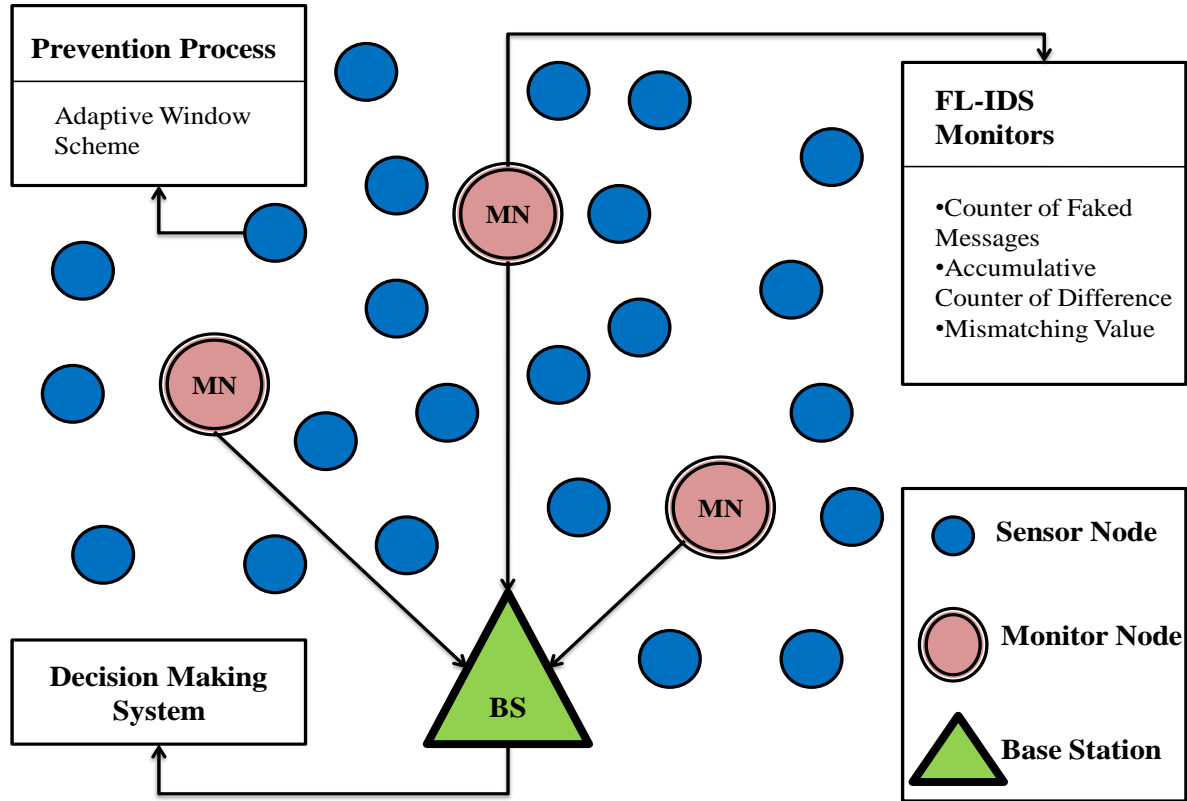


Figure 6: IPDS Architecture

As shown in Figure 7, when a message arrives to the IPDS system the prevention and the detection processes work in parallel. Then, each sensor node will run the prevention process which is based on the adaptive window scheme proposed by (Al-Momani, et al., 2010). Its basic idea depends on that each sensor node has a local parameter called window size (W) which represents the maximum number of hops with which the message can be forwarded without being verified. On the other hand, each message has hop counter (H) that represents the number of hops the message passed by without being verified. By message arrival, the condition (H against W) must be verified. If ($H \geq W$), then the sensor must verify the message before being forwarded, then if the message is authentic, the hop

counter on the message is set to 0, the message must be forwarded and the window size must be updated increasingly. Otherwise, the message must be dropped out and the window size must be updated decreasingly.

On the other hand, if the condition ($H \geq W$) is not valid, then the sensor node will increment the hop counter of the message and forward it before the authentication process. Although this scheme reduces the damage introduced by DoS attacks by containing them temporarily to a small portion of the network, an opportunistic further DoS attacks from the same contained attackers are still forming a threat. This means that after a while of sending a huge number of authentic messages and growing in the windows sizes occurs, contained attackers can again introduce the threat to the network. This necessitate a second line of defense in order to protect these sensors from the adversaries.

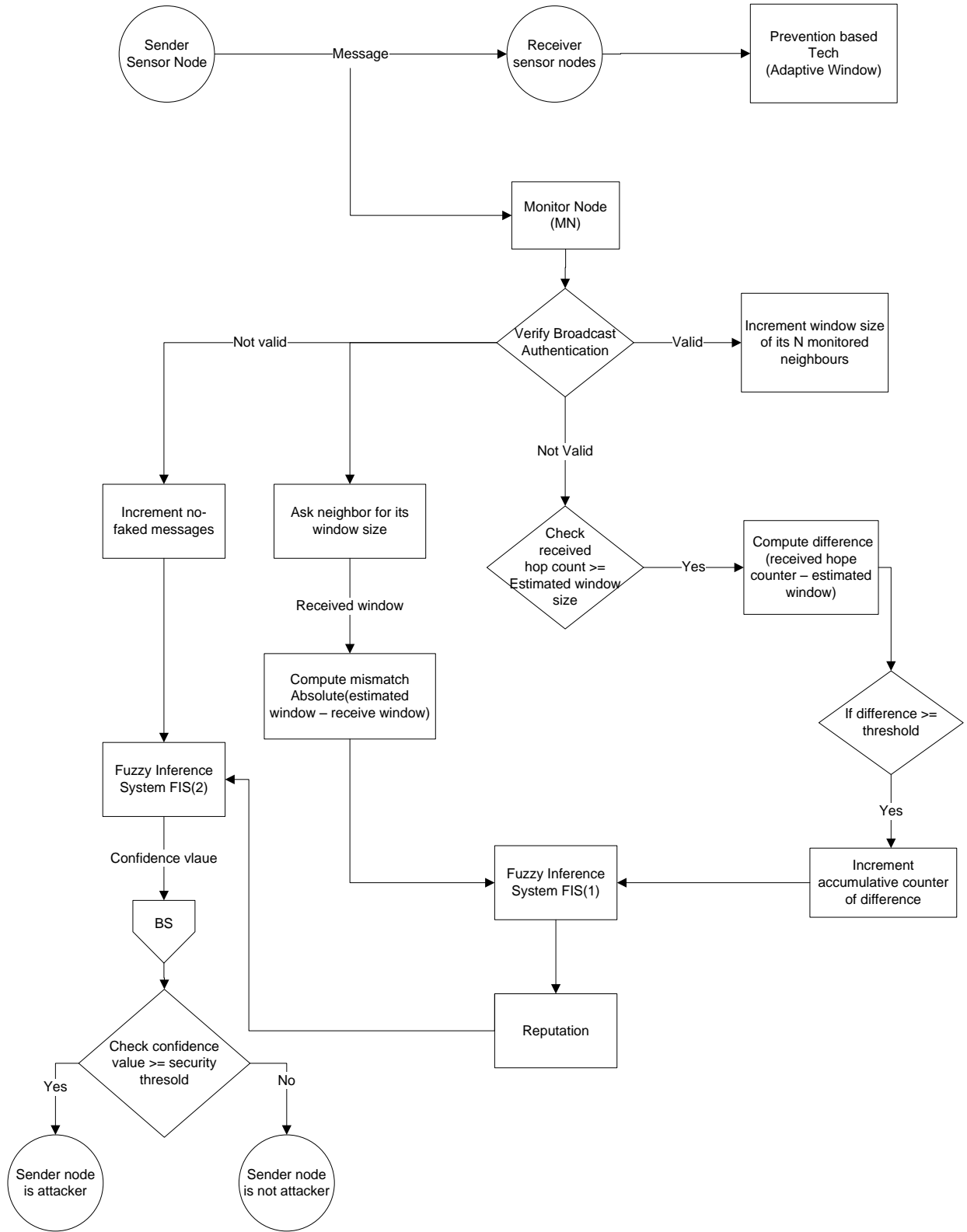


Figure 7: The Proposed IPDS Flow Chart

On the other hand, the monitoring system runs only at monitor nodes, and works in parallel with the prevention process. In the detection part, the proposed FL-IDS uses three factors. The total number of faked messages sent by specific node, the accumulative counter of the difference between the estimated window size that computed by the monitor node and the received hop counter, the mismatching value between the estimated window size and the received window size. The monitor nodes use the specification-based detection system that defines set of rules for the attacker (based on the three factors mentioned above), and the behavior of each sensor node is checked against these rules. If there is any rule that is not satisfied, then the monitor will increment the confidence value for that node of being a malicious node. Accumulatively, if the confidence value exceeds a predetermined threshold value, then the monitor will send alarm to BS indicate the existence of an attacker. This confidence value that determines the existence of an attacker is computed by Fuzzy Logic Inference System.

In the configuration phase of the proposed system, each sensor node is assigned to a certain monitor node. Then each monitor node will store a list of its neighbors and will be responsible to collect the needed information about them and detect any of their bad behaviors. Initially, each sensor node will have a local window size (W) that is generated randomly at this stage and used mainly for the prevention part. On the other hand, each monitor node will store an initial value for the window size for each sensor node in its neighbors list, these window sizes are used for the detection part. At this stage, the initial stored windows sizes in each monitor node must be identical to those of its neighbors.

Upon receiving a message to the FL-IDS, the monitor node will check the validity of the broadcast authentication by verifying the digital signature as shown in the proposed FL-

IDS algorithm in Figure 8. If it is valid, then the monitor node will update the estimated window size (EW) increasingly for all of its neighbors. To update the window size, the monitor node uses the updating function that is used in the adaptive window scheme (prevention part) according to equation (1). The goal of such update is to keep matching between the window size stored by each monitor for its neighbors and the window stored locally in each sensor. This information (window size) will give the proposed system a good indication about the behavior of the nodes; if any mismatching occurs between window size stored locally in sensor nodes and that in their monitor node, this may indicate an attacking opportunity. So the window size is very important factor in the proposed IPDS for the prevention and detection parts. Table 4 demonstrates the notations and parameters used in IPDS.

Table 4: Notations and Parameters used in IPDS

Item	Attributes
M	Broadcast message
BA	Broadcast Authenticator
I	Index from the chain
W	The window to be compared against the hops
CW	The current window, could be decimal
AIMD_W	The window size that is computed according to AIMD approach
H	Hop counter on the broadcast message
A	$0 < \text{Ratio} < 1$
EW	Estimated Window size
RH	Received Hop counter

On the other hand, if the digital signature is not valid, this means that the monitor received a faked message. Consequently, the proposed FL-IDS starts to collect the needed information in order to build a reputation about the forwarder of the faked message, in order to decide if this sensor node is an attacker or not. The decision about the suspicious node will not be determined from the first faked message received from this node, but by continuous tracking of the behavior of this abnormal node for a certain period of time. This means that the proposed FL-IDS will depend on recording an accumulative history to the abnormal behaviors, and then use it in judging and marking the suspicious nodes.

The monitor node has specific counters that count the number of faked messages received by each specific forwarder. Every received faked message from a specific forwarder will increment its specific counter by one unit.

Algorithm1: FL-IDS in each Monitor Node upon Receiving The Broadcast Message from Sensor Node (SN)

Input: msg (i, M, BA_i, H)

```

1: msg = ( i, M, BAi, H)
2: Validity=Check_Broadcast_Authenticator (BAi);
3: if Validity is true Then
4:     // update the window size for all of its neighbors
5:     AIMD_W=CW+1;
6:     assign a proper  $\alpha$  value for authentic messages;
7: else // Validity is false
8:     // computing the first factor
9:     Faked_Messages_Counter(SN)=Faked_Messages_Counter(SN)+1;
10    //computing second factor
11:    if Received Hop>=Estimated Window(SN) Then
12:        Difference=(Received Hop- Estimated Window(SN));
13:        if Difference>=threshold Then
14:            Accumulative_Counter_Difference(SN)= Accumulative_Counter_Difference(SN)+1;
15:        end if;
16:    end if;
17:    // computing third factor
18:    ask forwarder of the faked message for its window size
19:    Mismatching(SN)=|Estimated Window(SN)- Received Window(SN) |;
20:    // send the second and third factor to the first fuzzy system
21:    Reputation(SN)= evalfis(Accumulative_Counter_Difference(SN), Mismatching(SN));
22:    // send the output of the first fuzzy system and the first factor to another fuzzy system
23:    Confidence(SN)=evalfis(Reputation(SN), Faked_Messages_Counter(SN));
24:    //send Confidence(SN) to the BS in order to decide about the attacker
25:    AIMD_W=CW/2;
26:    assign a proper  $\alpha$  value for faked messages;
27: end if;
28: Update W for all of the neighbors of the monitor node:
29: CW= $\alpha$ *CW+(1-  $\alpha$ )*AIMD_W;
30: W=Round(CW);
31: Return W;
```

Figure 8: The Proposed FLIDS Algorithm Description

This forms the first factor in the FL-IDS, but it gives a weak indication to decide about the forwarder of the message. The issue that the forwarder of the message might be just in forwarding first mode; the sensor node had checked the condition ($H \geq W$) in the prevention process (adaptive window scheme) and it was not satisfied, thus forwarded the faked message accordingly. So it is not fair to consider such node as compromised based on this factor, but it will be used in the final decision about the attacker as discussed later.

The second factor is a vital one which is the accumulative counter of difference. This factor depends on comparing the estimated window size (EW; computed by the monitor node for that forwarder) against received hop counter (RH) that was heard by the monitor node from the surrounding environment (by assuming that the monitor node can hear what the sensor node can hear). Accordingly, if RH is greater than or equal to EW ($RH \geq EW$), then this will give the monitor node a strong indication that the forwarder is not a benign node.

To explain this, the monitor node assumes that its EW and RH must match the updated W that stored locally in the forwarder of the faked message and its hop counter H, respectively. If the condition is valid ($RH \geq EW$), then the monitor node will assume that the forwarder of the faked message was in the authentication first mode and the authenticity of the message must be verified before forwarding it, and forward it just if it was not faked. Although the condition ($H \geq W$) in the prevention part was valid, the forwarder of the message forwarded it, and this indicate a bad behavior from this node. Even though, the monitor node will not over judge this node and take any action immediately, instead, the monitor node assumes that there might be a mistake in calculating EW. So, it gives the forwarder another chance by computing the difference

between EW and RH (RH-EW). If the difference is greater than a predefined threshold, then the bad behavior of the forwarder is noteworthy, and then the monitor node will increment the accumulative counter of this difference by one unit for that sensor node in order to record the behavior of this node during a certain period of time. This counter represents the history of the bad behavior of this node. The reason why the monitor node does not consider (RH-EW) difference unless it exceeds a certain threshold, is that the monitor node will take into account the probability of any mistakes in computing the EW, so if the difference is very small, this value will not ensure the occurrence of attacking. The power of such factor is that, if the difference between EW and RH (RH-EW) is greater than a predetermined threshold, this means that RH is greater than EW with a non-negligible value. This difference will give the monitor node a strong indication about the existence of abnormal behavior.

Detecting such behavior assumes an intentional attacking. Nevertheless, this suspicious node will not be judged until its behavior is been tracked for a certain period of time. If the accumulative counter of difference that represents the history of that node is growing with time, then the suspicion about the abnormal behavior of that node is increased.

Upon receiving the faked message and checking the first two factors, the mismatching value must be computed which is the last factor in the FL-IDS. This factor represents the absolute difference between the EW that computed by the monitor node for the forwarder and the local W stored in that sensor node. In order to get this local W value, the monitor node sends a small request message to the forwarder of the faked message in order to request that value. Then the forwarder sends a small replay message with this value. This message must be signed with the forwarder's private key and the monitor node will verify

this message with the forwarder's public key. After that, the monitor node extracts the window size from the verified replay message and utilizes it to compute the mismatching value between the two sizes $|EW-W|$.

If the two sizes are identical, the mismatching value will be zero and this indicates a benign behavior. But if the node is malicious one, then it will send the monitor node unreal window size in order to justify why it forwarded that faked message. That means, it will give a large window size in order to pretend to be a benign innocent node and it is just in forwarding first mode, hence the condition $(H \geq W)$ was not valid in the prevention process. Generally, if the mismatching value is greater than a certain threshold, this will give a high certainty about the existence of attacking and high confidence value about the bad behavior. Also when this factor is very small, it will not be considered as a strong indicator, because of the probability of any mistake in computing the EW.

After the evaluation process of the three factors, the monitor node will update EW for all of its neighbors decreasingly according to the update function used in the adaptive window scheme (equation 1). The reason behind this decreasing is to keep matching with the W stored locally in sensor nodes, and thus monitor nodes can still monitor the behavior of any suspicious nodes with the future incoming messages during the life time of the network.

In this section, the applications of the three factors were discussed separately. But how these results could be interpreted, and how could they be integrated together to assess and finally judge the threat facing WSN, will be discussed in the following subsection.

3.3 Fuzzy Logic based Intrusion Detection System (FL-IDS)

In order to interpret the results obtained from measuring the three factors mentioned earlier, the proposed FL-IDS uses two Fuzzy Logic Inference Systems (FIS) that are implemented in two tiers as shown in Figure 9. The purpose of integrating fuzzy logic with the proposed FL-IDS is to assign the three factors different weights in order to take the final decision about the attacker.

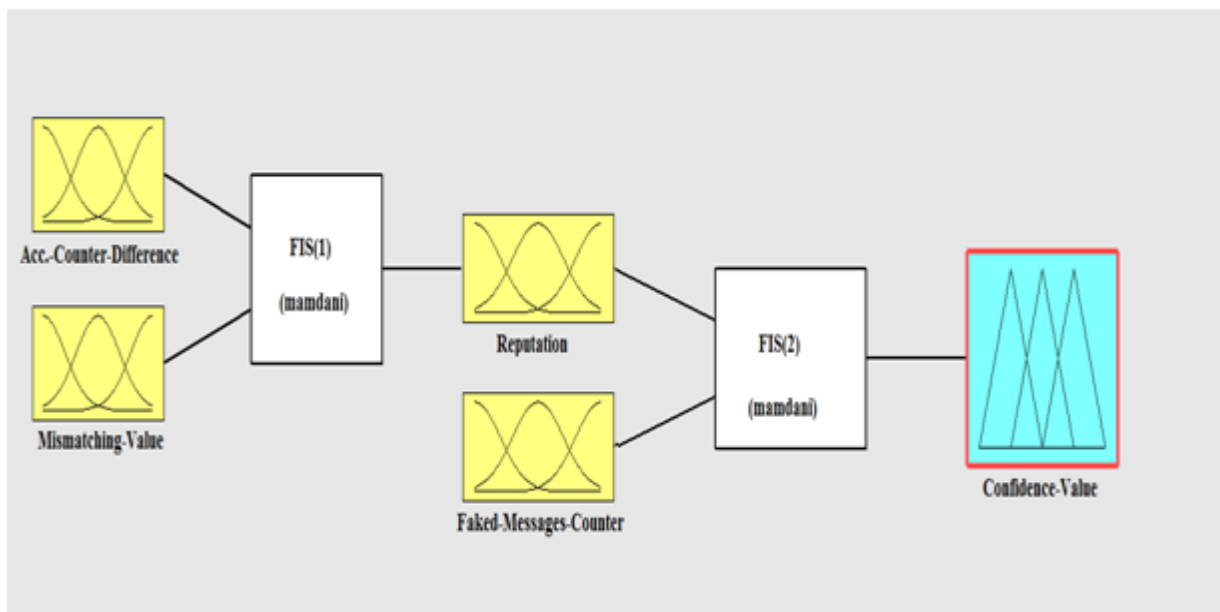


Figure 9: Two Tier FL-IDS

Usually in logic we have a series of statements or actions that are either true or false, 0 or 1, in this context, the statement “ this node is compromised or suspicious “ is an objective one and is either true or false. However, in many situations we cannot just judge the node directly and the answer is more like “that depends”, “maybe” and so on (McNeill and Thro, 1994).

Fuzzy logic deals with uncertainty means we are not sure if the answer is “YES” or “NO” in many fields which security and intrusion detection are part of. However, fuzzy logic has commercial and practical benefits in general. Commercially, fuzzy logic has been used with great success to give very suitable outputs that can better match the ambiguous inputs, not only this but fuzzy logic has also great success when it's implemented, and can be understood and implemented by non-specialists in the used field. In control problems where simplicity and speed of implementation is important then fuzzy logic is a strong candidate. Practically fuzzy logic gives better and accurate outputs and covers ranges of values instead of discrete values like binary logic does, also outputs using fuzzy are smoother means outputs values are somehow continuous and strongly connected to inputs values at anytime (McNeill and Thro, 1994).

Now regarding the motivation behind using fuzzy logic in the IDS rather than binary logic in our context, is that when a node is probable of being compromised we have more judgment parameters that we can adopt rather than just “YES” it's compromised or “NO” it's not, but instead we may deal with :

DEFINITELY YES,

PROBABLY YES,

MAYBE,

PROBABLY NO,

DEFINITELY NO.

So, fuzzy logic copies this feature of human decision making using levels of possibility in a number of uncertain (or fuzzy) categories, and then acts accordingly.

For these reasons, using fuzzy logic is proposed to build the IDS, taking the metrics mentioned earlier as input to the FIS to investigate the seriousness of the generated results. Beside connecting and testing more than one input at the same time to get one output that acts depending on all inputs together.

In more details, the fuzzy logic system requires a definition of the membership functions of all input metrics. In addition, fuzzy rules need to be defined in order to formulate the conditional statements that make the fuzzy inference rules. There are three main steps of the fuzzy inference process involved in this system; the first one is the fuzzification of the input variables which means comprises the process of transforming crisp values into grades of membership for linguistic terms of fuzzy sets. The second one is the implication from the antecedent to the consequent and the aggregation of the consequents across the rules using the rule table. The third one is the defuzzification, where step one takes place in reverse, means converting the fuzzy output values to crisp values back (McNeill and Thro, 1994).

As shown in Figure 10, the first FIS (FIS (1)) takes the accumulative counter of difference and mismatching value factors as input parameters. The output of this FIS (1) is the attacker's reputation value. Then this reputation value is integrated with the counter of faked messages factor to form the input parameters to the second fuzzy system (FIS (2)) in the second tier. The final output of this fuzzy system will provide the confidence value regarding the existence of the attacker as shown in Figure 11 .

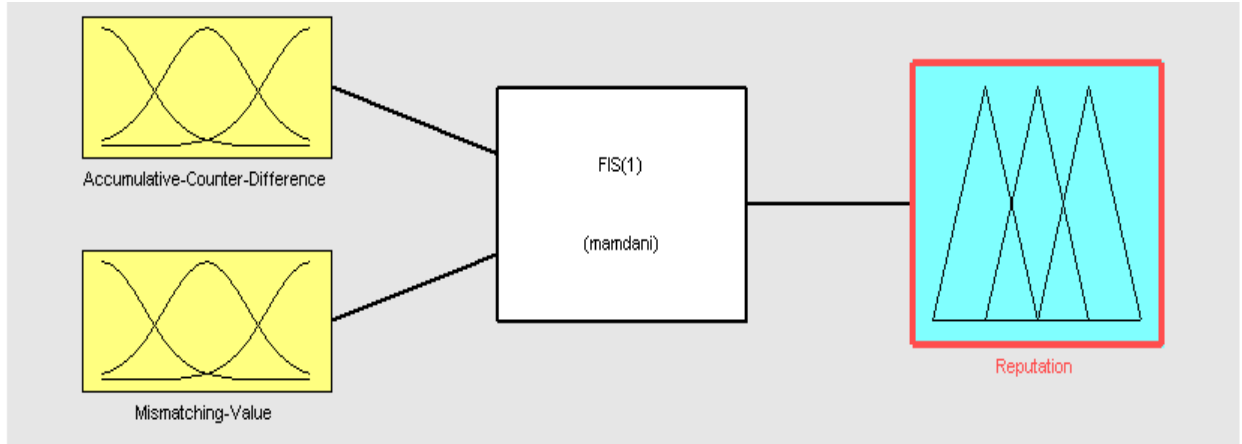


Figure 10: Fuzzy Logic Inference System (1)

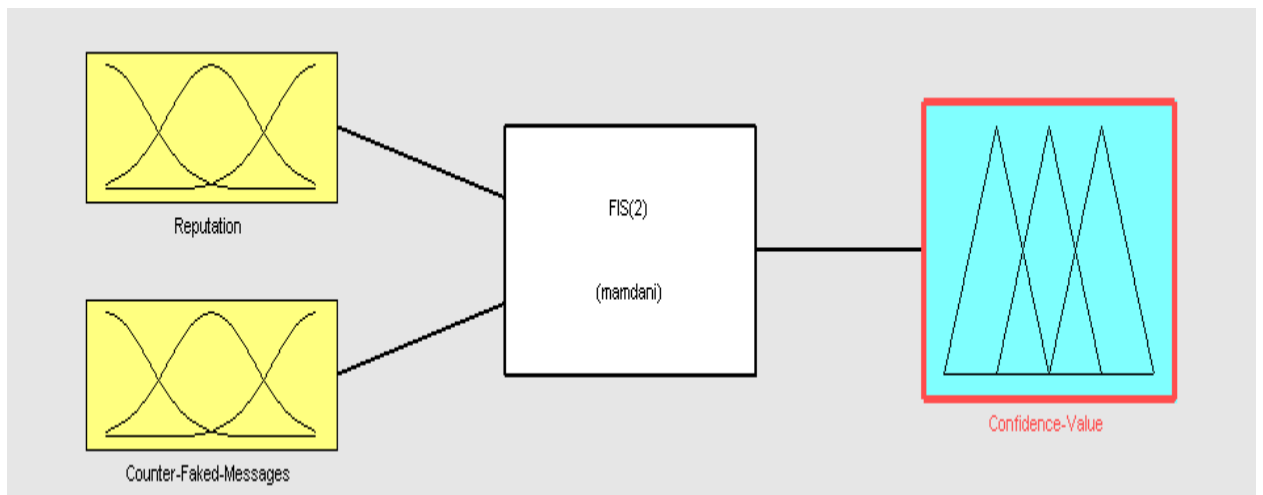


Figure 11: Fuzzy Logic Inference System (2)

Each input and output parameter in FL-IDS will be given a fuzzy membership function according to its value. Figure 12 shows the fuzzy membership function for the accumulative counter of difference that ranges from zero to five. Their assigned fuzzy values are grouped into three main values (Low, Medium and High). If the accumulative counter of difference value is high then the membership function (fuzzy value) is also high.

The maximum value for this factor that can be tolerated by the proposed system is five; that means the system can tolerate only five records on the accumulative counter of difference. For example, if the accumulative counter of difference has a low value (e.g. 1); that means the suspicious node has recorded a large difference between EW and RH, but this was an episodic event that can be tolerated by the proposed system, so the assigned fuzzy value will be low. On the other hand, if the accumulative counter of difference has a high value (e.g. 5), this means that multiple recurrent large RH and EW differences were recorded and this frequency of these recurrent episodes exceeds the predetermined threshold, so the fuzzy value will be high.

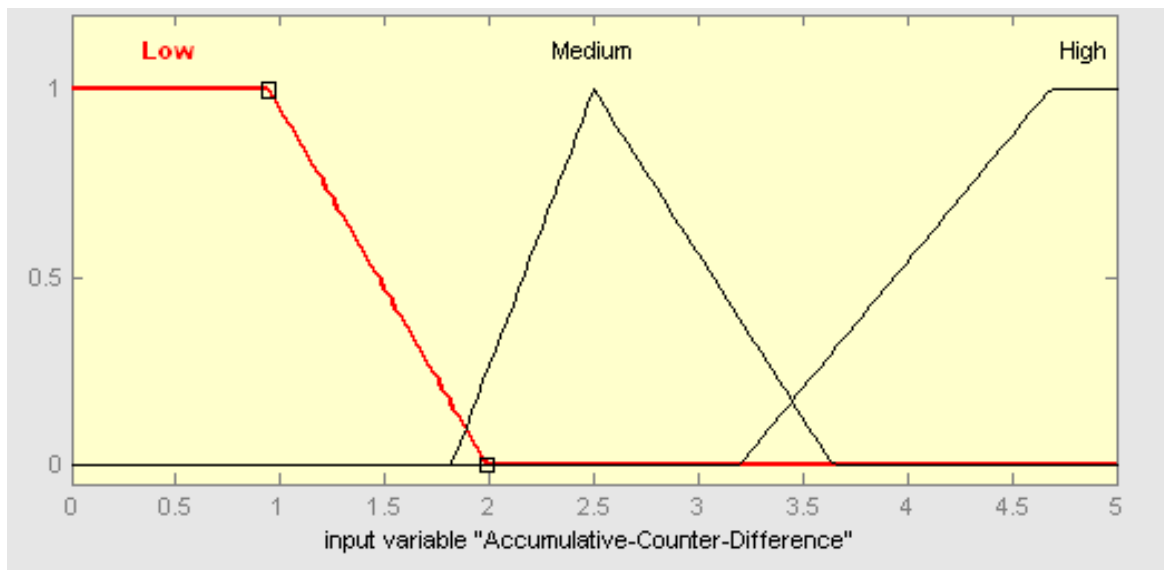


Figure 12: Fuzzy membership function for the accumulative counter of difference factor

Figure 13 shows the fuzzy membership function for the mismatching value that ranges from zero to three. Their assigned fuzzy values are grouped into two main values (Low and High). The higher mismatching value will have a higher membership function value. Unlike the accumulative counter of difference, this factor gives a quick sign about the

existence of bad behavior; it is considered more sensitive metric. So its range is shorter than the accumulative counter of difference range. For example, if the mismatching value is (e.g. 1), then this value will be assigned a low fuzzy value, because the absolute difference between the EW and W is considered low (probability of mistake in calculating EW is present). On the other hand, if the mismatching value is high such as (e.g. 3), then the fuzzy value will be high, because the probability of mistakes is low and the difference between two windows is large. Thus, the probability of the attacking existence is high.

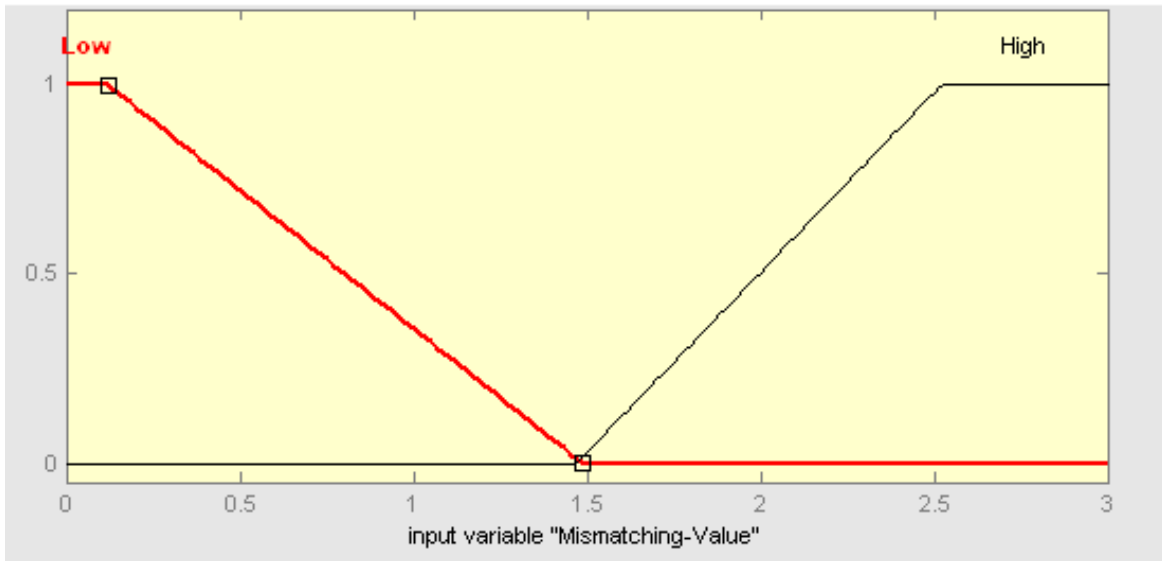


Figure 13: Fuzzy membership function for the mismatching value factor

The obtained results from calculating the accumulative counter of difference and the mismatching value will be entered into the FIS (1) by using the IF-THEN rules. The output of the FIS (1) will be calculated to give the reputation output to that suspicious node which ranges from zero to one. Their assigned fuzzy values are grouped into three main values (Low, Medium and High). The membership function of this output is shown in Figure 14.

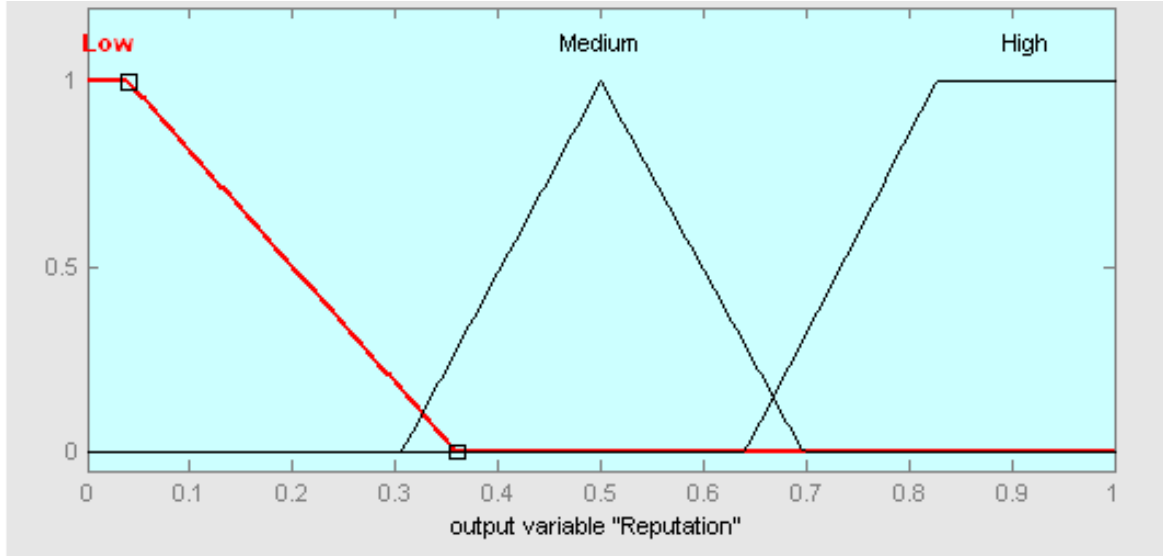


Figure 14: Fuzzy membership function for the reputation output parameter

According to Table 5, if the accumulative counter of difference is low and the mismatching value is high, then the probability that the node is an attacker is high. To explain this; when the mismatching value is high, this means the probability of any mistake in computing the EW is very low, and thus the confidence about the attacker is high. On the other hand, if the accumulative counter of difference is high and the mismatching value is high, the possibility of having an attacker is also high.

Table 5: Fuzzy IF-THEN rules for FIS (1)

		Acc. Counter of Difference Factor		
		Low	Medium	High
Mismatching Factor	Low	Low	Low	High
	High	High	High	High

The second fuzzy system (FIS (2)) represents the fuzzy system in tier two of the proposed FL-IDS. The FIS (2) uses the output of tier one (reputation value) and integrates it with the counter of faked messages as input parameters to this tier. Accordingly, this fuzzy system will give the final confidence value about the existence of the attacker as shown previously in Figure 11.

Figure 15 shows the fuzzy membership function for the reputation value as input parameter in FIS (2). The higher the reputation value, the higher its membership function value. For example, if the reputation has a low value (e.g. less than 0.1); this means the probability of having an attacker is low, so the assigned fuzzy value will also be low. On the other hand, if the reputation value is high (e.g. 0.9), this means the probability of attacking existence is high, so the fuzzy value will be high.

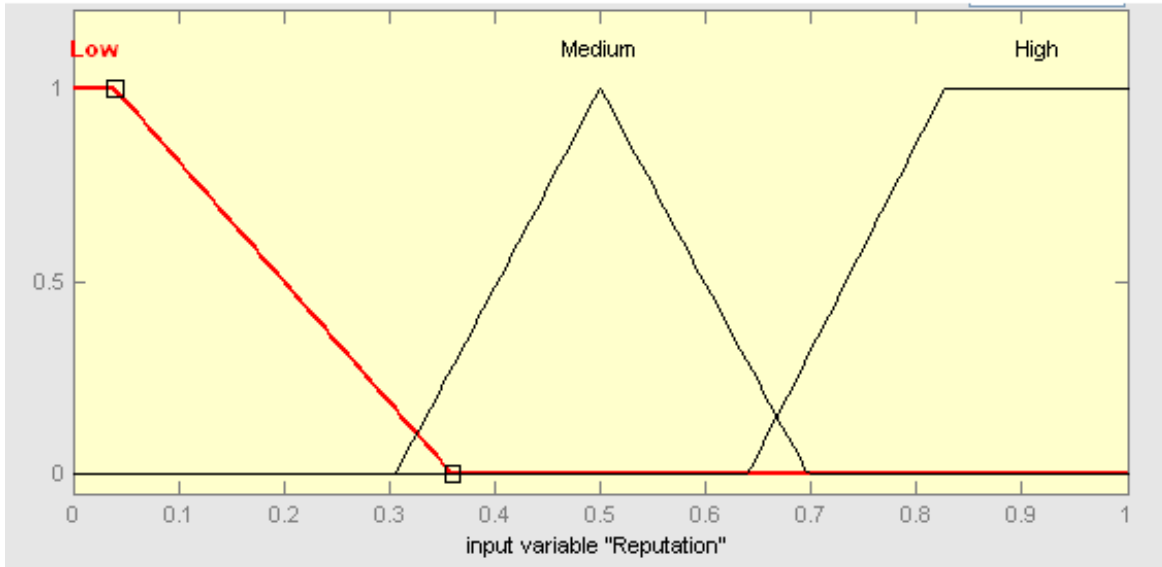


Figure 15: Fuzzy membership function for reputation as input parameter to FIS (2)

Figure 16 shows the fuzzy membership function for the counter of faked messages factor that ranges from zero to twenty five. Their assigned fuzzy values are grouped into two main values (Low and High). If the counter of faked messages is high, then its membership function (fuzzy value) is also high. For example, if this counter has a low value (e.g. 5), that means; the forwarder of the message forwarded just 5 faked messages, but maybe it is just in forwarding first mode. So this value will not give any indication about the existence of the attacker. So the fuzzy value for 5 is low.

On the other hand, if this value is high (e.g. 23), then its fuzzy value will also be high, and the forwarder of the message will be marked as suspicious node as it forwarded too many faked messages. But still this factor does not give an absolute indication about the attacker, so it was given a small weight in the final decision even if the fuzzy value of the counter is high.

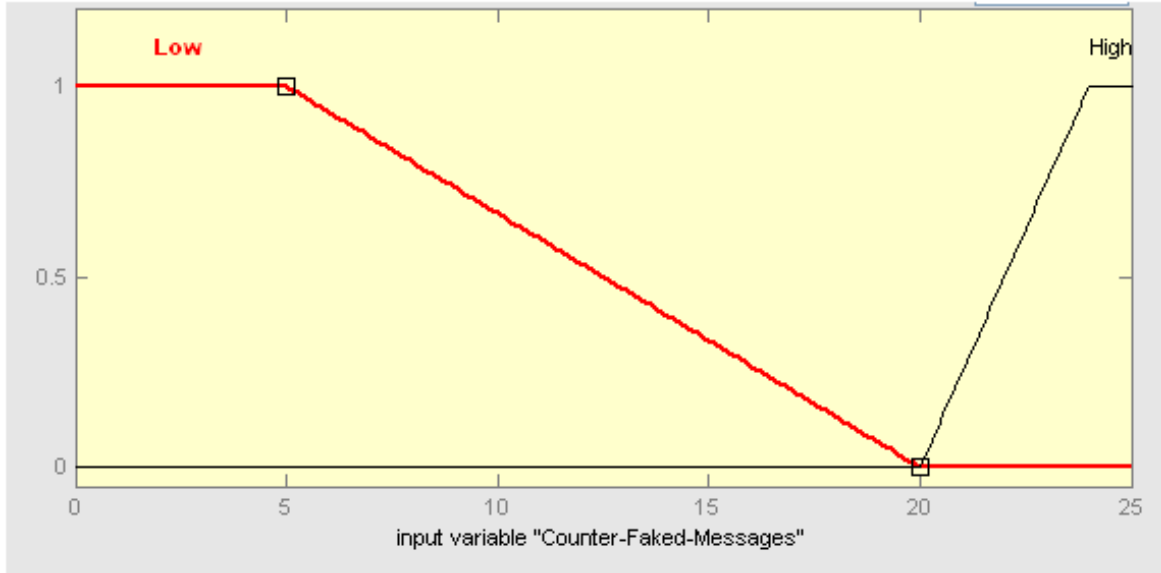


Figure 16: Fuzzy membership function for counter of faked messages factor

The reputation and the counter of faked messages values will be entered into FIS (2) by using IF-THEN rules. Then the output is calculated to give the final confidence value of the proposed FL-IDS. The confidence output parameter membership function is shown in Figure 17 that varies from 0 to 1. Their assigned fuzzy values are grouped into three main values (Low, Medium and High). The high confidence value will be assigned a high fuzzy value. For example, if the confidence value is low (e.g. 0.1), then the fuzzy value will also be low, as the possibility of attacking existence is very low. On the other hand, if the confidence value is high (e.g. 0.8), then the fuzzy value is also high, as this will give a high certainty about the existence of the attacking.

As shown in Table 6, if the reputation value is low and the counter of the faked messages is high, then the probability of attacking existence is low, because a heavy weight is given to the reputation value in the proposed FL-IDS. Therefore, even if counter of faked messages is high, still it does not guarantee the bad behavior. On the other hand, if

reputation value is high, regardless of the counter of faked messages value, then that will ensure the presence of an attacker.

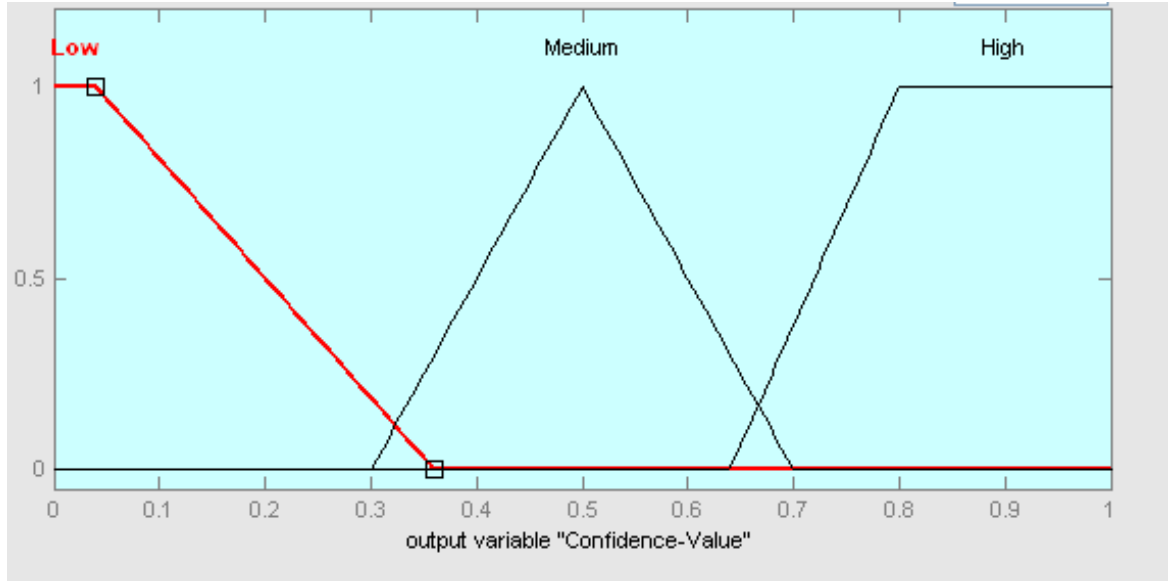


Figure 17: Fuzzy membership function for the confidence value output parameter

Table 6: Fuzzy IF-THEN rules for FIS (2)

		Counter-Faked-Messages	
		Low	High
Reputation	Low	Low	Low
	Medium	Medium	High
	High	High	High

After getting the confidence value, the monitor node will send this value to BS which in turns will take the final decision about the attacker as shown in Figure 18. In BS, there is a security threshold that depends on the sensitivity of the application for which the WSN is

applied. The BS will compare the confidence value against this security threshold. If the confidence value is greater than or equal to security threshold (confidence value \geq security threshold), then an alarm must be generated and sent to all monitor nodes in order to announce the existence of an attacker. Finally, this malicious node will be excluded from WSN.

This security threshold must be chosen carefully, and it is fully dependant on the type of the application. If the proposed system is deployed in sensitive applications (e.g. military environment) and cannot tolerate the existence of the attacker, the security threshold must be low (e.g. 0.3) in order to take an urgent decision about the attacker. On the other hand, if it is deployed in less sensitive applications (e.g. medical environment), then the required security threshold must be high (e.g. 0.7) that will give more delay in taking the final decision about the attacking process.

<p>Algorithm2: Decision Making System in BS upon Receiving the Confidence Value of Sensor Node(SN)</p>
<p>Input: Confidence(SN)</p> <p>1: Confidence(SN)</p> <p>2: if Confidence(SN) \geq security threshold</p> <p>3: SN is an attacker</p> <p>4: send an alarm message to announce the existence of the attacker to monitor nodes</p> <p>5: Exclude SN</p> <p>6: else</p> <p>7: SN is not attacker</p>

Figure 18: The proposed Decision Making System Performed by BS

4. IPDS System's Evaluation

This chapter starts with briefly discussing the simulation environment, and then it illustrates the evaluation metrics and the parameter values that are used in this research. Finally, it ends with evaluating the results of the proposed scheme.

4.1 Simulation Environment

Matlab (MATHWORK, 2007) is a high-level technical computing language that is generally easy to use. It represents an interactive environment that is used mainly for algorithm development, data visualization (Graphical User Interface), data analysis and numerical computing. The main advantage of using Matlab products is that any technical computing problem can be solved faster than when using any other traditional programming language such as C, C++ and Fortran.

In this research, using Matlab version 7.7.0, a new simulator for WSNs is developed from scratch. It is found to be accurate and easy to manipulate. Furthermore, in order to implement the Fuzzy Logic Inference Systems that is proposed in this research, the Matlab Fuzzy Logic Toolbox is used.

The schemes in this research were tested on a computer running Windows 7 Home Premium Operating System with Intel® Core™2 Duo processor T5550 @ 1.83GHz and 3 Gigabytes of RAM.

4.2 Evaluation Metrics

Despite the great technical advancement that network security had witnessed during the last few years, and in parallel with the increased deployment of WSN in variant sensitive

applications; DoS attacks can still form a great challenge. They can deplete the energy of sensor nodes by forcing them to perform unnecessary huge number of false verifications and huge number of forwarding and receiving the faked messages. They can also prevent authentic messages from being received by sensor nodes and thus delay the response from them back to the BS.

The adaptive window scheme that is used in the prevention part of the proposed IPDS can reduce the damage of DoS attacks on WSN to involve only a small portion of sensor nodes (only the ones around the attacker could be affected). On the other hand, the proposed scheme in the detection part (FL-IDS) can monitor, detect and finally exclude such attacks from the communication process. So, it does not only reduce their damage, but it does also stop such great damage that threatens WSN.

IPDS scheme can protect the WSN against DoS attacks by saving more energy and minimizing the average broadcast delay for the authentic messages. Thus, not only reducing the spread of faked messages in sensors network, but it also stops such spread by isolating the DoS attacks, thus forwarding as many authentic messages as possible before the verification process.

In this chapter, the performance of the proposed scheme (IPDS) in this research is studied, by comparing it with that of other prevention based techniques such as: adaptive window scheme and dynamic window scheme. These two schemes are the most up to date and related ones to the IPDS and they are considered among the best schemes that tried to prevent DoS against broadcast authentication in WSNs.

Two main metrics are used to evaluate the proposed IPDS in this research:

- **Amount of wasted energy consumed in the sensor network:** the wasted energy consumed in this simulation is evaluated by measuring the amount of energy (in Joules) that is consumed by the sensors to perform unnecessary receiving and forwarding of faked messages. Two major determinants are used to calculate the amount of wasted energy: number of nodes that received faked messages and number of nodes that forwarded such messages. The latter value will reflect good impression about IPDS, because it determines the effectiveness of any prevention or detection scheme in protecting WSN against DoS attacks.

In order to compute the energy consumption in Joule, first of all, we must compute the two important values: total number of received faked actions (RA) and total number of forwarded faked actions (FA). The energy model for sensor nodes used in this research is based on the first order radio model (Hinzelman, et al., 2000a), (Hinzelman, et al., 2000b) and (Kalpakis, et al., 2002). In this energy model, the sensor node consumes $\epsilon_{elec} = 50 \text{ nJ/bit}$ to run the transmitter or receiver circuitry. On the other hand, it consumes $\epsilon_{amp} = 100 \text{ pJ/bit/m}^2$ for the transmitter amplifier.

Thus, the energy consumed in receiving a k-bit data packet is given by the following equation:

$$R_x = \epsilon_{elec} * k \quad (3)$$

While the energy consumed in transmitting a data packet is given by:

$$T_x = \varepsilon_{elec} * k + \varepsilon_{amp} * k * d^2 \quad (4)$$

Where (d) is the distance between the sending and receiving nodes. According to the energy transmission formula (4), each forwarded faked action (FA) consumes energy with the value T_x . So, if we have (Y) forwarded faked actions, then the total amount of wasted energy on them (WE_{FA}) will be computed as the following equation:

$$WE_{FA} = T_x * Y \quad (5)$$

Then, the percentage of wasted energy in forwarded faked actions ($WE_{FA}\%$) can be computed according to the following equation:

$$WE_{FA}\% = \frac{WE_{FA}}{E} \quad (6)$$

Where (E) is the total energy of the whole sensors network and is represented by the summation of all nodes energy as following equation:

$$E = \sum_{i=1}^{i=n} e_i \quad (7)$$

Thus, if we have a sensors network with identical energies (all the nodes have the same energy), then the total network's energy will be computed as the following equation:

$$E = n * e_i \quad (8)$$

Where n is the number of sensor nodes and e_i is the amount of energy for each sensor node.

According to the receiving energy formula, as shown in equation (3), each received faked action (RA) consumes energy with the value R_x . So, if we have (Z) received faked actions, then the total amount of wasted energy (WE_{RA}) will be computed as the following equation:

$$WE_{RA} = R_x * Z \quad (9)$$

And the percentage of wasted energy in received faked actions ($WE(RA)\%$) will be computed as the following equation:

$$WE(RA)\% = \frac{WE_{RA}}{E} \quad (10)$$

- **Average broadcast delay of authentic messages:** this metric is evaluated in this research in terms of the number of signature verifications performed on each message during its journey from BS until it reaches the sensor node multiplied by the time required for each verification operation. This metric reflects a real impression about the performance of the prevention and detection schemes. The BS commonly sends a request or command to a sensor node in order to get some data which must be sent back to the BS as soon as possible. In order to minimize the response time, the sensor node, in its turn, must accomplish this task as quickly as possible before any authentication process is being performed. But the risk that adversaries will keep forging a large number of faked messages that will

consequently enforce the sensor node to verify the authentication of messages before any forwarding process. This will prolong the response time and thus introduce an additional broadcast delay. Therefore, minimizing such main metric will have a significant impact on such limited network resources.

Thus, the average broadcast delay is computed by counting the number of signature verifications performed on each message before reaching the sensor node from the BS. This number is then multiplied by 2 (the assumed number of seconds needed for a single verification process) according to the following equation:

$$Delay = 2 * num\ of\ verifications \quad (11)$$

In this research, the simulation experiments show that there are other factors that might significantly affect the performance of the proposed scheme. Some of these factors are the density of the sensors network (degree of connectivity), the window size in each sensor node, the (α) parameter value which determines the ratio taken from the new update in the window size and finally the intensity of the DoS attacks.

4.3 Parameter Values

In the proposed simulation, a network of 500 sensor nodes is generated. These nodes are randomly deployed in a way to form a sparse network (implemented as a sparse graph). This network structure is selected to be more suitable environment to study the problems we are trying to solve (broadcast delay and energy consumption) as they are more visible there. In dense networks, each node is connected to a large number of nodes via single hop; thus, messages can be exchanged using short paths with very few hops. In order to generate such a sparse network in this implementation, the maximum set of neighbors of

each node is limited to a specific number that is determined according to the total size of the network.

In order to implement the IPDS, additional external static monitor nodes are deployed randomly in the sparse network, this deployment is applied in a dynamic way. That means the number of deployed monitor nodes is not fixed and can be changed according to their efficiency in monitoring the sets of their neighbors. In the proposed simulation, 10% of the network size determined the number of monitor nodes (there will be 50 monitor nodes and each one is in charge of monitoring 10 sensor nodes that lie in its transmission range). These monitor nodes are assumed to have higher capabilities than the ordinary sensor nodes but not as powerful as BS. So, if more efficient monitor nodes are used, then their number can be reduced to be less than 10% of the network size as each monitor node will be able to monitor more sensor nodes in its range. On the other hand, if they have a lower efficiency in monitoring sensor nodes, then their number need to be increased to be greater than 10% of the network size.

As been said, these monitor nodes are exploited as additional external nodes to the total size of the network; they are not part of the original size of the network. This means, if the 10% percentage is deployed for monitors in this research, then the total number of nodes will be 550 (500 sensor and 50 monitor nodes). These external nodes are deployed just for monitoring purposes, they are not responsible for forwarding messages, and thus they are not participating in the communication process. The reason why these nodes are exploited as additional ones (externals) is to mimic the same network structure and satisfy the conditions when we compare IPDS with the adaptive window scheme and dynamic window scheme.

Since the Mixed-Authentic message attacking model is the most realistic one in most applications, it is used in this research to simulate the attacking model (Wang, et al., 2007). Mixed-Authentic message attacking model is generated, in this simulation, by using a random function that produces a random number of faked and authentic messages which have random distribution in each simulation run.

The maximum window size on each sensor node and on each monitor node for all of its neighbors must be determined with respect to the size of the network. It can be computed according to the following equation:

$$max_win = round(0.0128 * N) \quad (12)$$

Where N is the total number of sensor nodes in the network (which is 500 in this case). Therefore, the maximum window size in this simulation will be 6. The ratio (0.0128) is related to the network size and is determined by experiments. The initial window size on each sensor node is generated randomly according to the following equation:

$$W = randi(max_win) \quad (13)$$

Where $randi$ is a random function that generates a random value from the interval $(1 \leq W \leq max_win)$, and max_win is computed according to equation (12). The window size in this implementation is updated according to the following equations:

$$cw = \alpha cw + (1 - \alpha)AIMD_W$$

$$W = round(cw)$$

where, $1 \leq W \leq \max_win$, cw is the current window, $0 < \alpha < 1$, $AIMD_W$ is computed by AIMD approach, in which $W = \text{ceiling}(W/2)$ in case of faked message, and $W = W+1$ in case of authentic message.

After updating the window size, if the new updated value exceeds the maximum window size, then the previous value before this last update will be restored and no update will take place. Limiting the window size in this way prevents the scheme from turning into forwarding first mode in which no filtering is performed on messages, and consequently this prevents faked messages from being distributed all over the network. As can be seen, the window size on each node is a very important factor that determines the potential success or failure for any proposed scheme.

In this research experiments, it is assumed that every authentication verification process (signature verification) will take two seconds as many researches in the literature have assumed (Wang, et al., 2007). This value is needed in computing the average broadcasting delay later on.

In order to compute the amount of wasted energy consumed in WSN, it is assumed in this research that all sensor nodes are identical, have the same level of energy and each one of them has a base line energy level of (1) Joule. As the total number of nodes is equal to 500 sensor nodes, so the total energy that is available in the whole network (E) is 500 Joule according to equation (8). The message size is assumed to be 1000 bits and the distance between any two nodes is the same in the whole network and equal to (1) meter.

4.4 Results and Evaluation

As mentioned before, the attacking model used in this simulation is Mixed-Authentic message model in which the intensity of DoS attacks is computed as the following equation:

$$DoSAttackIntensity = \frac{numFakedMsgs}{numAuthMsgs} \quad (14)$$

The number of faked messages in the experiments varies from 33% to 94% of the total number of messages. Therefore, the corresponding number of authentic messages will vary between 67% and 6%, respectively. Accordingly, the ratio of DoS attacks intensity will range from 0.5 to 15, respectively, according to equation (14). In this simulation, the energy consumption and the average broadcast delay of authentic messages are studied by changing the intensity of DoS attacks in different multiple experiments. So, the proposed scheme in this research is evaluated under various DoS intensity values.

4.4.1 Energy Consumption of Faked Messages under Various DoS Attacks Intensities

In order to evaluate the wasted energy consumed in this research, the percentages of wasted energy in receiving faked messages ($WE_{RA}\%$) and that in forwarding faked messages ($WE_{FA}\%$) are computed. Combined together, these two percentages give the amount of wasted energy in the whole network that is consumed in performing unnecessary operations by such resource constraint devices.

The performance of the proposed scheme in this research (IPDS) is evaluated by comparing its amount of wasted energy with that of other schemes proposed in the literature such as adaptive window scheme and dynamic window scheme. As will be

discussed later, the proposed IPDS in this research is found to outperform the other two schemes. It is found from the simulation experiments that the wasted energy consumed in receiving faked messages and forwarding them is reduced by up to 90% and 73%, respectively, when compared to adaptive window scheme. On the other hand, the wasted energy consumed due to receiving faked messages is found to be minimized by up to 98% and that on forwarding by up to 98% when compared to dynamic window scheme.

The percentage of wasted energy in receiving faked messages indicates how much faked messages are spread through network and the degree of communication overhead, and other losses in network resources caused by forged messages. On the other hand, the percentage of wasted energy in forwarding faked messages indicates the ability of any scheme to limit the effect of faked messages, and prevent them from spreading over the network.

Figure 19 shows the percentages of energy wasted in receiving and forwarding faked messages produced by IPDS under various DoS attacks intensities. These percentages do not commensurate with the attacking intensities in WSN. This figure also shows that IPDS has a good ability to minimize the number of forwarded faked actions in the networks compared with the number of received ones.

As shown in Figure 19, the behavior of this scheme is oscillating in energy consumption, which means; it is not steadily increased or decreased with increasing or decreasing the attacking intensities. To explain this, the energy consumption in the proposed IPDS, rather than to be dependent on the attacking intensities, is found to depend on the time when such attacking could be detected by the network. This means, the earlier the attacker is detected,

the fewer faked messages will spread across the network. As a result, fewer received and forwarded faked actions are recorded. According to this, the total energy that is wasted in faked actions is reduced. Therefore, the only factor that determines the amount of wasted energy is the number of faked messages that is distributed throughout the network before the intrusion detection. For example, if the IPDS detected the attacker after the fifth message, then the wasted energy due to the faked actions will be greater than if IPDS detecting the attacker after the second one, because the number of received and forwarded faked actions will be less in the latter.

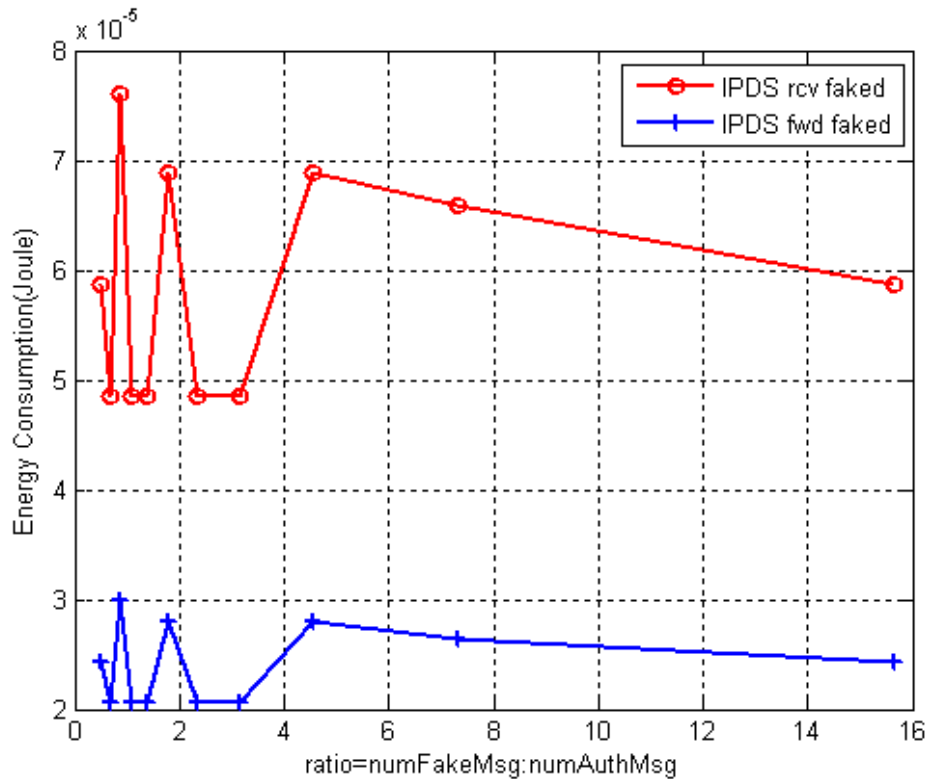


Figure 19: Energy Consumption: The percentages of wasted energy in receiving and forwarding faked messages under various DoS attacks intensities in IPDS

Figure 20 and Figure 21 show the percentages of wasted energy in receiving and forwarding faked messages respectively that is consumed by IPDS, adaptive window scheme and dynamic window scheme under various DoS attacks intensities. If the three schemes are compared on the same ratio of intensities, then it is clear from these figures that the IPDS consumes much less amount of wasted energy in performing faked actions than the other schemes. This is expected from the IPDS, because at the beginning of the network life time, the proposed scheme will depend only on the prevention part (adaptive window scheme) in reducing received and forwarded faked actions. But later on, when enough information is available about the attacker, the IPDS will detect and exclude the attacker, and this will totally stop receiving faked messages from the malicious node. In contrast to other schemes, the IPDS not only reduces the number of received and forwarded faked actions, but it also totally stops such actions by isolating the attacker.

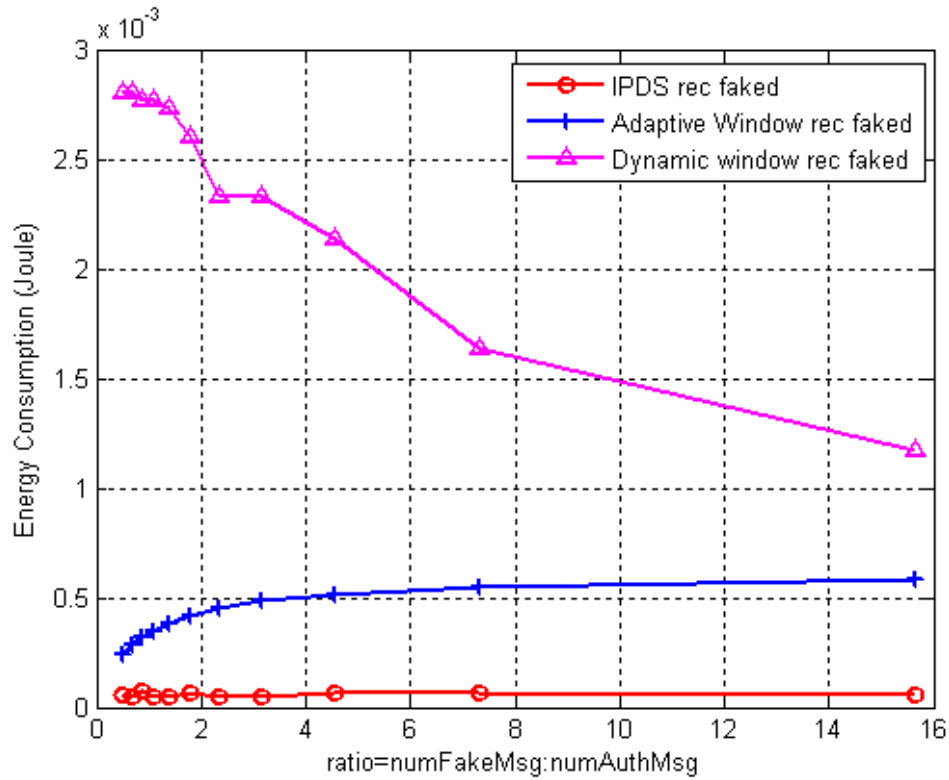


Figure 20: Energy Consumption: The percentage of wasted energy in receiving faked messages under various DoS attacks intensities in IPDS, adaptive window and dynamic window schemes

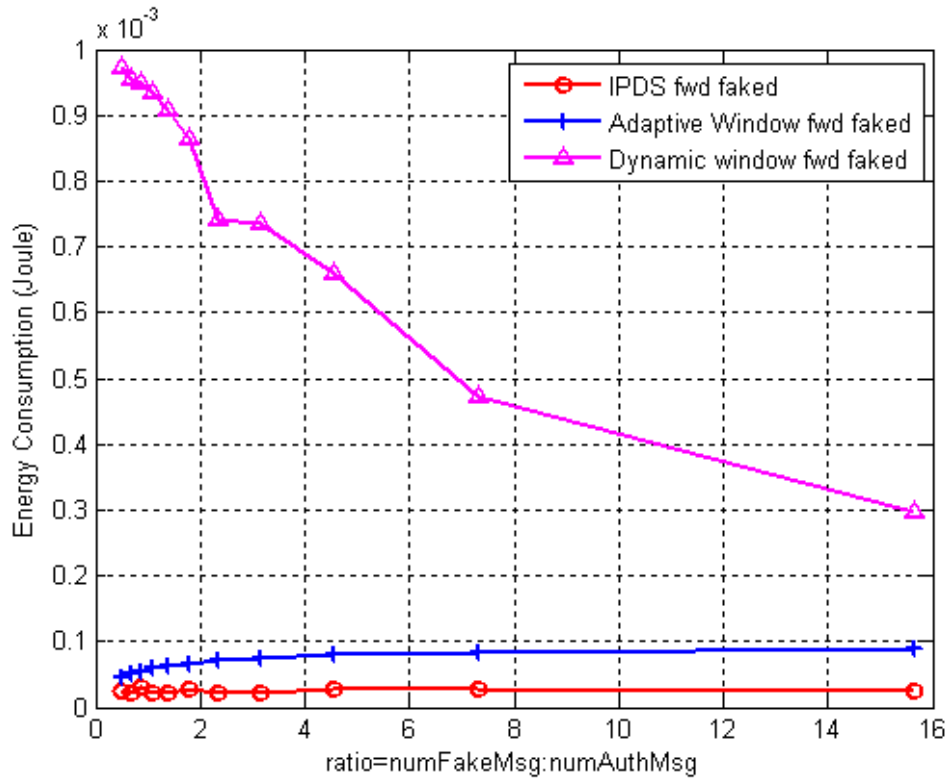


Figure 21: Energy Consumption: The percentage of wasted energy in forwarding faked messages under various DoS attacks intensities in IPDS, adaptive window and dynamic window schemes

When we compare the behavior of the IPDS with the adaptive and dynamic window schemes, as clear in Figure 20 and Figure 21, on the same ratio of attacking intensities, it can be seen that the percentages of wasted energy consumed by the IPDS in receiving and forwarding faked messages are very small compared to that of the other schemes. Such behavior of the dynamic window scheme is because this scheme depends purely on the window size stored locally in sensor nodes in reducing the effect of the DoS attacks. The attacker can intentionally send huge number of authentic messages. Accordingly, the window sizes will be rapidly increased according to $(W=W+I)$. This will enforce the sensor nodes to enter the forwarding first mode. Suddenly, the attacker sends huge number

of faked messages that spread throughout the entire network. Thus, the number of received and forwarded faked actions will be increased, which in turns will increase the percentages of wasted energy on such actions.

As shown in Figure 20 and Figure 21, dynamic window scheme is found not efficient in reducing the effect of DoS attacks; it works well only when the attacking intensity is high. Any weak attacker with only few faked messages can damage the entire network. Thus, the scheme is unable to protect the network resources from such threat despite its weakness, because the amount of wasted energy in receiving and forwarding these few faked messages is very high. The decreasing behavior of such scheme with increasing the attacking intensities can be explained as the following: with receiving few faked messages, the window sizes will be slightly decreased but not to a limit that will enforce the sensor nodes to enter the authentication first mode immediately, rather than that, they will continue in the forwarding first mode. So, the faked messages will take this opportunity to spread across the network. But when the attacking intensity is high with huge number of faked messages, the decrease in window sizes will occur more rapidly, which will enforce the sensors to enter the authentication first mode faster and thus decrease the chance of spreading of received and forwarded faked actions in the network.

Moreover, as shown in Figure 20 and Figure 21, it is clear that the adaptive window scheme consumes much less amount of energy in receiving and forwarding faked actions than the dynamic window scheme. But when compared with IPDS, this scheme is still found to consume a significant amount of energy. When the sensor nodes in the adaptive window scheme receive the intentional huge number of authentic messages, the window sizes stored locally in these nodes will be increased in a slower fashion compared to

dynamic window scheme and according to equation (1). This occurs as only a percentage of the newly updated window sizes is taken, so it will take longer time to enter the forwarding first mode. Then, if the network, at this time, is subjected to high intensity of attacking, then the number of received and forwarded faked actions will be less than those in dynamic window scheme. But still such attacking can consume a non-negligible amount of energy compared to IPDS. So, in this scheme the effect of DoS attacks is reduced compared to dynamic window scheme, but it cannot get rid of such attacks on WSN. The attacker will continue to threaten the network during the rest of its life time.

Figure 22 and Figure 23 show the effect of changing α value that is assigned for faked messages on the wasted energy consumed by IPDS and adaptive window schemes under various DoS attacks intensities. The α value is a parameter value which determines the ratio taken from the new update in the window size and it may range from zero to one. As can be seen, varying α value has a small effect on the IPDS performance, whereas it is seen to have a significant impact on the adaptive window scheme. This is expected from IPDS, because it consists mainly of two parts, the prevention part that depends only on the adaptive window scheme and the detection part (FL-IDS) that monitors and excludes the attackers. On the contrary, the adaptive window scheme depends purely on windows stored locally inside the sensor nodes; specifically it depends on α value which determines the percentage that must be taken from the newly updated window size (AIMD_W) in order to compute the current window. Thus, α value is a major determinant of the performance of this scheme.

To interpret the effect of changing the α value on these two schemes, this effect on each scheme will be discussed independently.

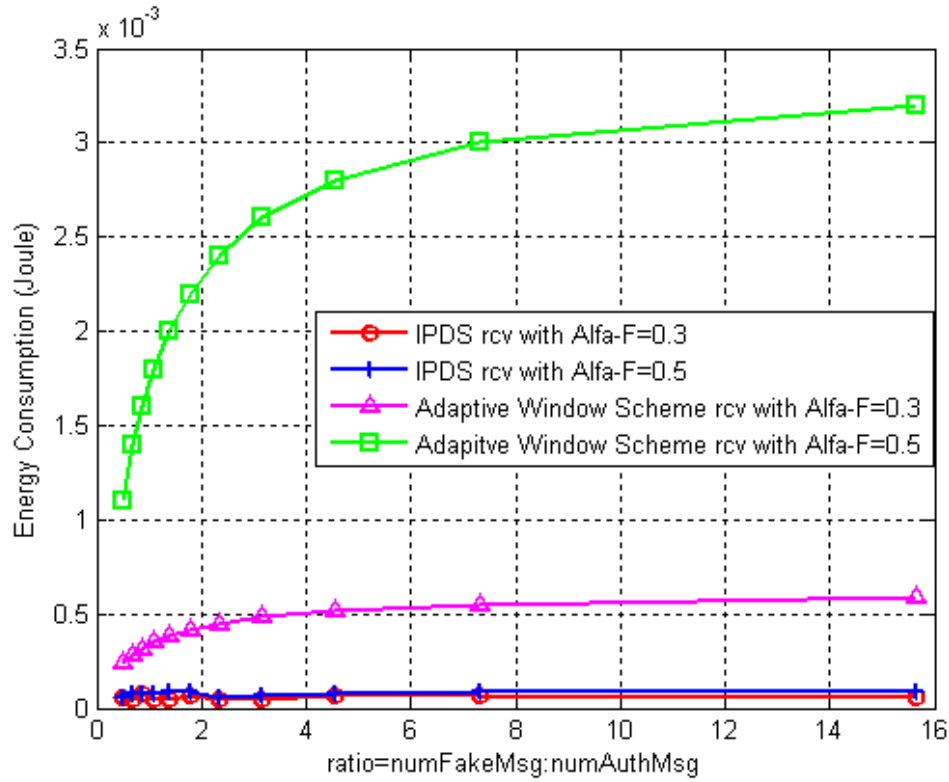


Figure 22: Energy Consumption: The percentage of wasted energy due to receiving faked messages under various DoS attacks intensities for both IPDS and adaptive window schemes with different α values

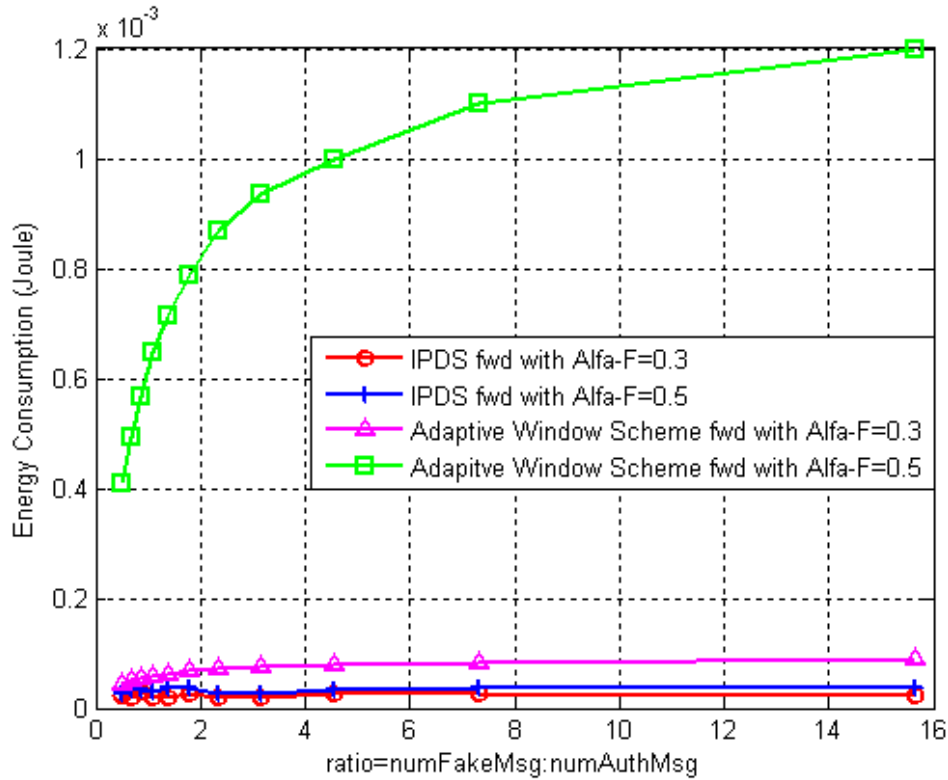


Figure 23: Energy Consumption: The percentage of wasted energy due to forwarding faked messages under various DoS attacks intensities for both IPDS and adaptive window schemes with different α values

Figure 24 and Figure 25 show the effect of changing α value on the performance of the adaptive window scheme regarding the wasted energy. Two α values (0.3 and 0.5) were chosen in order to study this effect. As indicated by equation (1), when $\alpha=0.3$ is used for faked messages, then the value $(1.0 - 0.3 = 0.7)$ will be taken from the newly updated window (AIMD_W) in order to compute the current window. Consequently, the window size will be decreased rapidly but not like in the dynamic window scheme.

For example, when the attacker sends huge number of faked messages, the windows that are stored locally inside the sensor nodes will be decreased a quite rapidly when using this α value, in order to switch most of the sensor nodes to the authentication first mode, and

thus reduce number of received and forwarded faked messages and reducing the amount of the energy that is wasted in faked actions. On the other hand, when using $\alpha=0.5$, the corresponding percentage that must be taken from the newly updated window will be $(1.0 - 0.5 = 0.5)$. This will cause a slower decrease in window sizes than using $\alpha=0.3$, and thus increase number of faked messages that are forwarded before any verification process. Therefore, and as much more energy is wasted in receiving and forwarding actions when higher α value is used in this scheme, α value must be chosen carefully in order to minimize the wasted energy as possible as can be.

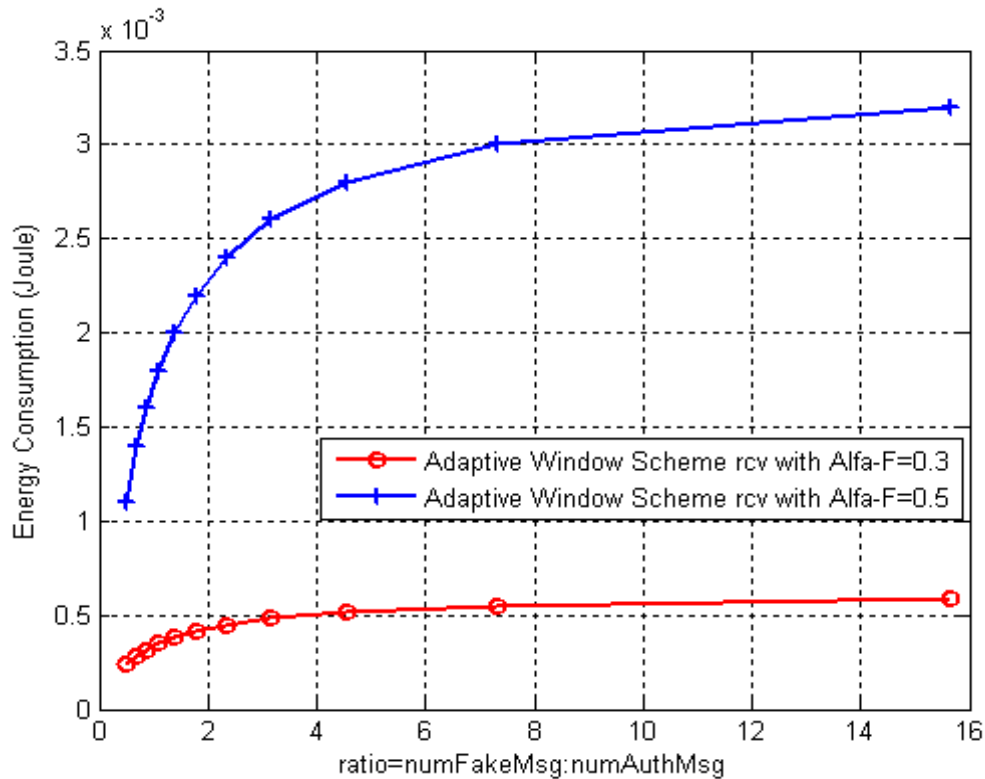


Figure 24: Energy Consumption: The percentage of wasted energy due to receiving faked messages under various DoS attacks intensities for adaptive window scheme with different α values ($\alpha=0.3$ and $\alpha=0.5$)

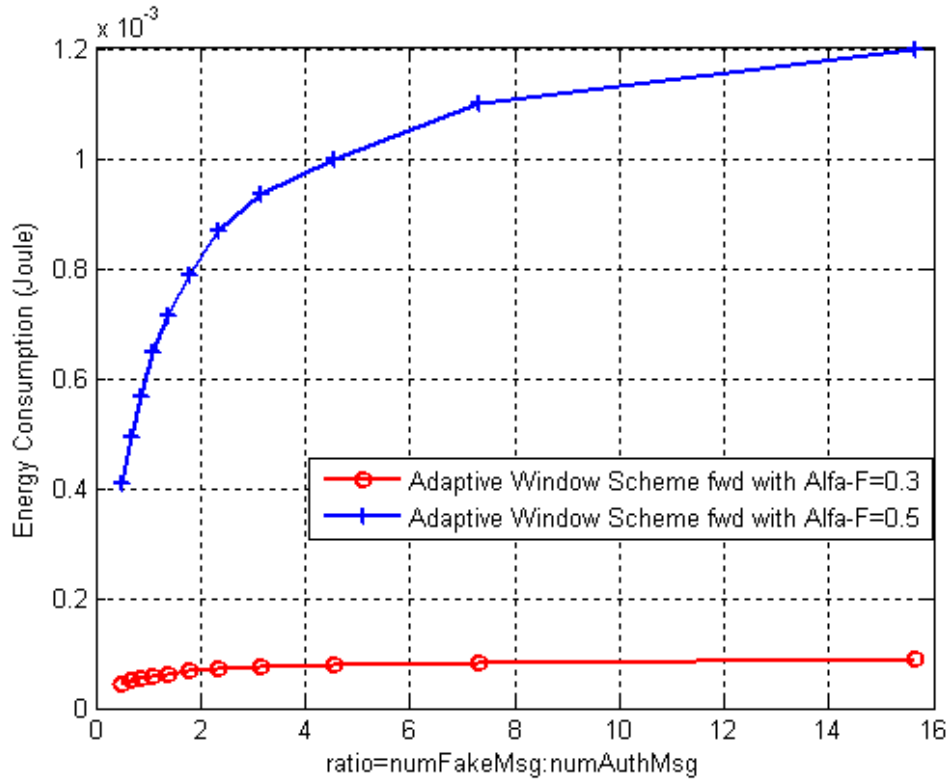


Figure 25: Energy Consumption: The percentage of wasted energy due to forwarding faked messages under various DoS attacks intensities for adaptive window scheme with different α values ($\alpha=0.3$ and $\alpha=0.5$)

Figure 26 and Figure 27 show the impact of using different α values for faked messages on the percentages of wasted energy that is consumed by IPDS. For fair comparison, this scheme is studied under the same α values used with the adaptive window scheme ($\alpha=0.3$ and $\alpha=0.5$).

As shown in these figures, varying α value has a small impact on the percentages of the wasted energy in receiving and forwarding faked messages for this scheme. Compared to adaptive window scheme with ($\alpha=0.3$) for faked messages, current window will take the same percentage (0.7) as the case was in the adaptive window scheme. On the other hand, when using ($\alpha=0.5$), windows stored locally inside the sensor nodes will be decreased

more slowly than when using ($\alpha=0.3$), this was the case in the adaptive window scheme. But it is different with IPDS; this percentage (0.5) will temporarily affect the window sizes and that occurs just at the early stages before the intrusion detection. Then, after the intrusion is been detected and isolated, the faked messages will no more affect the window sizes. This means, this α value will not affect the window sizes after the intrusion detection. This is why α value has a small effect on this scheme.

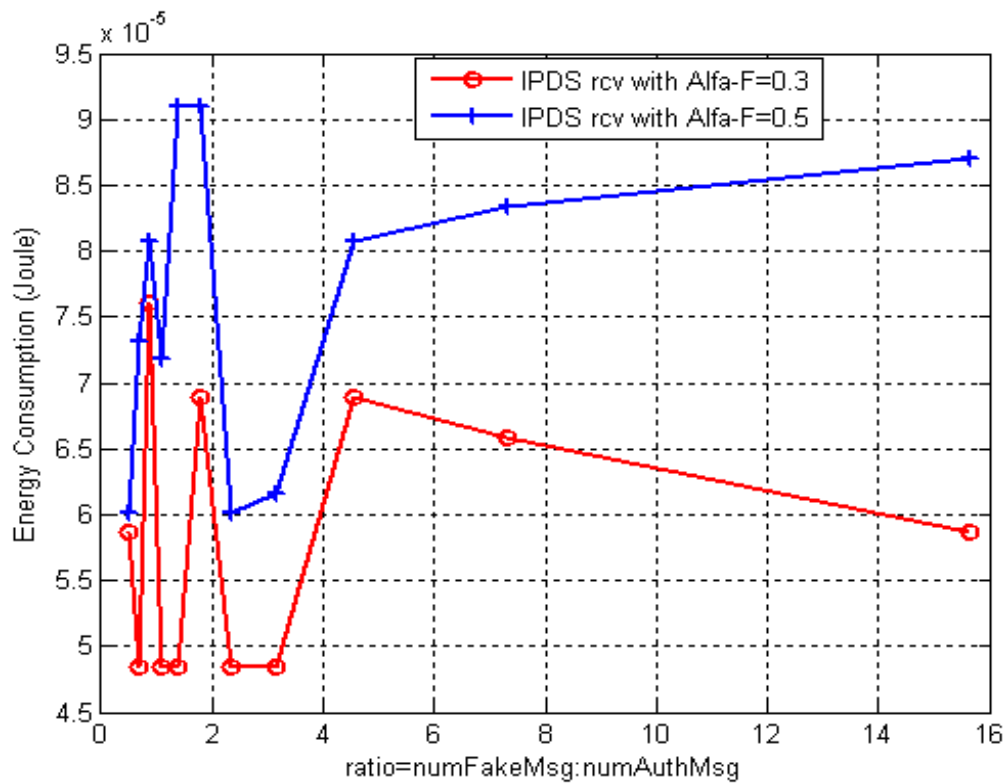


Figure 26: Energy Consumption: The percentage of wasted energy due to receiving faked messages under various DoS attacks intensities for IPDS scheme with different α values ($\alpha=0.3$ and $\alpha=0.5$)

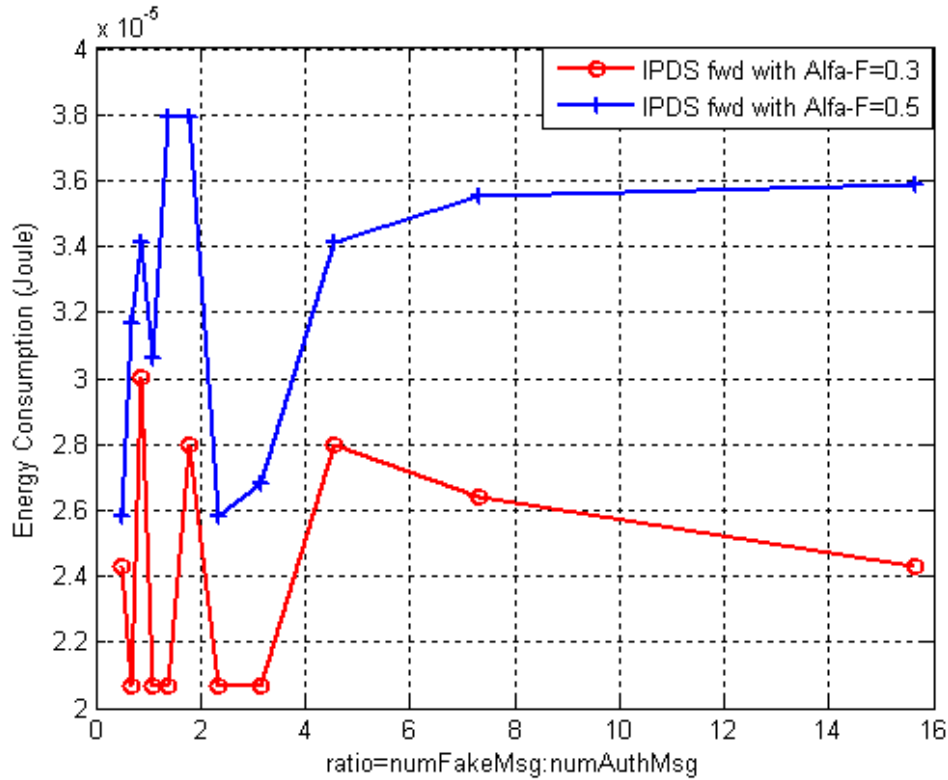


Figure 27: Energy Consumption: The percentage of wasted energy due to forwarding faked messages under various DoS attacks intensities for IPDS scheme with different α values ($\alpha=0.3$ and $\alpha=0.5$)

4.4.2 Average Broadcast Delay for Authentic Messages under Various DoS Attacks Intensities

In order to evaluate the proposed IPDS, the average broadcast delay on authentic messages produced by IPDS is compared with that of the adaptive window scheme, dynamic window scheme and authentication first scheme. As will be discussed later, the proposed (IPDS) in this research is found to outperform the other three schemes by reducing average broadcast delay on authentic messages by up to 55% compared to adaptive window scheme, up to 65% compared to dynamic window scheme and up to 90% compared to authentication first scheme.

Figure 28 shows the average broadcast delay of authentic messages produced by IPDS, adaptive window, dynamic window and authentication first schemes under various DoS attacks intensities. If the four schemes are compared on the same ratio of intensities, then it is clear that IPDS produces much less broadcast delay than the other schemes. This expected behavior of IPDS can be justified as the following: when the DoS attacks intensity is high, and as the sensor nodes receive some of these faked messages at the beginning, their response will be to decrease their window sizes according to equation (1). In the meanwhile, the IPDS will monitor the behavior of the malicious node and according to the available information about the abnormal node, it will exclude the attacker. This means, the WSN will no more receive any faked message from the malicious node and only authentic messages will pass through the sensor nodes. Accordingly, the window sizes stored locally in each sensor node will grow (because of receiving authentic messages only) until reach the maximum window size. As a result of these large windows, the sensor nodes will do more forwarding before any verification process, and continue in this process until the detection of another bad behavior. Therefore, number of signature verification before the forwarding process will be minimized.

In IPDS, faked messages affect the WSN just at the early stages of the communication process. At that stage, there is no enough information available about the suspicious node to totally exclude it from the network. Once they are available, faked messages will not affect the WSN anymore.

When the behavior of the IPDS is compared with the authentication first scheme, as clear in Figure 28, the broadcast delay introduced by IPDS is relatively very small with respect to that introduced by authentication first scheme. This is because the authentication first

scheme, regardless of the authenticity of the message, always performs the signature verification before forwarding the message, and forwards it only when it is valid. That is why it introduces much more broadcast delay than any other schemes that alternates between the two modes (authentication first and forwarding first modes).

Although the dynamic window scheme introduces less amount of broadcast delay compared to the authentication first scheme, it still introduces much more broadcast delay on the authentic messages than IPDS as shown in Figure 28. When the DoS attacks intensity is high, the window size on each sensor node in the dynamic window scheme will be decreased strictly according to $W = \left\lfloor \frac{W}{2} \right\rfloor$. That results in increasing the number of messages that will be verified before being forwarded, and decreasing the number of messages that will be forwarded before being verified. Consequently, much more delay is introduced using this scheme. So, in this scheme, in contrast to IPDS, the attacker will affect the WSN during life time of the network. Even more, the attacker can purposely send too many authentic messages to allow the windows to grow locally and suddenly at that moment it will send huge number of faked messages causing the windows to dramatically decrease. This will enforce most of the sensor nodes to enter the authentication first mode leading to more broadcast delay. Although the sensor nodes in this scheme alternate between authentication first and forwarding first modes, as a whole this scheme fails to totally prevent the attackers from sending faked messages and affecting the network, it just reduces such effect.

As noticed in Figure 28, the adaptive window scheme introduces much less amount of broadcast delay than authentication first and dynamic window schemes, but when

compared with the IPDS, it still introduces a significant amount of broadcast delay on the authentic messages. In the adaptive window scheme, when the DoS intensity is high, the window size is decreased according to equation (1); thus, only a percentage of the newly updated window (AIMD_W) will be taken when the current window is computed. This scheme results in decreased number of verifications on the authentic messages in spite of the existence of high attacking intensity when compared to the authentication first mode and dynamic window scheme. Despite that, the attacker will still exist and can affect WSN during the rest of its life time. So, by using this scheme we cannot get rid of the attacker, rather we can just reduce the effect of it to involve only a small portion of the network.

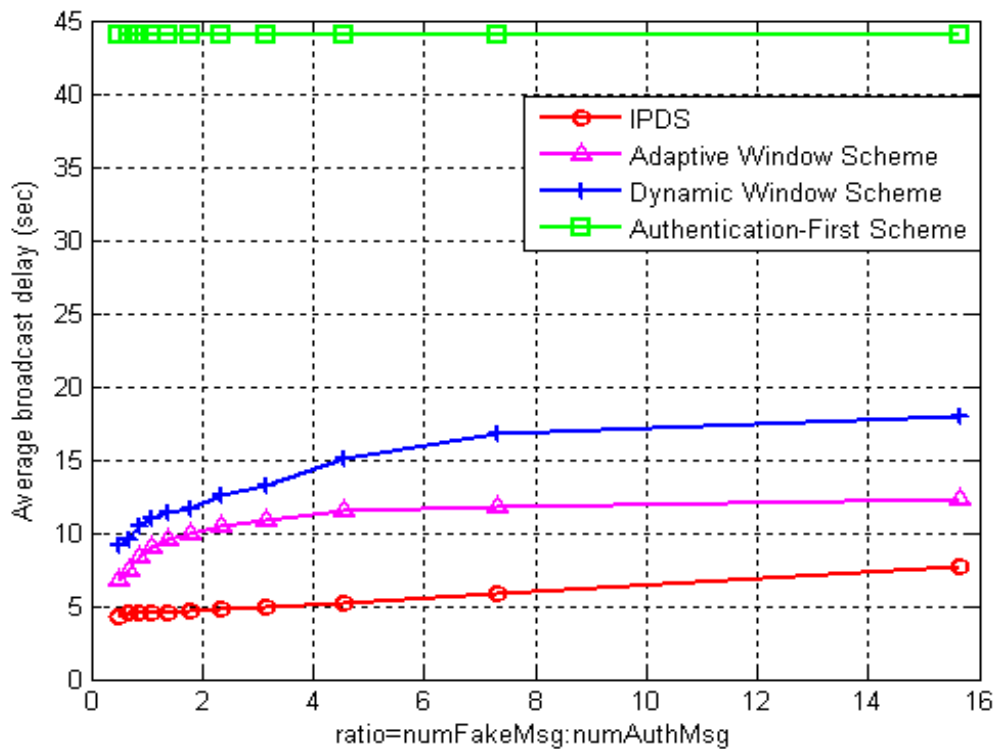


Figure 28: Average broadcast delay for authentic messages under various attacks intensities for IPDS, adaptive window, dynamic window and authentication first schemes (with $\alpha=0.5$ for authentic messages and $\alpha=0.6$ for faked messages)

Figure 29 shows the average broadcast delay of authentic messages that is introduced by the adaptive window and IPDS schemes under various DoS attacks intensities using different α values that are assigned for faked messages. As can be seen, changing α value has a small impact on the IPDS performance. On the other hand, such change in α value is found to have a significant impact on the adaptive window scheme. This is expected, because the IPDS, as has been illustrated before, involves a prevention part that depends mainly on adaptive window scheme and detection part (FL-IDS) that monitors and excludes the attacker. Comparatively, the adaptive window scheme depends mainly on the window size stored locally on each sensor node; specifically it depends on α value which determines the percentage that must be taken from the newly updated window size (AIMD_W) in order to compute the current window. Thus, changing α value will have a significant impact on the performance of this scheme.

To justify the effect of changing the α value on these two schemes, the effect of that on each scheme will be discussed independently.

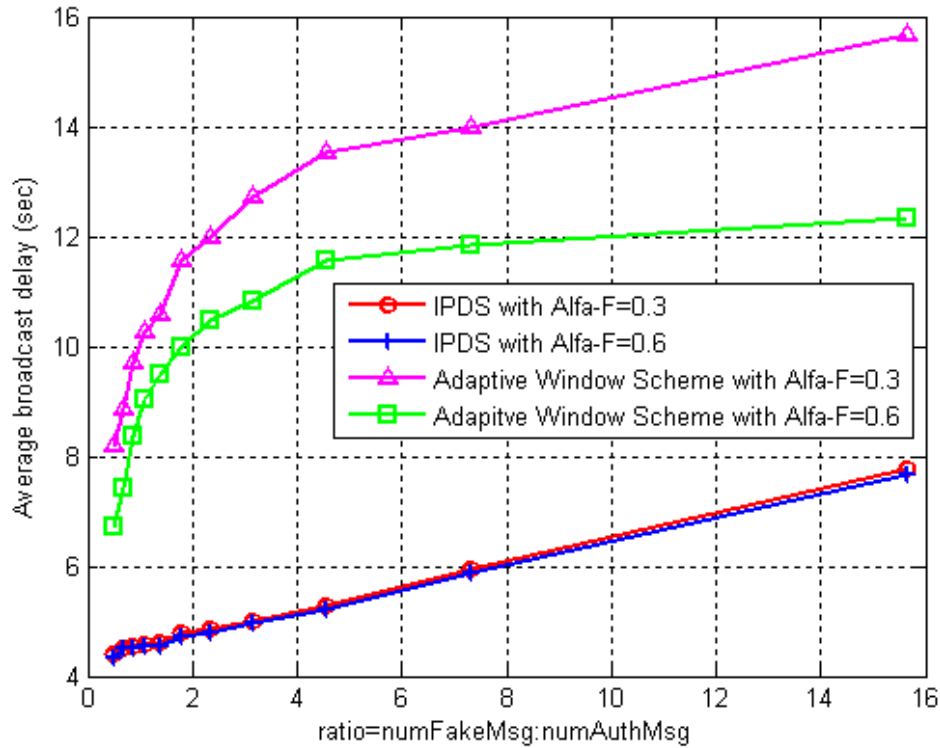


Figure 29: Average broadcast delay for authentic messages under various attacks intensities for both IPDS and adaptive window schemes with different α values

Figure 30 shows the difference between broadcast delay values for authentic messages introduced by adaptive window scheme by using different α values. Two α values (0.3 and 0.6) were chosen in order to study this effect. As indicated by equation (1), when $\alpha=0.6$ is used for faked messages, then the value $(1.0-0.6=0.4)$ will be taken from the newly updated window (AIMD_W) in order to compute the current window, so the window will be decreased slowly. On the other hand, when using $\alpha=0.3$, the percentage that must be taken from the newly updated window will be $(1.0-0.3=0.7)$, which causes a faster decrease in window sizes, and thus increase the number of messages that must be verified before being forwarded. Therefore, much more broadcast delay will result when lower α

value is used. As α value decreases, it can be noticed that the behavior of the adaptive window scheme can reach that of the dynamic window scheme.

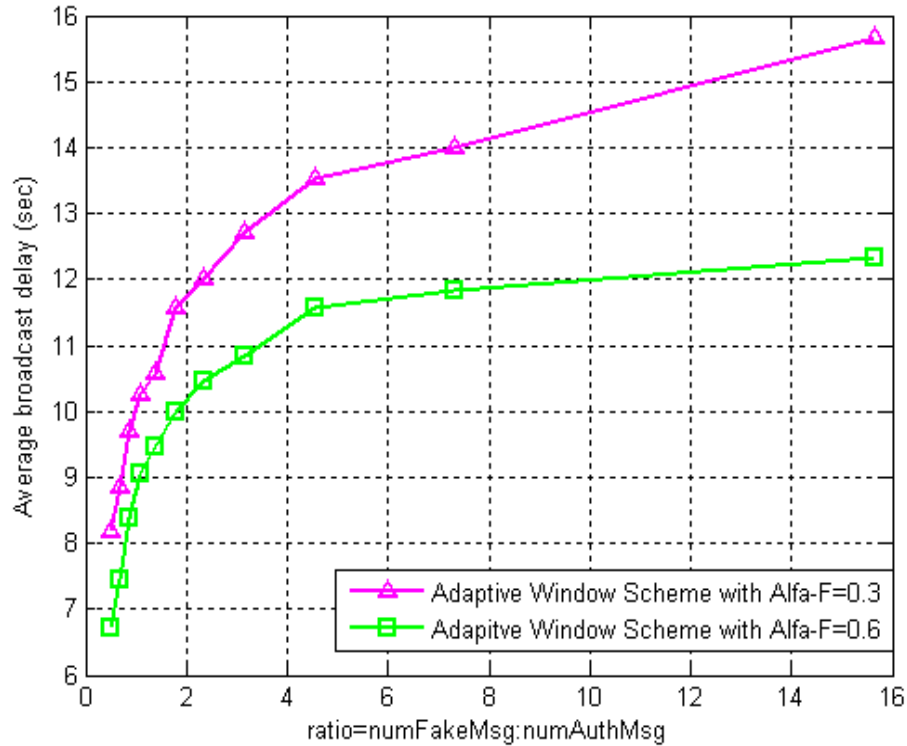


Figure 30: Average broadcast delay for authentic messages under various attacks intensities for adaptive window scheme with different α values ($\alpha=0.3$ and $\alpha=0.6$)

Figure 31 shows the impact of using different α values for faked messages on the average broadcast delay of authentic messages when using IPDS. For fair comparison, this scheme is studied under the same α values used with the adaptive window scheme ($\alpha=0.3$ and $\alpha=0.6$). As can be seen, changing α value has a negligible impact on the average broadcast delay for this scheme. With ($\alpha=0.6$) for faked messages, the current window will take the same percentage (0.4) as the case was in the adaptive window scheme. On the other hand, when using ($\alpha=0.3$), the windows that stored locally in the sensor nodes are supposed to be

decreased strictly accordingly to (0.7) as the case was in the adaptive window scheme, but the case is different with IPDS. This percentage (0.7) will temporarily affect the window sizes and that occurs just at the early stages before detecting the attacker. Then after intrusion is been detected and isolated, the faked messages will no more affect the window sizes, and window sizes will start to grow inside the sensor nodes. This means, this α value will not affect the window size after intrusion detection. That is why, in IPDS, the difference in delay values on the same DoS attacks intensity by using different α values is very small.

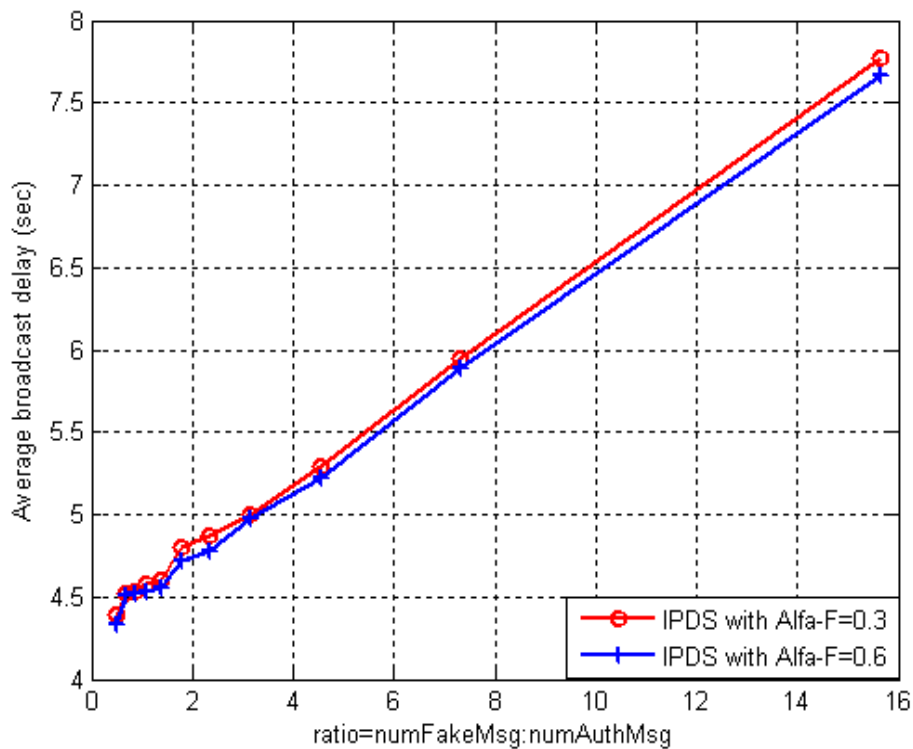


Figure 31: Average broadcast delay for authentic messages under various attacks intensities for IPDS with different α values ($\alpha=0.3$ and $\alpha=0.6$)

5. Conclusions and Future Works

Broadcast authentication is a critical process, specifically in the WSNs, that must be accomplished in order to guarantee that the intended application will function properly without intervention from an adversary or any possible attack. The main broadcast authentication approaches; digital signature and TESLA, are vulnerable to different types of attacks including the DoS attacks. In order to protect such authentication approaches, many schemes are proposed in the literature to contain the DoS attacks to involve only a small portion of the network or to prevent them from launching. Despite that, DoS attacks continue to form a great challenge. This research presented IPDS scheme that can prevent, detect and finally exclude DoS attacks from launching against broadcast authentication in WSNs.

IPDS consists of two main parts; prevention and detection. The prevention part is based on the adaptive window scheme that tried to reduce the effect of DoS attacks to involve only a small portion of the network, and it is installed in each sensor node. On the other hand, in the detection part FL-IDS was proposed in order to detect and exclude the attacker from the communication process. This scheme depends on the availability of the information produced by the prevention part. It utilizes the FIS in order to make the final decision about the malicious node. By exploiting the fuzzy logic, the proposed system achieves a high detection rate by considering factors such as: the total number of received faked message, accumulative counter of the difference between EW and RH, and the mismatching value in the estimated window size and the received window size. The introduced detection part uses specification-based detection policy that depends on

defining set of rules for the attackers, and checking the behavior of nodes against these rules in order to detect the abnormal behavior.

The performance evaluation in this research showed that the proposed IPDS outperforms the performance of other schemes by reducing average broadcast delay of authentic messages by up to 55% compared to adaptive window scheme, up to 65% compared to dynamic window scheme and up to 90% compared to authentication first scheme. The IPDS is also found to minimize the wasted energy consumed in receiving faked messages by up to 90% and that on forwarding them by up to 73% when compared to adaptive window scheme. On the other hand, the wasted energy consumed in receiving faked messages is found to be minimized by up to 98% and that on forwarding them by up to 98% when compared to dynamic window scheme.

The performance of the IPDS regarding the broadcast delay and energy consumption could allow preservation of the network's constraint-resources, and thus provide optimization of the security issue of WSNs.

As a future work, studying the impact of using different attacking models on the performance of the IPDS is suggested. Furthermore, in order to optimize the performance of the IPDS, genetic algorithm may be used to find the best combination for (α) values used for authentic messages and the values used for faked ones. Another suggestion is to integrate a dynamic monitoring system instead of static one to the IPDS in order to reduce the cost that is introduced by deploying the external monitor nodes.

References

Abduvaliyev Abror, Lee Sungyoung and Lee Young-Koo, (2010), Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks, **International Conference on Electronics and Information Engineering** (Kyoto), IEEE , vol. 2, pp. 25-29.

Akyidiz Ian F., Su Weilan, Sakarasubramaniam Yogest and Cayirci Erdal, (2002), A Survey on Sensor Networks. **IEEE Communications Magazine**, vol. 40, no. 8, pp. 102-115.

Al-Momani Iman, Karajeh Ola and Abdullah Lamya, (2010), Reducing the Vulnerability of Broadcast Authentication against DoS Attacks in Wireless Sensor Networks, **Mediterranean Journal of Computers and Networks**, Submitted.

Chi Sang Hoon and Cho Tae Ho, (2006), Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks, **Lecture Notes in Artificial Intelligence**, Springer, vol. 4223, pp. 725-734.

Dong Qi, Liu Donggang and Ning Peng, (2008), Pre-Authentication Filters: Providing DoS Resistance for Signature-Based Broadcast Authentication in Sensor Networks, **Proceedings of ACM Conference on Wireless Network Security**, pp. 2-12.

Du Xiaojiang, Guizani Mohsen, Xiao Yang and Chen Hsiao-Hwa, (2008), Defending DoS Attacks on Broadcast Authentication in Wireless Sensor Networks, **IEEE International Conference on Communications** (Beijing), pp. 1653-1657.

Farooqi Ashfaq Hussain and Khan Farrukh Aslam, (2009), Intrusion Detection Systems for Wireless Sensor Networks: A Survey, **Communications in Computer and Information Science**, Springer, vol. 56, pp. 234-241.

Gan Xian and Li Qiaoliang, (2009), A Multi-user DoS-containment Broadcast Scheme for Wireless Sensor Networks, **IEEE International Conference on Information Technology and Computer Science**, vol. 1, pp. 472-475.

Gura Nils, Patel Arun, Wander Arvinderpal, Eberle Hans and Shantz Sheueling Chang, (2004) , Comparing Elliptic Curve Cryptography and RSA on 8-bit CPU, **Proceeding of Cryptographic Hardware and Embedded Systems**, Springer, vol. 3156, pp. 925-943.

Hai Tran Hoang, Khan Faraz and Huh Eui-Nam, (2007), Hybrid Intrusion Detection System for Wireless Sensor Networks, **International Conference on Computational science and its Applications**, Springer, vol. 4706, pp. 383-396.

Heinzelman Wendi Rabiner, Sinha Amit, Wang Alice, and Chandrakasan Anantha P., (2000a), Energy Scalable Algorithms and Protocols for Wireless Microsensor networks, **Proceedings of the International Conference on Acoustics, Speech, and Signal Processing** (Istanbul , Turkey), IEEE, vol. 6, pp. 3722-3725.

Heinzelman Wendi Rabiner, Chandrakasan Anantha and Balakrishnan Hari, (2000b), Energy-Efficient Communication Protocol for Wireless Microsensor Networks, **Proceedings of the 33rd Hawaii International Conference on System Sciences**, IEEE, vol. 2, 10 pp.

Huang Ying, He Wenbo, Nahrstedt Klara and Lee Whany C., (2008), DoS-Resistant Broadcast Authentication Protocol with Low End-to-End Delay, **IEEE INFOCOM Workshops** (Phoenix, AZ), pp. 1-6.

Islam Md. Safiqul, Khan Razib Hayat and Bappy Dewan Muhammad, (2010), A Hierarchical Intrusion Detection System in Wireless Sensor Networks, **International Journal of Computer Science and Network Security**, vol. 10, no. 8, pp. 21-26.

Jian-hua Song and Chuan-Xiang Ma, (2008), Anomaly Detection Based on Data-Mining for Routing Attacks in Wireless Sensor Networks, **Second International Conference on Communications and Networking** in China, IEEE, pp. 296-300.

Kalpakis Konstantinos, Dasgupta Koustuv and Namjoshi Parag, 2002, Maximum Lifetime Data Gathering and Aggregation in Wireless Sensor Networks, **Proceedings of IEEE International Conference on Networking**, pp. 685-696.

Kesselman Alex and Mansour Yishay, (2003), Adaptive AIMD Congestion Control, **Proceedings of the Twenty-Second Annual Symposium on Principles of Distributed Computing** (Boston), ACM, pp. 352-359.

Luk Mark, Perrig Adrian and Whillock Bram, (2006), Seven Cardinal Properties of Sensor Network Broadcast Authentication, **Proceedings of the Fourth ACM Workshop on Security of Ad hoc and Sensor Networks** (New York, NY, USA), pp. 147-156.

Martynov Dmitriy, Roman Jason, Vaidya Samir and Fu Huirong, (2007), Design and Implementation of an Intrusion Detection System for Wireless Sensor Networks, **IEEE International Conference on Electro/Information Technology** (Chicago, IL), pp. 507-512.

MATHWORK, MATLAB, (2007), **Society for Industrial and Applied Mathematics**, Philadelphia, PA.

McNeill F.Martin and Thro Ellen, (1994), Fuzzy Logic A Practical Approach, **Academic Press, Inc.**

Moon Soo Young and Cho Tae Ho, (2009), Intrusion Detection Scheme against Sinkhole Attacks in Directed Diffusion Based Sensor Networks, **International Journal of Computer Science and Network Security**, vol. 9, no. 7, pp. 118-122.

Ning Peng, Liu An and Du Wenliang, (2008), Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks, **ACM Transactions on Sensor Networks**, vol. 4, no.1, pp. 1-35.

Onat Ilker and Miri Ali, (2005), An Intrusion Detection System for Wireless Sensor Networks, **Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications**, vol. 3, Montreal, Canada, pp. 253-259.

Perrig Adrian, Canetti Ran, Tygar J.D. and Song Dawn, 2002, The TESLA Broadcast Authentication Protocol, **RSA Cryptobytes**, 2-13.

Raymond David R. and Midkiff Scott F., (2008), Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, **IEEE Pervasive Computing**, vol. 7, no. 1, pp. 74-81.

Ren Kui, Yu Shucheng, Lou Wenjing and Zhang Yanchao, (2009), Multi-User Broadcast Authentication in Wireless Sensor Networks, **IEEE Transactions on Vehicular Technology**, vol. 58, no. 8, pp. 4554-4564.

Rivest R. L., Shamir A. and Adleman L., (1978), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, **Communications of the ACM**, vol. 21, no. 2, pp. 120-126.

Roman Rodrigo, Zhou Jianying and Lopez Javier, (2006), Applying Intrusion Detection Systems to Wireless Sensor Networks, **Third IEEE Consumer Communications and Networking Conference**, vol. 1, pp. 640-644.

Sabbah Eric and Kang Kyoung-Don, (2009), Security in Wireless Sensor Networks, **Computer Communications and Networks**, Springer, pp. 491-512.

Stallings William, (2007), Network Security Essentials, **Pearson Prentice Hall**.

Tan Hailun, Ostry Diethelm, Zic John and Jha Sanjay, (2009), A Confidential and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Networks, **Proceedings of the second ACM conference on Wireless network security**, pp. 245-252.

Tian Jingwen and Gao Meijuan, (2009), Intelligent Community Intrusion Detection System Based on Wireless Sensor Network and Fuzzy Neural Network, **ISECS International Colloquium on Computing, Communication, Control, and Management (Sanya)**, IEEE, vol. 3, pp. 102-105.

Wang Ronghua, Du Wenliang and Ning Peng, (2007), Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks, **Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing**, pp. 71-79.

Wood Anthony D. and Stankovic John A., (2002), Denial of Service in Sensor Networks, **Computer**, IEEE, vol. 35, no. 10, pp. 54-62.

Yan K.Q., Wang S.C. and Liu C.W., (2009), A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks, **Proceedings of the International MultiConference of Engineers and Computer Scientists**, vol.1, pp. 411-416.

حماية شبكات الإستشعار اللاسلكية ضد هجمات الحرمان من الخدمات

إعداد
علا عبد الرحيم كراجة

المشرف
الدكتورة إيمان المومني

المشرف المشارك
الدكتور حازم الحيارى

ملخص

يعتبر التأكد من مصداقية بث المعلومات في شبكات الإستشعار اللاسلكية من العمليات المهمة لحمايتها من أخطار الإختراق وبخاصة ما يهدف منها إلى تعطيل الخدمات الموفرة من قبلها. بشكل عام، يوجد طريقتين لتحقيق مصداقية البث في هذه الشبكات مثل TESLA و التوقيع الإلكتروني (digital signature) إلا أن هاتين الطريقتين أيضا معرضتين لخطر هجمات تعطيل الخدمات. إذ يقوم المهاجم ببث عدد كبير من الرسائل المزيفة بهدف استنزاف موارد الشبكة وخصوصا مصادر الطاقة فيها.

يهدف البحث في هذه الأطروحة إلى تقديم حل جديد يدعى IPDS (Intrusion Prevention and Detection based Scheme - نظام منع وكشف هجمات الإختراق) مركب من جزئين يهدف إلى حماية شبكات الإستشعار اللاسلكية من هجمات الحرمان من الخدمة. يحاول الجزء الأول من الحل المقترح من تخفيف أضرار المهاجم على سير عمل الشبكات في حين أن الجزء الثاني يحاول تحديد المهاجم وعزله لإيقاف استقبال الرسائل المزيفة منه.

لتوضيح مدى فعالية النظام المقترح في كشف وإيقاف هجمات الإختراق، تمت مقارنته مع حلول أخرى مقترحة في الدراسات السابقة في ضوء معيارين: أولهما المتوسط الحسابي لنسبة التأخير الحاصل على الرسائل الموثوقة بسبب تعرض الشبكة لهجمات الإختراق. أما الثاني فيقيس مقدار الطاقة المصروفة على إستقبال وإرسال الرسائل المزيفة.

وقد أظهرت نتيجة تطبيق النظام المقترح أثر واضح في تخفيف نسب التأخير والطاقة المصروفة مقارنة بالحلول المقترحة في الدراسات السابقة. إذ تفوق النظام المقترح (IPDS) على بقية الأنظمة المطبقة في الدراسة من حيث تقليل المتوسط الحسابي لنسبة التأخير للرسائل الموثوقة بنسبة تصل إلى 55% مقارنة مع طريقة النافذة المتكيفة، و65% مقارنة مع طريقة النافذة المتغيرة، و90% مقارنة مع طريقة التحقق أولاً. ومن جهة أخرى، وجد أن النظام المقترح (IPDS) يقلل نسبة الطاقة المستهلكة في استقبال الرسائل المزيفة إلى حد يصل إلى 90%، و نسبة الطاقة المستهلكة في تمرير تلك الرسائل إلى حد يصل إلى 73% مقارنة مع طريقة النافذة المتكيفة. أما بالمقارنة مع طريقة النافذة المتغيرة، قلل نظام ال (IPDS) نسبة الطاقة المستهلكة في استقبال وأيضاً في إرسال الرسائل المزيفة إلى حد يصل إلى 98%.