Securing Broadcast Authentication in Wireless Sensor Networks Against DoS Attack

Ahmed Alghamdi1† and Mohammed Arozullah2††,

Department of Electrical Engineering and Computer Science, Catholic University, Washington, DC, USA

ABSTRACT

Timed Efficient Stream Loss-tolerant Authentication (TESLA) and digital signature are security implementations of broadcast authentication in Wireless Sensor Networks (WSNs). Both approaches, however, are considered vulnerable to DoS attacks. Encountering this attack requires a scheme that addresses two security measures: prevention and detection.. This paper provides a hybrid solution between prevention and detention scheme., namely Combined Prevention and Detection Scheme (CPDS). The prevention part is based on the dynamic window scheme installed at each sensor node. The detection part adopts the Fuzzy Logic Intrusion Detection Scheme (FL-IDS) installed at monitor nodes. Both parts work coherently where the detection part relies on predefined information provided by the prevention part. The evaluation metrics includes the average broadcast delay of authentic messages and the energy consumption. The implemented CPDS scheme improved the average broadcast delay of authentic messages by 75% and 43% compared to Authentication first mode and Dynamic window scheme respectively. In terms of energy consumption, CPDS was evidently more efficient by 60% and 30% compared to Authentication first mode and Dynamic window scheme respectively.

Key words:

Wireless Sensor Network, DoS Attack, Security, Denial of Service, Broadcast Authentication.

1. Introduction

As a result of the growth of networks over the years, the network attacking tools and methods have greatly improved. In 1980's the attackers needed to have a sophisticated level of computer programming and networking knowledge. Nowadays the attackers' methods and tools have improved drastically. The attackers are no longer in need of such sophisticated level of knowledge. Wireless Sensor Network is currently used in many variant applications; for example military, medical, navy, emergency and even civilian applications. In these networks, the sensors are actually restricted by resource constraints, regarding power consumption, transmission rate, available bandwidth and computational power.

2. Problem Definition

The actual communication approach used in Wireless Sensor Network is broadcasting requests or commands from the base station to the sensor node; after that, the sensor nodes need to respond to those requests. Hence, the broadcast request needs to authenticate properly whether the requests are originally sent from the base station by using broadcast authentication to ensure the authenticity of messages. All the properties are satisfying the authentication property to provide a proof of the base station identity. Digital signature [11] and TESLA [12] are most the important well-known approach. Initially, the digital signature is based on public key cryptography is considered impractical due to the high computational power needed to perform it with the constraints on resources in Wireless Sensor Network. However, recent studies have used modern devices to perform public key cryptography with more optimized digital signature techniques that is possible to perform PKC on resource-limited sensors.

The verification of Elliptical Curve Digital Signature Algorithm using 160-bit elliptical curve on AT Mega 128 processor will take 1.62 seconds [15]. TESLA is classified as a symmetry approach; it provides asymmetry property by delaying the disclosure of authentication keys by using the uniqueness of key per time interval. Both Digital signature and Timed Efficient Stream Loss tolerant Authentication are vulnerable to DoS attacks. Since an attacker can inject a forged message forcing the sensors to do some unnecessary verification. This will result in spreading the forged message across the entire network, leading sensors to perform large computation and eventually draining the battery power of sensor nodes [16] and [9].

3. Purpose

Many approaches were proposed to reduce unnecessary verification to secure broadcast authentication and forwarding of broadcast message. Some of them targeted for containing the impact of DoS attacks to include a small portion of the network. Whereas there are some that attempted to keep such attacks from propelling against the broadcast authentication approaches.

As of now, there is no such scheme that can identify and avoid DoS attacks from abusing the broadcast authentication process. Hence, this paper goes for proposing a combined scheme that can counteract and

Manuscript received April 5, 2015
Manuscript revised April 20, 2015

distinguish DoS attacks, especially those attacks that start against the broadcast authentication within the WSN.
The prospect scheme in this analysis is named Combined Prevention Detection based Scheme (CPDS). It is focused on the two main sections:

1. prevention part
2. detection part

In the prevention part, the dynamic window scheme proposed by (Wang, et al, 2007) [9] is used as first line of defense that can decrease the harm caused due to DoS attacks to include just a small portion of the network. However, this part is installed in every sensor node.
In the detection part, for each monitor node [10], a proposed Fuzzy Logic based Intrusion Detection Scheme (FL-IDS) is used as second line of defense. This second resistance approach relies on the accessible data created by the dynamic window system and uses the Fuzzy Logic Inference System (FIS) so as to settle on a right decision about the attacker. In section 4 we can review previous work related preventing DoS attacks against broadcast authentication. Then we illustrate the overall system in section 5. Section 6 will describes the simulation results and discussion regarding broadcast authentication against the DoS in wireless sensor network. Finally section 7 contains a conclusion to this paper.

3.1 Scope

The proposed scheme will detect the forged message and reduce the unnecessary computation in broadcast authentication. In this way we can easily reduce the injection of fake message in wireless sensor network by attackers as well as minimize the average broadcast delay.

3.2 Goals

To prevent and detect DoS attack and reduce the energy consumption and increase the wireless sensor network life time by doing proper broadcast authentication and verification against the forged message. This scheme had provided the improvement in energy efficiency, throughput and delay.

.

Hardware Configuration

- Processor : Intel Core Due.
- RAM : 1 GB and above.
- Hard Disk Space : 20 GB and above.
- Input Device :Network Interface Card.
- Output Device : High resolution monitor.

Software Configuration

1. Operating System : Ubuntu 12.04.2
2. Tools : NS2

4. Related Work

In Wireless Sensor Networks, many solutions have been proposed to contain or resist Denial of service DoS attacks against broadcast authentication to prevent unnecessary authentication and verification which leads to more battery consumption. They may differ in assumption and purposes, regarding many criteria. Since this can be distinguished as a hop-by-hop schemes such as proposed in [7] and not famed as hop-by-hop in [6]. In wireless sensor networks, the hop-by-hop scheme only resists the interrelated nodes with DoS attack. [21] Luk has described seven properties that are cardinally accepted for any broadcast authentication algorithm in wireless sensor network. By these seven properties which leads to resistant to compromised nodes, immediate authentication message set at irregular time interval period with high message entropy, less communication overhead, less power consumption in WSNs, increased wireless sensor network lifetime, low computation overhead and more robustness toward packet loss. Most current schemes satisfy almost all of them. The Digital signature will satisfy all the cardinal properties except low consumption overhead. In Message specific puzzle has been proposed by (Ning *et al*., 2008) [6], which is used to mitigate the DoS attacks. Weak authenticator technique has been used on every broadcast message.
The weak authenticator is not a replacement of authentication approaches like Digital signature and Timed Efficient Stream Loss-tolerant Authentication; instead it is used to differentiate the forged broadcast messages. A sensor node receives a broadcast message and will check it with the weak authenticator first to ensure that it's valid. Then the sensor node will perform the signature verification or packet forwarding by either using Digital signature or TESLA. These approaches have two limitations: they require a computationally powerful sender in order to compute the puzzle solution and they cause a delay in sending packets to receiver. In [14] proposed a new scheme that allows the receiver sensor node to recognize forged message before 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. In [8] has proposed to use Pre-authenticator filters to provide a first line of authentication before the main broadcast authentication such as Digital Signature and Timed Efficient Stream Loss-tolerant Authentication is applied.
This approach will follow group based or key chain based pre-authentication filter; which requires key distribution in re-grouping. The group based approach provides the

possibility of compromised node within the group and results in communication overhead due to additional key management mechanism. Tan [19] demonstrated a solution that pursues to provide both confidentiality and authentication that resists the possible Denial of service attacks Dos, in order for code dissemination specifically which is the process of distribution new programs image over the wireless sensor network to update program versions. Hence this approach depends on the idea of chaining then relay in finding the cipher puzzle to avoid denial of service attack when compared to MSP in [8]. They this is better than the Message Specific Puzzle due to chaining of hash results in previous packets. Huang *et al*. proposed a broadcast authentication scheme in [17] called DREAM which stands for DoS Resistant Efficient Authentication Mechanism. This process which contains a false packet by frequently using authentication first and which nodes must verify the authenticity of the message before forwarding the packet and also its sends the small number packet to receiver node without verifying the packet; which reduces the overall delay. So the remote node gets the message more quickly. In this solution the sensors periodically exchange hello message with one hop neighbor, then the one hop neighbor size is included in each hello messages. Then these messages must be signed and verified. This introduces an extra overhead. DREAM is used in MANET. In [22] focused on environment in networks, the nodes know each neighbor node at least once in a while. In Ren [13] use the bloom filter to allows the node to a certain receiver is part of the network, but bloom filter which results in false positive, which provides additional security concerns. Similarly in research of (Du *et al*., 2008) depends on nodes to be verified with each other neighbor node in the network by using the sender specific one way chain. Keys in the chain are unique for each node then each receiver must verify the key according to which the message has been received from.

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.

The idea behind this solution is to conduct using booth 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 assed form 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.

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, [20] Kesselman 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 message the window must rapidly decrease, and when authentic message is received 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 = 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, fakes 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 [9].

The scheme based on specification for the intrusion detection is explained by using the simulator scenario developed in C#. Moreover, such type of scheme based specification accomplishes a higher and better intrusion detection rate along with a low rate of false positives. Each node of the wireless sensor network needs to be considered in a unique manner. At times, it is observed that the schemes based on the centralized distributed detection process may not recognize the behavior of the network. Hence, for the wireless sensor network, the distributed security system is an ideal approach. Also to achieve effective throughput values and optimized energies for the wireless sensor networks, the intrusion detection schemes must be applied on to the clustered hierarchical routing protocol [1].

There are two schemes based on the traffic control parameter that can be utilized to predict the concept of fuzzy logic. The network efficiency for the conventional as well as measurement-based connection admission control is improved with the help of prediction of fuzzy logic. In addition to the network efficiency, the QoS (Quality of Service) measurements have also been observed to depict efficient values by using the fuzzy logic prediction. Also, the implementation of fuzzy logic to the traffic controller schemes proves to be very effective as compared to the conventional ones [2].

It has been observed that whenever an anomaly detection-based security scheme is applied, the large scale wireless sensor network demonstrated a stable behavior. Since each node of the WSN (wireless sensor network) is capable of building a statistical model based on the adjacent nodes, the intrusion detection within the network becomes easier. A node can also successfully recognize an intrusion when smaller set of features for the received packets are considered.

The research has implemented the algorithm for the anomaly detection by executing it separately at each node. The intrusion detection and containment procedure are improved by using the cooperative algorithms demonstrating low levels of complexity. There have been diverse feature sets that are available for the various routing algorithms as well as for the algorithms dealing with medium-access and distributed control access systems. There is a continuous need for establishing optimized node features that are able to address the detailed vulnerabilities and result in introducing better detection algorithms with sensor node features [3].

The use of hybrid intrusion detection system for the wireless sensor network has high rate of success results. This coupled with the misuse and anomaly detection models promotes higher accuracy with effective detection rate.The simulation results also depict the efficiency of the scheme as it is highly energy efficient, economical and supports accurate detection. The scheme is yet to be tested for detecting the attacks in an environment dealing with radio jamming attacks [4].

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 [10].

5. Combined Prevention Detection based Scheme (CPDS)

The proposed CPDS 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 1. The proposed detection system (FL-IDS) in this paper could be categorized as distributed-centralized IDS [1]. 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) use 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.

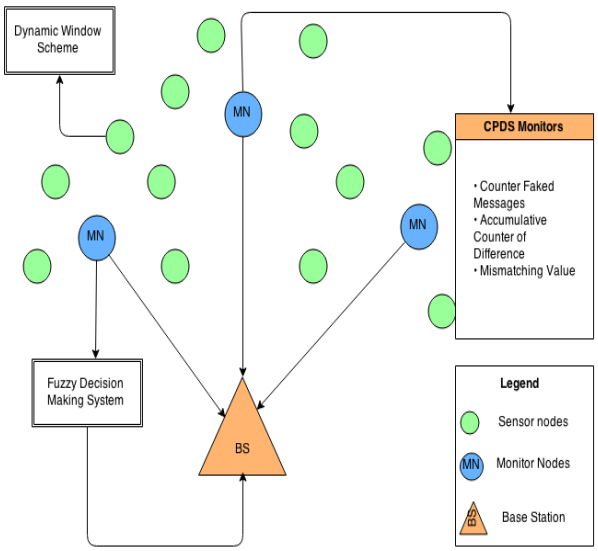

Figure 1: CPDS Architecture

5.1 System Design

As shown in Figure 1and 2, when a message arrives to the CPDS system the prevention and the detection processes work in parallel. Then, each sensor node will run the prevention process which is based on the dynamic window scheme proposed by (Wang, et al., 2007). Its basic idea depends on that each sensor node has local parameter called window size (W) which represents the maximum number of hops which the message can be forwarded without being verified. On the other hand, each message has hop counter (dist) that represents the number of hops the message passed by without being verified. By message arrival, the condition (dist against W) must be verified. If (dist>=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 (dist>=W) is not valid, 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 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 huge number of authentic messages and growing in the windows sizes occurs, contained attackers can again introduce the threat to the network. This necessitates a second line of defense in order to protect these sensors from the adversaries.

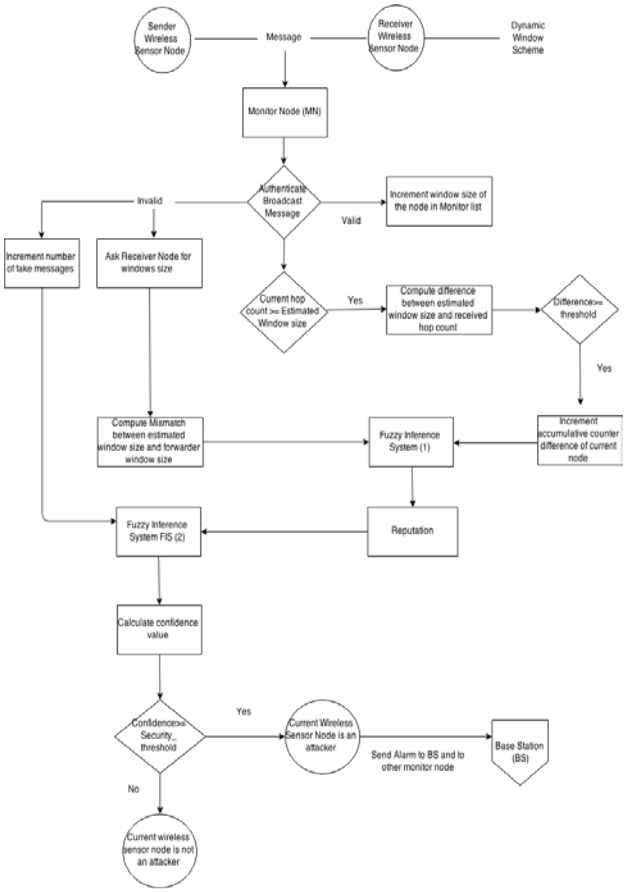

Figure 2: The proposed CPDS Flow Chart

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 use three factors. 1) The total number of faked messages sent by specific node, 2) the accumulative counter of the difference between the estimated window size that computed by the monitor node and the received hop counter, 3) the mismatching value between the estimated window size and the received hop 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 BS and other monitor nodes indicate the existence of an attacker. This confidence 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 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 we named (est_win); 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 3. If it is valid, then the monitor node will update the estimated window size (est_win) increasingly for the node on its neighbors list. To update the window size, the monitor node uses the updating function basic on AIMD law that is used in the dynamic window scheme (prevention part) according to equation:

Increasing:

$\psi f(\omega) = \omega + 1$ (unless ω max is reached).

Decreasing:

$$\psi s(\omega) = \left[\frac{w}{2}\right] \text{ (unless } \omega \text{ min is reached).}$$

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 in the proposed CPDS for the prevention and detection parts. Table 1 demonstrates the notations and parameters used in CPDS.

Table 1: Notations and Parameters used in CPDS

Attributes	Description
W	Window size on Sensor Node
CW	Current Window Size
Fake_Message_Counter	Counter of Fake messages
est_win	Estimated window size in MN
Id	Index from the chain
M	Broadcast Message
Dist	Hop counter on broadcast message

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 receives 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.

CPDS Algorithm

Input: msg(M, dist, id)

```
1.  Msg=( M,dist , id)
2.  Validity = Authenticate the broadcast message
3.   validity = true
4.  // update the estimate window size
5.  Est_win= CW +1
6.  else
7.  // compute first factor
8.  Faked_Messages_Counter=Faked_Messages_Counter+1;
9.  //compute second factor
10. if Received_Hop(dist)>=Estimated_Window (est_win)  Then
11. Difference=( dist – est_win );
12. if Difference>=2 Then
13. Accumulative_Counter_Difference=Accumulative_Counter_Difference+1;
14. end if;
15. end if;
16. // Computing third factor
17. ask forwarder of the faked message for its window size
18. Mismatch = Estimated_window – Received windows size;
19. //send the second and  factor to the FIS 1
20. Reputation = (Accumulative_counter_Difference, Mismatch)
21. // send the output first fuzzy system and first factor to confidence calculator system
22. Confidence = confidence(Reputation(SN), Faked_Messages_);
23. if confidence>=security_threshold
24. Current SN is an attacker
25. Send an alarm  to BS and announce the attacker to monitor nodes
26. Exclude current SN
27. else
28. SN is not an attacker
29. //Update est_win for all of the neighbors of the monitor node
30. Est_win = CW/2
31. Esit_win = CW;
```

Figure 3: 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 (dist>=W) in the prevention process (dynamic 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 (est_win; computes by the monitor node for the node) against received hop counter (dist) 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 the monitor node computes the difference between est_win and dist (dist-est_win). 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 (dist-est_win) difference unless it exceeds a certain threshold, is that the monitor node will take into account the probability of any mistakes in computing the est_win, 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 est_win and dist (dist-est_win) is greater than predetermined threshold, this means that dist is greater than est_win 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 mismatching factor in FL-IDS. This factor represents the absolute difference between the estimate window size (est_win) 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 node request the current windows size value, this value of windows size will be decreased base on AIMD law because this message is fake. Then the forwarder sends a small replay message with updated value.. 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 [est_win - w].

In case if the message is authentic the mismatching value will be zero but if node received fake message the window size in the node will be less than estimate window size in monitor node and this indicates a benign behavior.

After the evaluation process of the three factors, the monitor node will update est_win for all of its neighbors. The reason behind this 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 discusses in the following subsection.

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

In order to interpret the results obtained from measuring the three factors mentioned earlier, the proposal FL-IDS uses two Fuzzy Logic Inference Systems (FIS) that are implemented in two tiers as shown in Figure 4. 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.

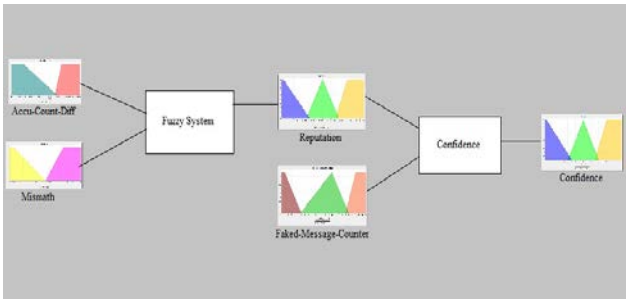

Figure 4: Two Tier FL-CPDS

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 maybe 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 implements 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 at anytime [19].

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 repetition 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.
Each input and output in FL-IDS will be given a fuzzy membership function according to its value. Figure 5 shows the fuzzy membership function for the accumulative counter of difference that ranges from zero to three. 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 three; that means the system can tolerate only three 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 difference between est_win and dist, 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. 3), this means that multiple recurrent large dist and est_win differences were recorded and this frequency of these recurrent episodes exceeds the predetermined threshold, so the fuzzy value will be high.

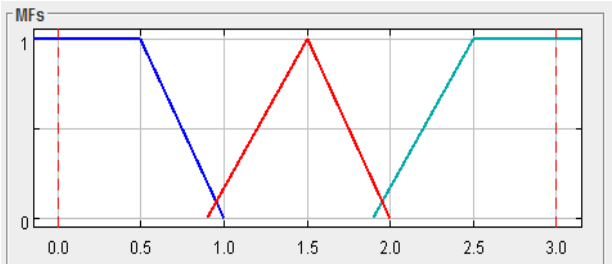

Figure 5: Fuzzy membership function for the accumulative counter of difference factor

Figure 6 shows the fuzzy membership function for the mismatching value that ranges from zero to two. 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. 0.5), then this value will be assigned a low fuzzy value, because the

absolute difference between the estimate window size (est_win) in monitor node and window size in sensor node (W) is considered low. On the other hand, if the mismatching value is high such as (e.g. 1), then the fuzzy value will be high, because the probability of mistakes is low and the difference between two windows are large. Thus, the probability of the attacking existence is high.

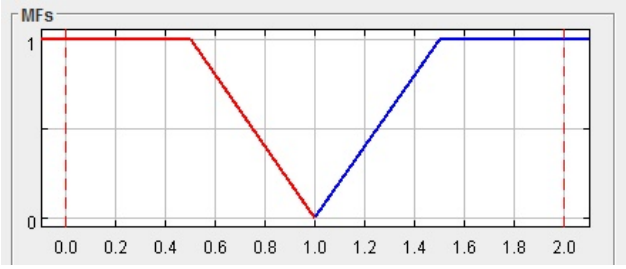

Figure 6: Fuzzy membership function for mismatching factor

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 7.

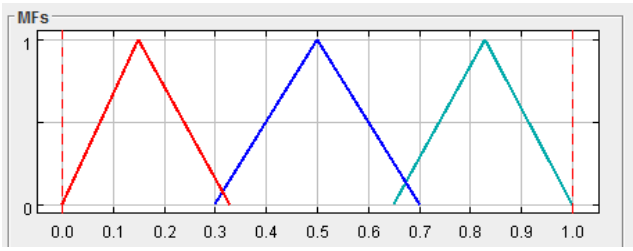

Figure 7: Fuzzy membership function for reputation of output parameter.

According to Table 2, 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. 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 2: 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 and 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 4.

Figure 7 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. 0.7), this means the probability of attacking existence is high, so the fuzzy value will be high.

Figure 8 shows the fuzzy membership function for the counter of faked messages factor that ranges from zero to twenty. 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. 2), that means, the forwarder of the message forwarded just 2 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 2 is low.

On the other hand, if this value is high (e.g. 7), them 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.

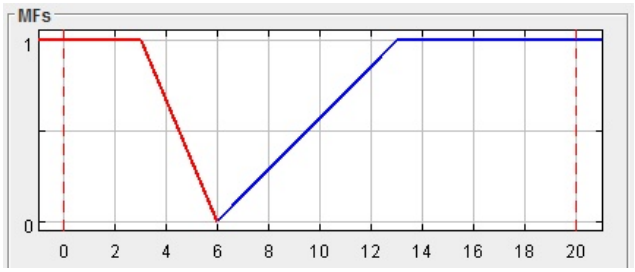

Fig 8: Fuzzy Membership function for counter of faked message factor

The reputation, the counter of faked messages value 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 9 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 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, the that will ensure the presence of an attacker.

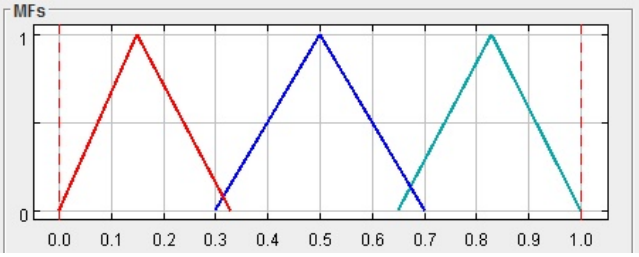

Fig 9: Fuzzy membership function for obtaining the confidence value

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 compare the confidence value against the security threshold (confidence value>= security threshold), then an alarm must be generated and sent to BS and to all monitor nodes. The security threshold will depend on the sensitivity of the application for which the WSN is applied; the BS nods 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 application (e.g. military environment) and cannot to 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.

6. CPDS System's Result Evaluation.

The proposed network of 17 sensor nodes has created for this simulation. A sparse network implemented as a sparse graph has been formed by randomly deploying these nodes. This kind of network structure is an optimum environment to analyze the problems which include broadcast delay and energy consumption. In sensor networks every node is connected to a large number of nodes through a single hop; hence, messages can be exchanged through short paths that require relatively fewer hops. Therefore, to generate such a sparse network in this implementation, the maximum set of neighbors for each node is limited and the number is based on the size of the network.
Additional external static monitor nodes are deployed in a random and dynamic manner in the sparse network to implement CPDS. It means that the number of deployed monitor nodes can be changed according to their efficiency in monitoring their neighbors'. In this simulation, there would be 2 monitor nodes and each one will be in charge of monitoring 17 sensor nodes which are in its transmission range. It is assumed that these monitor nodes have higher capabilities than the ordinary sensor nodes but are not as powerful as BS.
The maximum window size for each sensor node and for all of the neighbors needs to be determined with respect to the size of the network. It can be computed according to the following equation:
$max\_win = N^2 / 100$
Where N is the total number of sensor nodes in the network (which is 20 in this case). The maximum window size in this simulation is 4.

6.1 Energy Consumption under intense DoS Attacks

Here the authentic scheme, Dynamic window scheme and CPDS are scaling from low to high and note that it is increasing accordingly from 2 to 14. By to comparing authentic scheme and dynamic window scheme. Both of CPDS and Dynamic window maintains the low energy consumption than authentic scheme. Whereas the authentic scheme is having the high energy consumption and it is moving towards high during simulation time.

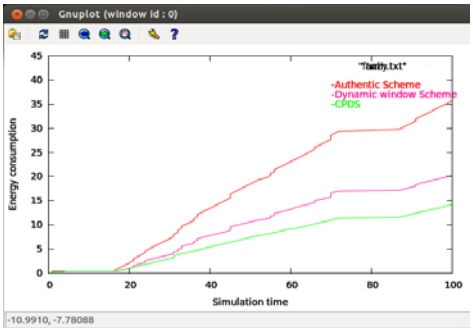

Figure 10: Total Energy of the sensor network

Figure 10 shows the various energy consumption for each scheme during the simulation time. The energy consumption measure indicates the power needed by each node toward processing message authentication. The simulation setup of the combined scheme for the energy consumption threshold for each node was 200mj for authentic messages and rise to 400mj in the case of fake messages. Thus, the difference between these two consumptions indicates a abnormal behavior. Comparing the three schemes, CPDS has the lowest energy consumption as it only consumes 14j during the simulation time of 100s. This low consumption was maintained throughout the simulation under the intense DoS attacks. On the other hand, the dynamic window scheme was evidently less efficient than CPDS as it consumes 21j during the same simulation time of 100s. Similarly, authentic scheme has the most energy consumption in this simulation at 37j. Thus, CPDS was evidently more efficient by 60% and 30% compared to AFS and DWS respectively.

The level of energy consumption is associated with the mechanism of broadcast authentication each scheme implement. The combined scheme (CPDS) has the least energy consumption due to the smart mechanism it implements for authentication. Monitor nodes compare previous and current energy consumption for their neighbor nodes upon unusual levels.. However, any mismatch between the requested energy consumptions is alarming as it reflects the node processing of faked messages. The reduced overall energy consumption under this scheme is due to the fact of turning the infected node alone to authentication mode while keeping other nodes at normal operation. On the other hand, the slightly higher consumption of the dynamic window scheme is due to the fact that each node under DoS attack scenario is turned to authentication mode. Hence, higher overall consumption results from this shift in the whole network.

6.2 Average Broadcast Delay under intense DoS Attacks

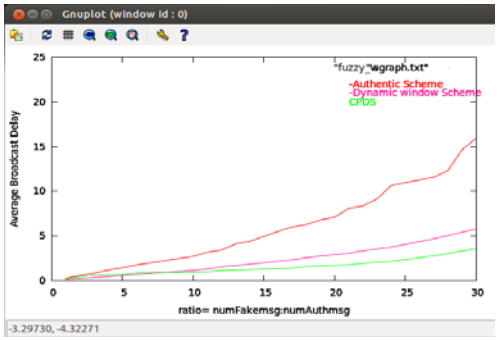

Figure 11: Average Broadcast Delay

Figure 11 shows the average broadcast delay of authentic messages for each scheme during the simulation. The ratio of fake messages to authentic ones is calculated by dividing the number of fake messages over the number of authentic messages. Under DoS attack, an incremental ratio is noticed as the number of fake messages increases. Accordingly, the average broadcast delay increases as well for each scheme as nodes consumes more time authenticating messages. The implemented CPDS scheme improved the average broadcast delay of authentic messages by 75% and 43% compared to AFS and DWS respectively.

CPDS has the least average broadcast delay of authentic messages due to its smart implementation of authentication mode using Fuzzy logic; only the infected node shift to authentication. On the contrary, the dynamic window has a higher average delay as it shifts between forwarding and authentication based on the window size (w) and the number of hops the last authentic message passed (dist). Upon comparing the two parameters of the dynamic scheme, the shift occurs to authentication mode if distance is greater than or equal to the window size locally store at the node; this shift to authentication mode locks until the distance parameter becomes smaller. Thus, dynamic window has a slightly higher average delay than CPDS.

Evaluation of the implemented scheme indicated an improved overall performance compared to the other two existing schemes: authentication first scheme (AFS) and dynamic window scheme (DWS). The evaluation metrics includes the average broadcast delay of authentic messages and the energy consumption. The implemented CPDS scheme improved the average broadcast delay of authentic messages by 75% and 43% compared to AFS and DWS respectively. In terms of energy consumption, CPDS was evidently more efficient by 60% and 30% compared to AFS and DWS respectively.

7. Conclusion

The contribution of this paper aims at avoiding DoS threats to WSN while improving its performance. This objective is achieved through securing the broadcast authentication from the common Denial of Service (DoS) network attack. Accordingly, researchers have mainly optimized two implementations in Wireless Sensor Networks (WSNs): Timed Efficient Stream Loss-tolerant Authentication (TESLA) and digital signature. Moreover, this paper has added to the efforts of securing the broadcast authentication through successful implementation of a comprehensive scheme, namely Combined Prevention and Detection Scheme (CPDS). The invented scheme improves the security of broadcast authentication in WSN against DoS attacks. The prevention part is based on the dynamic window scheme

installed at each sensor node. The detection part adopts the Fuzzy Logic Intrusion Detection Scheme (FL-IDS) installed at monitor nodes. Both parts work coherently where the detection part relies on predefined information provided by the prevention part. Adoption of the Fuzzy Logic Inference System (FIS) helps to determine suspicious nodes and make the final decision about the attack. The scheme proactively identify misbehaving nodes through four measures: 1) comparing the node's own current window size and the monitor's node estimate window sizes, 2) Computing the difference between hop counter and estimate window size in monitor node, 3) setting a counter of fake messages). The implementation has the advantages of reserving the resource-constraint networks and extending their expected lifetime.

Evaluation of the implemented scheme indicated an improved overall performance compared to the other two existing schemes: authentication first scheme (AFS) and dynamic window scheme (DWS). The evaluation metrics includes the average broadcast delay of authentic messages and the energy consumption. The implemented CPDS scheme improved the average broadcast delay of authentic messages by 75% and 43% compared to AFS and DWS respectively. In terms of energy consumption, CPDS was evidently more efficient by 60% and 30% compared to AFS and DWS respectively.

As a future work, studying the impact of using different attacking models on the performance of the CPDS and different network topology.

References

[1] Ashfaq Hussain Farooqi, Farrukh Aslam Khan, Jin Wang, Sungyoung Lee (2013). "A novel intrusion detection framework for wireless sensor networks"

[2] Hiam Hiok Lim and Bin Qiu (2001). "Fuzzy logic traffic control in broadband communication networks"

[3] Ilker Onat and Ali Miri (2005). "An intrusion detection system for wireless sensor networks"

[4] Abror Abduvaliyev, Sungyoung Lee and Young-Koo Lee (2010). " Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks "

[5] David R. Raymond and Scott F. Midkiff (2008). "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses"

[6] PENG NING, AN LIU and WENLIANG DU (2008). "Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks"

[7] QI DONG and DONGGANG LIU (2013). "Providing DoS Resistance for Signature-Based Broadcast Authentication in Sensor Networks"

[8] Qi Dong Donggang Liu, Peng Ning (2008). "Pre-Authentication Filters: Providing DoS Resistance for Signature-Based Broadcast Authentication in Sensor Networks"

[9] Ronghua Wang, Wenliang Du, Peng Ning (2007). "Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks"

[10] Sang Hoon Chi and Tae Ho Cho (2006). "Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks"

[11] Stallings, W. 2014. Network Security Essentials, Pearson Prentice Hall 5th edition.

[12] Perrig, A., R. Canetti, J. D. Tygar and D. Song, 2000. "The TESLA Broadcast Authentication Protocol", work was done at UC Berkeley and IBM Research.

[13] Ren, K., S. Yu, W. Lou and Y. Zhang, 2009. "Multi-User Broadcast Authentication in Wireless Sensor Networks", *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 8.

[14] Al-MomaniIman, Karejah Ola and Abdullah Lamya, 2010, Reducing the Vulnerability of Broadcast Authentication against DoS Attacks in Wireless Sensor Networks, Mediterranean Journal of Computers and Networks.

[15] Gura, N., A. Patel, A. Wander, H. Eberle and S. Shantz, 2004. "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPU", In CHES 2004, Cambridge, MA.

[16] Wood, A. D. and J. A. Stankovic, 2002. "Denial of Service in Sensor Networks," IEEE.

[17] Huang, Y., W. He, K. Nahrstedt and W. C. Lee, 2008. "DoS-Resistant Broadcast Authentication Protocol with Low End-to-End Delay", Computer Communication Workshops.

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

[19] 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. 352-3