Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme

Rawan S. Hassoubah*, Suhare M. Solaiman, Manal A. Abdullah
Department of Computer Science, King Abdul Aziz University, Jeddah, Saudi Arabia.

*Corresponding author. Tel.: 00966500087386; email: r.hassoubah@gmail.com
Manuscript submitted August 18, 2014; accepted February 12, 2015.
doi: 10.17706/ijcce.2015.4.3.156-165

Abstract: Wireless sensor networks (WSN) is type of networks that recently emerged to have many important applications. They are targeted against many attacks such as sinkhole, selective forwarding, hello flood and node replication attacks. Location verification algorithms are used to detect and verify nodes locations in WSN and can be used for intrusion detection system (IDS). In this paper, we purpose an IDS based on nodes location verification algorithm for WSNs to detect the locations of malicious nodes. In addition, this IDS detects hello flood attack and report the attack and goal nodes. The presented IDS achieved high detection rate with the average value 9.0643 and low false positive rate with average 0.3263 and low false negative rate with average 0.1362.

Key words: Intrusion detection, wireless sensor network, location verification, hello flood attack, greedy filtering using matrix, GFM, on-spot location verification.

1. Introduction

Wireless sensor networks (WSNs) have become a hot research topic in recent years. Applications include military, rescue, environment monitoring, and smart houses. A WSN is composed of hundreds or even thousands of small, cheap sensors nodes which communicate with one another wirelessly [1]. WSNs are distributed in nature using the multi hop communication model. These networks are usually deployed in such areas where direct human interaction is either impossible or very difficult. Furthermore, WSNs have limitations in terms of computation, bandwidth, memory, and energy. These limitations are considered while designing any proposal for such networks. Due to the hostile environments of WSNs, security is one of their most important aspects.

Intrusion detection systems (IDSs) are widely used for securing WSNs. IDS has the ability to detect an intrusion and raise an alarm for appropriate action due to the energy and computational power limitations, designing appropriate IDS for WSN is a challenging task [2].

WSNs are targeted against number of security attacks that affects its performance. The most important ones are such as, sinkhole/blackhole attack, selective forwarding attack, node replication attack, hello flood attack and wormhole attack. One of those attacks is the hello flood attack where this type of attack appears in networks that its routing protocols need to broadcast HELLO packets in order to discover one-hop neighbours. An attacker node with a large radio range and enough processing power can send HELLO packets to a large number of sensor nodes by flooding an entire section of the network. A node which receives such a packet may assume that the attacker is within normal radio range. Hence, sensor nodes can

be persuaded that the adversary is their neighbour. Possible solutions to detect this type of attacks could be the use of bidirectional verification of links, secure multipath routing, and use of multiple base stations [3]. The best practice to secure wireless networks is to implement such a security mechanisms; that is why IDSs are more critical in wireless networks.

In WSNs, localization of nodes is important in applications like target tracking and environment monitoring. It is very important to obtain accurate location information to accomplish the related applications requirements. The locations of sensor nodes are very important for the following reasons: Network operations depend on the locations of sensor nodes, second, he events detected by sensor nodes usually should be bound with locations and location verification of sensors considered as security second line of defence. The location verification mainly categorized into two types either on-spot verification or in-region verification. On-spot verification performs two algorithms, namely, the greedy filtering by matrix (GFM) algorithm and the greedy filtering by trustability-indicator (GFT) algorithm. Both algorithms exploit the inconsistency between sensors' estimated locations and their "neighbourhood observations" (the messages that each sensor can receive from other sensors in its neighbourhood) [4].

In this paper, our focus will be on using the on-spot location verification, specifically, the GFM algorithm for verifying locations of sensors to differentiate between malicious nodes and others. Also, to perform intrusion detection for hello flood attacks and to improve the security level in WSN. In addition, achieve high detection rate for the location verification, low false positive and false negative rates for the intrusion detection process. The paper starts with presenting some related work in location verification and some solutions for detection of the hello flood attack in Section 2. Then, in Section 3 it discusses the hello flood attack. Next, Section 4 presents the proposed system in details starting with the GFM algorithm and the process of intrusion detection of the hello flood attack. Later, Section 5 discusses the results. Finally, Section 6 concludes the paper.

2. Related Works

In recent years, a large number of localization schemes such as [5]-[13] were proposed for Wireless sensor networks. Other approaches such as: [14], [15] used to filter out bad location references using stochastic methods. Yawen Wei and Yong Guanhave introduced greedy filtering by matrix (GFM) algorithm and trustability indicator (TI) algorithm [16], to explore the consistency between sensors' locations and their neighbourhood observations to detect location anomalies. Recently, Talasila and others in [17] proposed a location authentication protocol named LINK (Location verification through immediate neighbours knowledge).

Most of the location verification algorithms focus on detecting location anomalies, in other words, verifying if sensors' claimed locations are far away from their true locations and they do not take the application's requirements into consideration. In addition, such algorithms as [12], [14], [15], [18], [19], they don't completely eliminate wrong location estimations and in case of attacks. From this sense, Yawen Wei and Yong Guan have proposed an improved version of their work presented in [4]. They introduced a light weight location verification algorithm that is the first work that takes the application requirements into consideration. They have also considered their algorithm as a tool of defence against malicious attacks. The algorithm performs on-spot and in-region verification. Based on their results the verification achieved low cost either in hardware or communication overhead.

Security in WSNs has taken the attention of many researches. They have implemented many solutions to detect attacks or avoid them. Some examples of countermeasures that are designed to detect or avoid the hello flood attack are such as the Multi-path multi-base station data forwarding technique that is proposed in [20]. Also, author in [21] suggests that hello flood attack can be counteracted by using "identity

verification protocol". This protocol verifies the bi-directionality of a link with encrypted echo-back mechanism, before taking meaningful action based on a message received over that link. This defence mechanism becomes in effective when an attacker has a highly sensitive receiver and a powerful transmitter. If an attacker compromises a node before the feedback message, it can block all its downstream nodes by simply dropping feedback messages. Thus, such an attacker can easily create a wormhole to every node within range. Since the links between these nodes and attacker are bidirectional, the above approach will unlikely be able to locally detect or prevent a "hello flood".

In [22] the authors used a cryptographic technique to prevent the hello flood attack. They assumed that any two sensors share the same secret key and every new encryption key is generated on fly during the communication. This phenomenon ensures that only reachable nodes can decrypt and verify the message and hence prevent the adversary from attacking the network. But the main drawback of this approach is that anyattacker can spoof its identity and then generate attacks.

A security mechanism based on signal strength and geographical information is proposed in [23] for detecting malicious nodes that launching hello flood and wormhole attack. Another Neighbour-based IDS for WSN is implemented in [24]. This algorithm is based on signals that are sent between nodes to detect hello flood attacks. This algorithm is promising since the false positive is becoming lower and the false negative becoming higher with signal strength increased with an average false positive 0.28 and average false negative 3.76 with signal strength 5dB. We will compare our work against this model later in the paper. In addition, a threshold based algorithm is proposed in [25] to defend against flooding attacks in MANET. The mobile nodes use a threshold value to check whether its neighbors are intruders or not. The following section will introduce the hello flood attacks in WSNs.

3. Hello Flood Attacks

Some routing protocols in WSN require nodes to broadcast hello messages to announce themselves to their neighbors. A node which receives such a message may assume that it is within a radio range of the sender. However, in some cases this assumption may be false; sometimes an attacker with large enough transmission power could broadcast routing or other information to convince every other node in the network that it is its neighbor. For example, an adversary advertising a very high quality route to the base station could cause a large number of nodes in the network to attempt to use this route. But those nodes which are sufficiently far away from the adversary would be sending the packets into oblivion. Hence the network is left in a state of confusion. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are mainly affected by this type of attack. An attacker does not necessarily need to construct legitimate traffic in order to use the hello flood attack. It can simply re-broadcast overhead packets with enough power to be received by every other node in the network [20]. Such example of a hello flood attacker that has large radio range even larger than the base station is shown in Fig. 1.

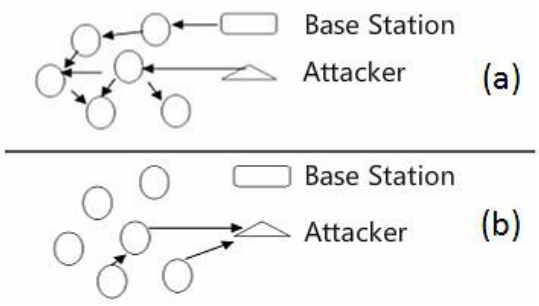


Fig. 1. Example of hello flood attacker.

As shown above in Fig. 1(a) an attacker broadcasting hello packets with more transmission power than a base station. Fig. 1(b) shows that a legitimate node considers attacker as its neighbor and also as an initiator [20].

4. Problem Statement

Due to the huge number of attacks that the WSNs could have those threats the system security and performance, a large number of designed systems were developed to detect or reduce the effect of such attacks. One of the famous attacks that the WSNs could face is the Hello flood attack as explained earlier. As a sequence, implementing an algorithm to detect the hello flood attack has taken the attention of many research works. Also, mainly in WSNs the use of location verification schemes is useful. It can be used to verify locations of sensors and to authenticate its trust ability. In addition, could be utilized as a second line of defense against attacks. However, there was no previous work that utilizes the location verification scheme to perform intrusion detection of specific type of attack in WSNs. In our work, we have noticed how the location verification model could be utilized to implement an intrusion detection model that detects specifically the hello flood attack. The intrusion detection system will later generate an alert of the attack to the network administrator. Therefore, it may stop or reduce the impact of it. The following sections will explain the system model and proposed algorithm in more details.

5. System Model and Assumptions

The system mainly will perform location verification to filter the nodes. Nodes with Abnormal locations or malicious will be considered as list of malicious nodes. The system will assume that one or more of these nodes are hello flood attack. Later, it will detect the attack from this list of malicious nodes and the intrusion detection system will generate an alarm whenever a hello flood attack is found.

In the system, each node finds its estimated location using some existing localization schemes which is called sensors' estimated or claimed locations. Node localization determines the distances between sensors' estimated locations and true locations. Each node has a communication range with certain radius. It is assumed that all sensors have the same communication range and each one of them will have certain number of nodes in its communication range.

In this paper our focus will be on utilizing the on-spot location verification scheme and specifically the greedy filtering by matrix algorithm (GFM) in [4] to detect the hello flood attack. This algorithm is chosen to be used in our system due to its lightweight and it is considering the application requirements. The on-spot verification, mainly, is to verify whether a sensor's estimated location is away from its true location less than a certain distance. The system has certain properties. First, it will be lightweight in terms of hardware cost and computation overhead. This means, it should not require expensive equipment and should not incur high communication overhead on sensor side, which would quickly consume the energy stored at sensors. Second, the verification algorithm should be able to provide accurate results even in presence of malicious attacks. Third, the system has to achieve high detection rate which is the ratio between the numbers of detected wrong locations and the number of all wrong locations. In addition, effectively achieve low false positive (false alarms) and low false negative rates. Where the false positive ratio is when the node is not a hello flood attack and the system detect it as a one, while the false negative ratio denotes the number of attacks that are not detected.

It is assumed that the hello flood attack is launched at the network and at least one attacker is producing flood messages. The system will perform the location verification and produce a list of malicious nodes with abnormal locations. It is assumed that the hello flood attack is one or more of these sensor nodes. Then, our algorithm will use the given results to make the intrusion detection. The information given by the location verifier will assist in further steps in attack detection. The following section will provide a detailed

explanation of our proposed algorithm.

6. Proposed Algorithm

The system first starts by applying the on-spot "greedy filtering by matrix (GFM) algorithm" to filter abnormal locations. Abnormal locations of nodes those that exceed certain difference between their estimated and true locations. Once the malicious nodes maybe located and filtered, we are resulted with a list of nodes that are likely to be any type of attack. And assuming that the hello flood attack is one or more of these malicious nodes, the algorithm will detect the attack. Intrusion detection of the hello flood will be done by testing every node that is malicious. The testing will be applied to some of the resulted information from the GFM. During detection process the intrusion detection system will generate an alarm whenever there is a hello flood attack exists.

In a sensor field with certain number of nodes n denoted by $S1$; ...; Sn. According to Fig. 2 the dark circles denotes sensor's true location and empty circles denotes sensor's estimated location. In case the distance was large then a localization error will occur [4].

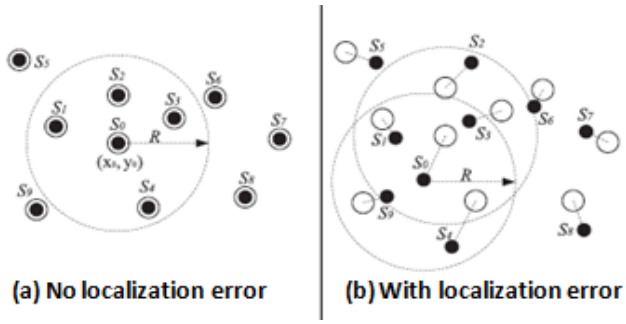


Fig. 2. Sensors filed [4].

6.1. Creating Matrices and Choosing Metrics

The GFM algorithm will create five square matrices each of size n ×n. The matrices are created depending on the reported information from sensors at verification centre side. The following are the matrices used:

- Observation matrix (M_o)
- Estimation matrix (M_e)
- Difference matrix (M_d)
- Inconsistency matrix (M_{inc})

And it applies four metrics for filtering the malicious nodes location they are:

- Active Difference Metric (AD_i)
- Passive Difference Metric (PD_i)
- Asymmetry Metric (AS_i)
- Consistent-Neighbor Metric (CN_i)

For further explanation about the GFM algorithm it is presented in [4] in much more details.

6.2. Malicious Nodes Filtering Procedure

In this section, we will describe how the GFM algorithm calculates all the above matrices and utilizes filtering metrics to greedily filter out abnormal locations or (malicious nodes).

The *VC* in the first round computes matrix M_{inc} and metrics AD_i, PD_i, and AS_i for all_i = {1; 2; ...; or n}. Then the metric values will be examined and if there is any sensor whose metric value exceed that metric's threshold, *VC* revokes the sensor with largest metric value (say node S_k), and sets all zeros to the kth row

and the *kth* column in matrixes M_e, M_o, and M_{inc}. This process will be repeated until no more sensors can be filtered out. After this, the metric CN_{iis} considered: sensors that do not have enough number of consistent neighbours are revoked. Finally, the remaining sensors are accepted by the *VC* as correctly localized sensors. In this procedure, the threshold value of different metric is obtained according to the desired detection rate and false alarm rate by training. Finally, after applying the greedy filtering procedure we have got a list of suspicious or (malicious) nodes with abnormal locations that are most likely to be an attack to the network. Later, it will pass through further steps for detecting if any hello flood attack exists among them.

6.3. Intrusion Detection of Hello Flood Attack

Once the location verification of sensor nodes has been applied, it is resulted with a list of malicious nodes with abnormal locations. Those will pass through the intrusion detection process to detect if any of them is a hello flood attack. The following is how the detection procedure implements. Once one of the malicious nodes has enough processing power and large communication range sends Hello message to a node or more (goal nodes) that are neighbours and in a specific communication range. The goal nodes will assume that this attack node (intruder) is their neighbour and in their same communication range, however, it does not. Therefore, goal nodes will perform regular interaction in the network through the routing path of the intruder. Thus, the intruder may utilize the packets or information that are interacted through it and performs undesired actions, damaging or changing it.

The intrusion detection process will start by monitoring those malicious sensors to detect any misbehaving. That information collected from previous step in location verification will be utilized as well. In order to detect the hello flood the system will first test the observation matrix (M_o), this matrix that already been computed using the sensors' neighbourhood observations. The detection algorithm checks if a malicious node sends a HELLO message and any goal node(s) have received it and at the same time the goal node does not observe it or flood back the message. And according to equation (1): and If $M_o(i, j) = 1$ but $M_o(j, i) = 0$ is satisfied. This means, if the intruder can observe the goal node while the goal node does not.

$$M_o(i, j) = \begin{cases} 1, if \quad sensor \quad S_i \quad observes \quad S_j, \\ 0, \quad otherwise \end{cases} \tag{1}$$

But this test is not enough for detection as some sensors may not observe others due to geographical difficulty or distribution. Then, the algorithm will proceed to perform another test for detection.

Second, the system will test the estimation matrix (M_e), this matrix that has been already computed to test if the sensors are located in the same communication range of each other. The detection algorithm will check for the distance between the estimated locations of the malicious node and goal node. It will test if the malicious node is out of the communication range of the goal node(s). Since according to equation (2):

$$M_e(i, j) = \begin{cases} 1, if & d_{ij} \le R, \\ 0, if & d_{ij} > R, \end{cases} \tag{2}$$

If $M_e(i, j) = 0$ this means , if the distance between the estimated locations of the intruder and the goal sensors is less than the R (radius of communication range of the goal) ,then, the intruder is out of the communication range of the goal node(s). Therefore, the location of the intruder confirms that they are not neighbours. Thus, the massages that are received are flood in and fake. Overall, after applying the two tests

to the malicious nodes, first, a message is received from the intruder to pretend to be its neighbour, but, the goal node cannot observe it. Second, the intruder is out of the communication range of the goal node. This makes it as a hello flood attack and Fig. 3 illustrates the proposed algorithm.

Intrusion Detection of Hello Flood Attack Algorithm.

// Location verification to filter nodes that are malicious

1. Compute matrix M_{inc}
2. Compute the metrics *AD*, *PD*, AS for all sensors in the field
3. **While** (sensor *Si* exists that can be filtered)
4. **if** *ADi*>*AD*_threshold
5. **then** revoke *Sk* that AD_k is the largest among all sensors.
6. **else if** $PD_i > PD_i$_threshold
7. **then** revoke S_k that PD_k is the largest among all sensors.
8. **else if** $AS_i > AS_i$_threshold
9. **then** revoke S_k that AS_k is the largest among all sensors.
10. Set zeros to *kth* row and *kth* column in M_e, M_o, M_{inc}
11. Recalculate metrics *AD*, *PD*, *AS* for all sensors
12. **While** (sensor S_i exists that $CN_i < CN$_threshold)
13. Revoke sensor S_i for not having enough neighbours.
14. Verify remaining sensors not revoked.

Intrusion Detection of Hello Flood Attack Algorithm (Cont.)

/ /Detection of the Hello Flood

15. while (malicious sensor **Smi** exists)

If $M_o(i, j) = 1$ and $M_o(j, i) = 0$
then if $M_e(i, j) = 0$
then sensor *i* is a Hello Flood attacker

Fig. 3. Algorithm of intrusion detection of hello flood attack using location verification.

7. Results and Discussion

By deploying different numbers of sensors in a field with area size: 100×100 m, and a communication range with radius R = 20m in MATLAB we have implement the state of location verification and then applying the intrusion detection system to detect the hello flood attack. The system will produce a graphical representation of the nodes and their interactivity. Also, it will output the number of the nodes, malicious nodes, attack node and goal node(s).

Let's take an example of what is given in Fig. 5 we have deployed 50 sensors in the field where red circle illustrates true location and green circle illustrates the estimated location of sensors. Also, blue lines between nodes denote the communication availability. A line between two sensor nodes exists when they are in the same communication range of each other.

In addition, the system as mentioned earlier will produce results such as the nodes numbers, malicious nodes, attack node and goal node(s) as shown in Fig. 4.

We have calculated the detection rate, false positive rate and false negative rates of the location verification. Fig. 5 is the results of the detection rate DR and false alarm rate FR and false positive rates FP with different anomaly degree and number of sensor nodes respectively. From the figure, we have noticed that the DR is increased with the anomaly degree increased, and didn't affect with the number of nodes. It achieved in average a high detection rates value of 9.0643. Also, the FP is decreased whenever we increase the anomaly degree and achieved in average low FP of value 0.3263. In addition, the FN is increased with the anomaly degree increased and in average it is low with value of 0.1362.

Our algorithm presented good results and compared to other algorithms that used as solutions to detect the hello flood. Our algorithm successes in achieving low false positive and low false negative while in

Neighbour-based IDS [24] the false positive is low but the false negative is high with signal strength increased as shown in Table 1 compares our results with other produced results in other solution.

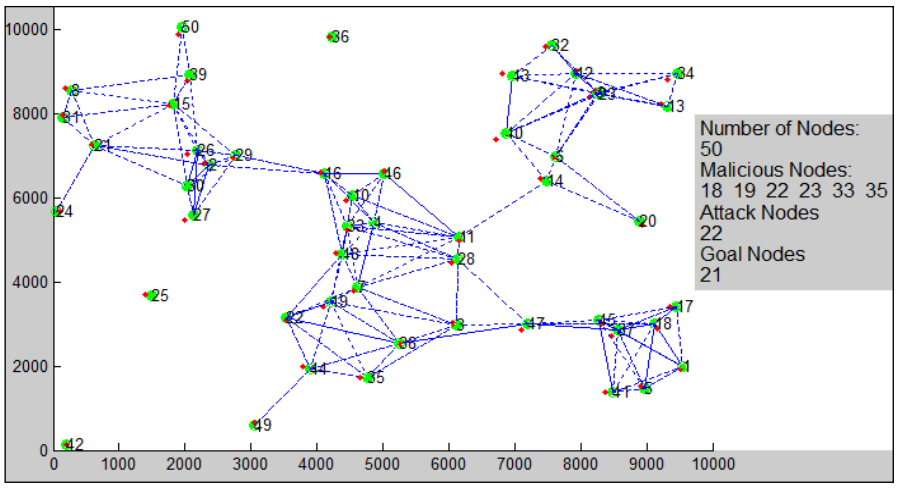
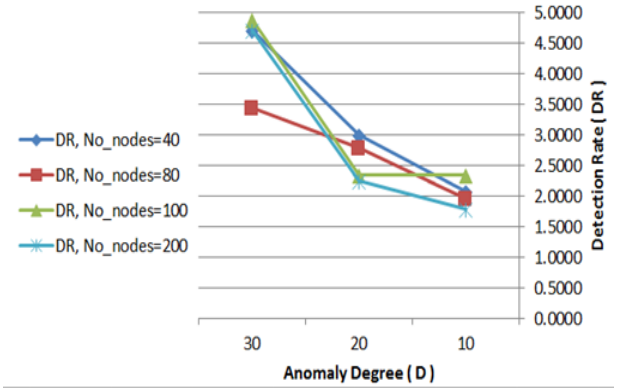
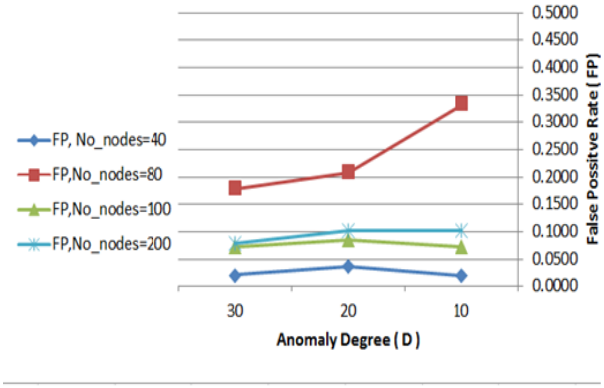


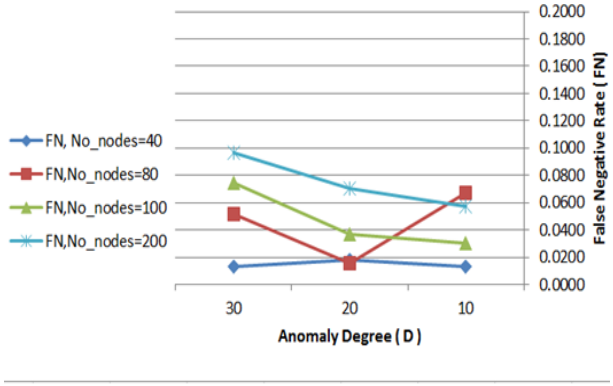
Fig. 4. Sensors filed in MATLAB with results 50 sensors with hello flood at sensor 22.



(a) Detection rate DR



(b) False positive rate (FP)



(c) False negative rate (FN)

Fig. 5. (a) Detection rate. (b) False alarm (positive). (c) False negative rates for hello flood detection using location verification.

Table 1. A Comparison between Our Location Verification Based IDS Algorithm and Neighbour-Based IDS Algorithm Presented in [24]

Algorithm	Average false positive	Average false negative	Criteria
Location verification based IDS	0.3263	0.1362	Anomaly degree
Neighbour-based IDS	0.28	3.76	Signal strength

8. Conclusion

WSNs are critical and widely used nowadays in a huge number of applications. One of the major factors that should be considered is its security due to its important role. There are number of security defence against the hello flood attack. However, there was no previous work that utilizes the location verification scheme for attacks detection. In this paper, we have implemented an intrusion detection system in MATLAB to detect the hello flood attacks on WSNs based on using the greedy filtering by matrix location verification scheme [1]. Our system has achieved high detection rate which in average 9.0643. The false positive rate is became lower and false negative rate is became higher with increasing the anomaly degree, but, both in general were low as required with average false positive rate 0.3263 and average false negative rate 0.1362.

9. Future Works

The algorithm presented in this paper is applicable to detect attacks that are somehow use the locations or communication range capabilities to be an intruder. Therefore, the algorithm could be modified to detect other type of attacks such that the locations and communication rages are used.

References

[1] Krishnan, M. (2006). Intrusion detection in wireless sensor networks. Project Paper, the University of California, Berkley.

[2] Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. *International Journal of Distributed Sensor Networks*.

[3] Abduvaliyev, A., Pathan, A. S. K., Zhou, J. Y., Roman, R., & Wong, W. C. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, *15(3)*.

[4] Wie, Y. W., & Guan, Y. (2013). Lightweight location verification algorithms for wireless sensor networks. *IEEE Trans. on Parallel and Distributed Systems*, *24(5)*.

[5] He, T., Huang, C., Blum, B., Stankovic, J., & Abdelzaher, T. (2003). Range-free localization schemes in large scale sensor network. *Proceedings of ACM MobiCom*.

[6] Moore, D., Leonard, J., Rus, D., & Teller, S. (2004). Robust distributed network localization with noisy range measurements. *Proceedings Second ACM Conf. Embedded Networked Sensor Systems*.

[7] Nagpal, R., Shrobe, H., & Bachrach, J. (2003). Organizing a global coordinate system from local information on an Ad-Hoc sensor network. *Proceedings of Second Int'l Conf. Information Processing in Sensor Networks*.

[8] Nicolescu, D., & Nath, B. (2001). Ad-Hoc positioning systems (APS). *Proceedings of IEEE GLOBECOM*.

[9] Niculescu, D., & Nath, B. (2003). Dv based positioning in Ad-Hoc networks. *J. Telecomm. Systems*, *22*, 267-280.

[10] Niculescu, D., & Nath, B. (2003). Ad-Hoc positioning system (APS) using AoA. *Proceedings of IEEE INFOCOM*.

[11] Want, R., Hopper, A., Falcao, V., & Gibbons, J. (1992). The active badge location system. *ACM Trans. Information Systems*, *10(1)*, 91-102.

[12] Du, W., Fang, L., & Ning, P. (2005). LAD: Localization anomaly detection for wireless sensor networks. *Proceedings of IEEE Int'l Paralleland Distributed Processing Symp*.

[13] Zeng, Y., Cao, J., Hong, J., Zhang, S., & Xie, L. (2010). Secure localization and location verification in wireless sensor networks: A survey. *J. Supercomputing*, 1-17.

[14] Liu, D., Peng, N., & Du, W. K. (2005). Attack-resistant location estimation in sensor networks. *Proceedings of Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05)*.

[15] Li, Z., Trappe, W., Zhang, Y., & Nath, B. (2005). Robust statistical methods for securing wireless localization in sensor networks. *Proceedings of Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05).*

[16] Wei, Y., Yu, Z., & Guan, Y. (2007). Location verification algorithms for wireless sensor networks. *Proceedings of Int'l Conf. Distributed Computing Systems (ICDCS)*.

[17] Talasila, M., Curtmola, R., & Borcea, C. (2010). LINK: Location-verification through immediate neighbors knowledge. Technical Report, Dept. of Computer Science, NJIT.

[18] Hu, Y., Perrig, A., & Johnson, D. (2003). Packet leashes: A defense against wormhole attacks in wireless Ad-Hoc networks. *Proceedings of IEEE INFOCOM*.

[19] Lazos, L., & Poovendran, R. (2004). SeRLoc: Secure range-independent localization for wireless sensor networks. *Proceedings of ACM Workshop Wireless Security (WiSe)*.

[20] Hamid, A., & Hong, S. (2006). Defense against lap-top class attacker in wireless sensor network. *Proceedings of ICACT.*

[21] Giruka, V. C., Singhal, M., Royalty, J., Varanasi, S. (2006). Security in wireless networks. *Wiley Inter Science*.

[22] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *IEEE*.

[23] J´unior, W. R. P., Figueiredo, T. H. de P., Wong, H. C., & Loureiro, A. A. F. (2004). Malicious node detection in wireless sensor networks. *IEEE*.

[24] Stetsko, A., Folkman, L., & Matyáš, V. (2010). Neighbor-based intrusion detection for wireless sensor networks. *Proceedings of 2010 6th International Conference on Wireless and Mobile Communications (ICWMC)* (pp. 420-425).

[25] Peng, B. C., & Liang, C. K. (2006). Prevention techniques for flooding attacks in Ad-Hoc networks. *IEEE*.

Rawan S. Hassoubah was born in Yanbu-Madinah at Kingdom of Saudi Arabia in 1987. She got her bachelor degree in computer information systems from Taibah University, Medina, Saudi Arabia in 2008. And recently received her MS degree in computer science from King Abdul Aziz University, Jeddah, Saudi Arabia. Her major fields of study are mobile computing, network security, Ad-Hoc and wireless networks.

She worked as an instructor at the Computer Science Department in YUC, Yanbu, Medina, Saudi Arabia till 2011. She also worked as an IT coordinator at the same time. Later, she worked as a teacher assistant at Effat University, Jeddah, Saudi Arabia till 2012.

Suhare M. Solaiman was born in Taif in Saudi Arabia on April 26, 1983. She is a MS student at King Abdul Aziz University, Jeddah, Saudi Arabia. The major field of her study is data mining.

She works as a teacher assistant at Taif university, Taif, Saudi Arabia.

Manal A. Abdullah received her PhD degree in computers and systems engineering, from Faculty of Engineering, Ain-Shams University, Cairo, Egypt, in 2002. She has experience in industrial computer networks and her research interests include computer networks, performance evaluation, WSN, network management, and BD management. Currently she is an assistant professor, at Faculty of Computing and Information Technology FCIT, King Abdulaziz University, KAU, Saudi Arabia.