Int. J. Nonlinear Anal. Appl. 13 (2022) No. 1, 305-320
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/IJNAA.2022.5491

A lightweight intrusion detection system based on RSSI for sybil attack detection in wireless sensor networks

Mahdi Sadeghizadeh[a]

[a] *Department of Computer Engineering, Quchan University of Technology, Quchan, Iran.*

(Communicated by Ehsan Kozegar)

Abstract

As the prevalence of Wireless Sensor Networks (WSNs) grows in the many mission-critical applications such as military and civil domains, the need for network security has become a critical concern. The inherently vulnerable characteristics of WSNs appoint them susceptible to various types of attacks. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack, where a node illegitimately claims multiple identities. Sybil attacks can severely deteriorate the network performance and compromise the security by disrupting many networking protocols. This paper presents a lightweight Intrusion detection system (IDS) based on received signal strength indicator (RSSI) readings of messages to protect WSNs against Sybil attack. Our idea in the proposed method is based on the local calculation (within each node and without the need for communications) the RSSI ratio from the suspected nodes to the Sybil attack. The obtained results demonstrate that Proposed System achieves high detection accuracy, low false alarm rate and low energy consumption appointing it a promising IDS candidate for wireless sensor networks.

Keywords: Wireless Sensor networks (WSNs), Sybil attack, Intrusion detection systems (IDS), Received signal strength indicator (RSSI)

1. Introduction

Wireless Sensor Networks because of their inherent advantages such as lower cost and easier deployment on the environment [1], to play a role in a wide range of applications such as military

*Corresponding author
Email address: m.sadeghizadeh@qiet.ac.ir (Mahdi Sadeghizadeh)

Received: September 2020 *Accepted:* September 2021

surveillance [4], fire control in forest, health care [9], safety monitoring on Structures and buildings, target tracking [14], and smart homes [12] are highly desirable and cost-effective. However, resource constrains, such as limited processing power, memory and energy are main challenge in WSN design and application, and subsequently address issues for researchers such as energy efficiency and extending network lifetime [15], enhancing reliability, effective routing [11].

Given that WSNs are often used in remote and unprotected locations or where adverse operating conditions or even hostile operating conditions, they are highly susceptible to intrusions and security attacks [13]. Most of attacks try to cause a sharp decline in network performance using this weakness.

In this work, we focus on the Sybil attack that is one of the common devastating attacks in WSNs and severely reducing network performance. In this attack, a single malicious node, in different illegal ways, forges multiple identifiers within a network in order to mislead the genuine nodes into believing that they have many. The main reason for the importance of this attack compared to other attacks is that Sybil attacks do not require specialized hardware and/or cooperation with other nodes in the network, yet they have the ability to create havoc to many network operations and protocols neighbors [19]. The most important network protocols that are disrupted by this attack are distributed storage, routing algorithm, voting operation, and fair resource allocation, and so on. For instance, as shown in Fig. 1, a malicious node generates multiple paths with the help of the Sybil identifiers and disrupts the operation of the routing protocol [16].

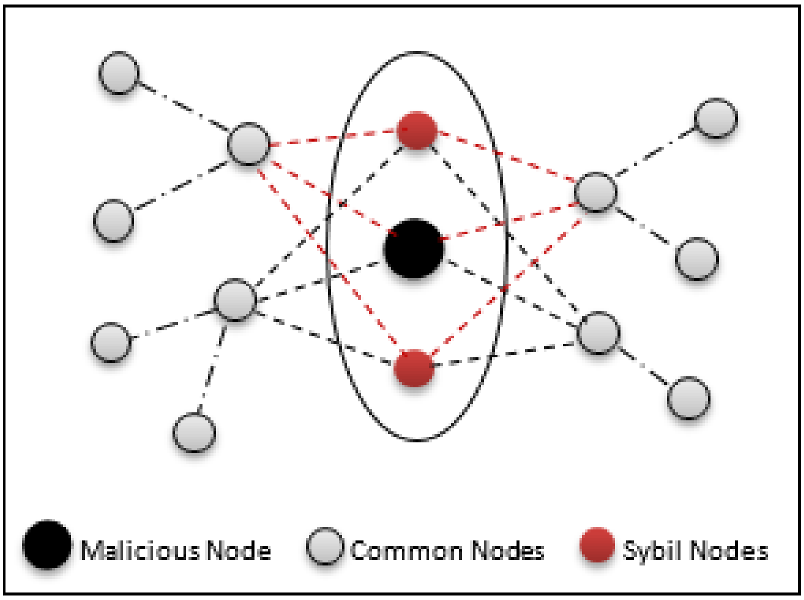


Figure 1: Sybil attack through several fake paths

In order to protect WSNs against destructive Sybil attacks, we must design an appropriate security mechanism. Given that in WSNs, sensor nodes are usually resource constrained in terms of computational and communication abilities, therefore, during the design of security systems for WSNs, the design guidelines should conform to the limited resources and capabilities of the sensor nodes [8].

Intrusion detection systems (IDSs) are one of the most effective ways to protect wireless sensor networks from Sybil attacks. By deploying IDS that is a set of tools, methods, and resources to help identify, assess, and report intrusions in these networks, we can keep the network efficiency at the optimum level by detecting timely Sybil attacks [17].

In this paper, a lightweight IDS based on the received signal strength indicator (RSSI) is proposed to protect the WSNs against a Sybil attack. In the proposed method, based on the behavior analysis of the Sybil attack and the presentation a series of related calculations, detection operations are carried out as much as possible locally and without communication, which results in a reduction of energy consumption in the network nodes. In addition to a significant energy saving of proposed method, its appropriate detection rate along with low false alarms rate, suggests this method as desirable IDS for WSNs.

The remainder of this paper is organized as follows: In Section 2, a review on the most important IDSs against of Sybil attack in WSNs is presented along with the introduction of their advantages and shortcomings. In Section 3, we propose an IDS against of Sybil attack, and in Section 4, the analysis and formulation of the detection rate and the false alarms rate of proposed IDS is presented. In Section 5, we will simulate the proposed IDS and present the related results. Finally, in Section 6, the paper ends with a conclusion and future works.

2. Related works

One of the important methods in detecting Sybil attacks in WSNs is the use of received signal strength indicator (RSSI), which has been used in several references [6, 10, 26, 7, 23], which we will examine in the following.

In [6] and [10] to detection of Sybil nodes, received signal strength indicator based algorithms (RSSI) in wireless sensor networks based on LEACH protocol are proposed. They have considered a model of Sybil attack in which the attacking node acts as a cluster head by relying on its Sybil nodes.

The authors in [26] have proposed an RSSI-based location scheme that determines the location of a new node based on the ratio of signal strength received from multiple nodes in the network. They argue based on a theory that if radio waves are monitored by at least four nodes in any area of the network, then any node cannot hide its location. Finally, by solving a series of complex equations, the location of nodes in the network is determined, and if the locations of different nodes are equal, they can be recognized as a Sybil attack. The main problems of the above method for detecting Sybil attack are heavy calculations to determine the location of nodes, the need for a large number of monitoring nodes with predetermined locations to cover the entire network, and also the high exchange of messages between monitoring nodes.

In reference [7], in order to elimination the heavy calculations of the above method, it has been noted that due to the fact that the location of the monitoring nodes in the network does not change, without determining the location of other nodes and only based on comparison of the received signal strength Indicator (RSSI) ratio for received messages, a Sybil attack can be detected.

In [24], a mechanism similar to the reference [7] is proposed, which operates based on the time difference of arrival messages (TDOA) between the attacking node and the monitoring node. This method requires at least three monitoring nodes, one of which is considered as the main monitoring node.

In [21] a method is proposed in which the identity of nodes in the network is detected based on the determination of their neighboring nodes. This method of detection is based on the fact that in a dense network, two different nodes cannot have the same set of neighbors. In a Sybil attack, because all cyber nodes are created by an attacking node, they will have the same neighborhood set. This feature of Sybil nodes can be used to detect of Sybil attack.

The authors in [2] have proposed a random password comparison algorithm (RPC) that focuses on different levels of traffic and security during data transmission in wireless sensor networks. This algorithm generates a routing table to store node location information. Intermediate nodes are also identified in the path between source and destination. During the communication between the nodes, the information of the intermediate nodes is compared with the RPC database and based on the comparison results, the algorithm decides whether the node is normal or Sybil.

In [22] a combination of Compare and match-position verification method (CAM-PVM) with Message Authentication and Passing (MAP) is proposed to identify, remove and finally prevent the entry of Sybil nodes in the network. In this method, in order to adapt the position, the nodes must be aware of the location, which practically requires heavy costs and calculations for the nodes. It also requires authentication by key verification via the base station node, which also requires high communication and memory.

Researchers in [3] have claimed to have developed a lightweight algorithm for detecting Sybil attacks for mobile wireless sensor networks. This algorithm performs its operations in two stages of configuration and testing. In the configuration phase, which takes place before the nodes are distributed in the environment, a unique identifier is assigned to each sensor node based on the mechanism presented in [5]. Then in each node a table to store random numbers related to each sink node and in each sink node a table to store random numbers related to normal nodes is provided. In the test phase, which is after the distribution of nodes in the network, based on the movement of nodes and communication with sink nodes, random numbers are generated by the relevant sink for them and stored in the relevant tables. Each node is then authenticated based on the random numbers generated, and through this, the Sybil nodes are also identified.

The authors in [20] have also claimed that they have provided a lightweight detection mechanism for Sybil attack. In order to reduce the computational complexity, they rely solely on the received signal strength Indicator (RSSI) and make their detection based on it. Their method is that first each cluster head by exchanging messages with nodes within its cluster forms a received RSSI table for them. Each cluster head then sends its information along with the corresponding RSSI table to the sink node. Next, the sink node, by examining the RSSI received from the cluster head and its related information, as well as the RSSI table of the cluster (based solely on the same RSSI in the cluster table), determines whether the cluster head or nodes within the cluster are Sybil.

In [18] a Rule-based Anomaly Detection System (RADS) is proposed in 4 stages, based on an ultra-wideband (UWB) ranging-based detection algorithm that operates in a distributed condition without the need for cooperation or information sharing between nodes. In the first phase, each node explores its neighbors by exchanging hello messages. In the second phase, each node creates a table using a series of local calculations to estimate the distance of neighbors. In the third phase, each node independently and based on the table produced in the previous phase, performs the operation of matching the distance between its neighbors and if the difference of each pair is less than the allowable limit, it recognizes them as Sybil nodes.

3. Proposed intrusion detection system

As we examined in Section 1, a Sybil attack in different ways invades a wireless sensor network; therefore, in order to detect a Sybil attack in its various executive manners, we must consider the specification that has the ability to distinguish the attacker's nodes. With this approach, the most important feature that the Intrusion Detection System can be introduced based on is that all nodes with different identifiers are in one place of the network; since they all are under the control of an attacker node with a unique hardware.

The proposed algorithm is designed in such a way that the remaining problems in [7] which increases the cost and energy dissipation, to minimizes. The main idea in the proposed method for detecting a Sybil attack is based on this principle that examines should be carried out as much as possible locally and within a node without communications, and if a node is suspected to Sybil attack, by sending a message to the cluster head, Make the final decision to it. In order to be able to do this, we first need to make calculations in such a way as to allow local operations on nodes. Suppose node i receives radio signal from node 0, then the RSSI is:

$$R_i = P_0.K/d_i^{\alpha} \qquad (1)$$

Where P_0 represents transmitter power, R_i is RSSI, K is constant, d_i is Euclidean distance, and α is distance-power gradient. So, According to equation (1), we have:

$$d_i^{\alpha} = P_0.K/R_i \qquad (2)$$

Now if the 2 nodes S_1 and S_2 with the sending powers of P_1 and P_2 have the same distance from node i, and d_i^k is the Euclidean distance of node k from node i, then we have:

$$\begin{aligned} &d_i^{S_1} = d_i^{S_2} && (3)\\ &P_1.K/R_i^{S_1} = P_2.K/R_i^{S_2} && (4)\\ &P_1/R_i^{S_1} = P_2/R_i^{S_2} && (5)\\ &R_i^{S_1}/R_i^{S_2} = P_1/P_2 && (6) \end{aligned}$$

Equation (6) shows that if two nodes S_1 and S_2 that are at the same distance from node i, with the sending powers of P_1 and P_2, send messages to it, then the RSSI ratio received from them in node i will be equal with the sending powers ratio of them.

Given that the attacker can send messages from Sybil nodes using different sending powers, we have considered the sending powers of P_1 and P_2 for two nodes S_1 and S_2. In order to determine if the two S_1 and S_2 nodes are in the same place as the sensor network, with assuming a two-dimensional space (one page), different states below will be examined.

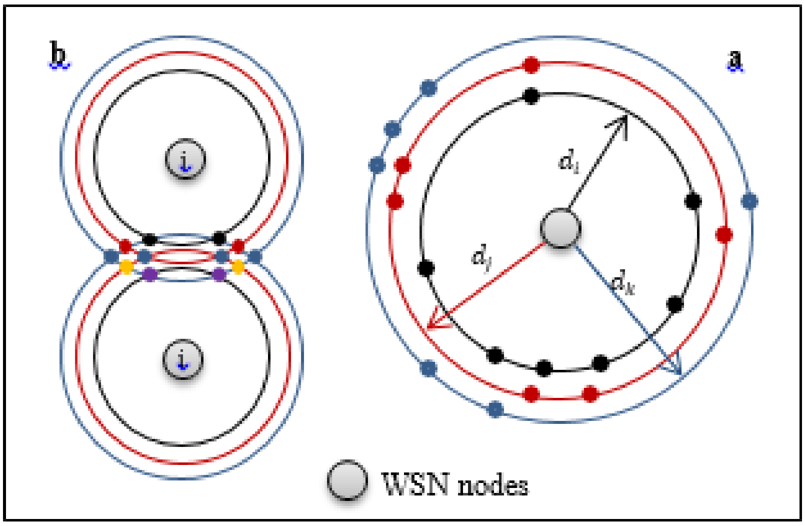


Figure 2: Points with the same distance from the network nodes

A) If only an observer node such as node i is considered, as shown in Fig. 2a, there are infinite points with the same distance and different locations from it, so that the probability of the same location of the nodes with the same distance will be very low.

B) If two nodes i and j as observers are considered, the pair of same color points in Fig. 2b are at the same distance from both observers but in different locations. Therefore, it is still impossible to conclude definitively that if their distance is the same then their location is also the same.

C) If we consider the three nodes i, j and f as observers, assuming that they are not on a straight line, then no pair of points can be found which have the same distance with three observers. Therefore, it can be conclusively said that if three different observers for the two nodes S_1 and S_2 report the same distance, they are definitely in one place of the network.

Given that the above conditions were checked for two-dimensional space, so in a 3D space, at least four observing nodes should report the same distance to determine the same location of the two nodes S1 and S2. That's mean, according to Fig. 3, it should be:

$$(d_i^{S_1} = d_i^{S_2})And(d_j^{S_1} = d_j^{S_2})And(d_f^{S_1} = d_f^{S_2})And(d_p^{S_1} = d_p^{S_2}) \tag{7}$$

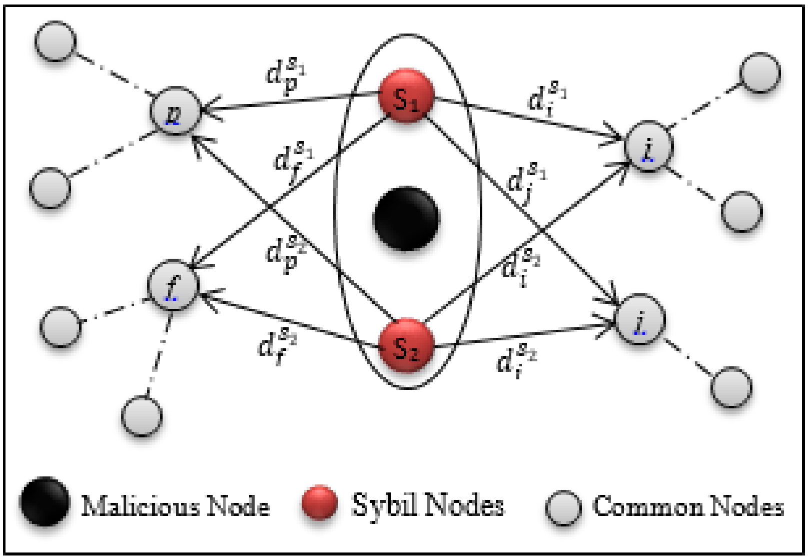


Figure 3: Distance between Sybil nodes of common nodes in network

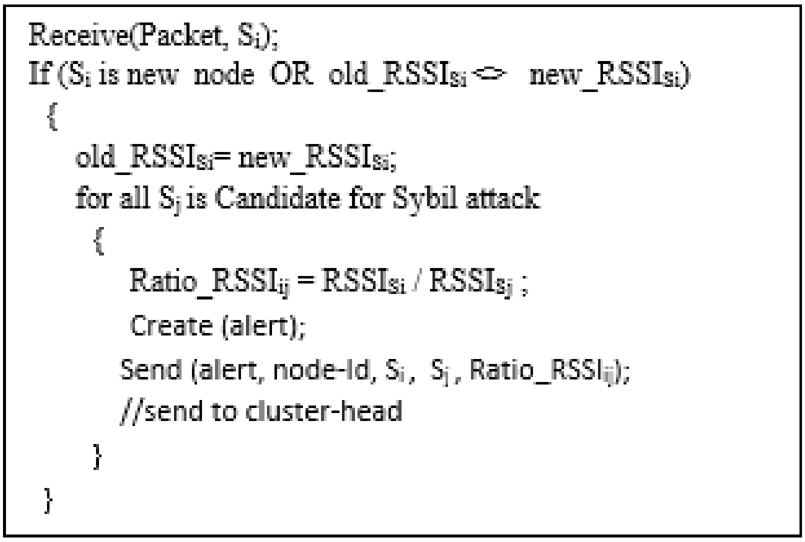
Finally, with respect to equations (6) and (7), we can say:

$$(\frac{R_i^{S_1}}{R_i^{S_2}} = \frac{P_1}{P_2})And(\frac{R_j^{S_1}}{R_j^{S_2}} = \frac{P_1}{P_2})And(\frac{R_f^{S_1}}{R_f^{S_2}} = \frac{P_1}{P_2})And(\frac{R_p^{S_1}}{R_p^{S_2}} = \frac{P_1}{P_2}) \tag{8}$$

Also, given that the right expression of all the equations is one thing, can write:

$$\frac{R_i^{S_1}}{R_i^{S_2}} = \frac{R_j^{S_1}}{R_j^{S_2}} = \frac{R_f^{S_1}}{R_f^{S_2}}\frac{R_p^{S_1}}{R_p^{S_2}} \tag{9}$$

Now, we can easily do the components of the equation (9) locally in each node, and then send each value to the CH node for the final check. For example, the left-hand side fractional expression in equation (9), which corresponds to Ratio of the Received Signal Strength Indicator (RSSI) in node i from the S_1 and S_2 nodes, is easily measurable without any additional connection with other nodes. Thus, in Fig. 4, the fractional expressions of equation (9) are locally computable in i, j, f, and p nodes respectively. Then, each of these nodes sends the values of the received RSSI ratio from the S_1 and S_2 nodes to the CH node.



```
Receive(Packet, $S_i$);
If ($S_i$ is new node OR old_RSSI$_{Si}$ <> new_RSSI$_{Si}$)
 {
   old_RSSI$_{Si}$= new_RSSI$_{Si}$;
   for all $S_j$ is Candidate for Sybil attack
     {
       Ratio_RSSI$_{ij}$ = RSSI$_{Si}$ / RSSI$_{Sj}$ ;
       Create (alert);
      Send (alert, node-Id, $S_i$ , $S_j$ , Ratio_RSSI$_{ij}$);
      //send to cluster-head
     }
 }
```

Figure 4: Sybil attack detection pseudo-code in common nodes

As shown in Fig. 5, in the pseudo-code of the cluster head operation to detect a Sybil attack, according to equation (9), sufficient to assign a counter to it that for each message received from a suspected node to the S_1 and S_2 nodes, add a unit to the counter if the value sent from suspected node is equal to the previous delivery value from another node. Finally, with respect to Equation (9), which must four nodes having equal ratios for the S_1 and S_2 nodes, if the counter receives more than 3 alerts, these nodes will be recognized as a Sybil attack and the CH update list of attackers and send to all nodes in the cluster.

Given the detection operation described above, it can be argued that the proposed algorithm for detecting a Sybil attack, based on simple local calculation and without any additional connection with other nodes, would have the least amount of energy consumed among the other algorithms. Also, the proposed algorithm performs its detection without the need for monitoring nodes in the network and only on the basis of local calculation in the common nodes of the network and therefore has a much lower cost than the existing algorithms.

4. Analysis and formulation of proposed method

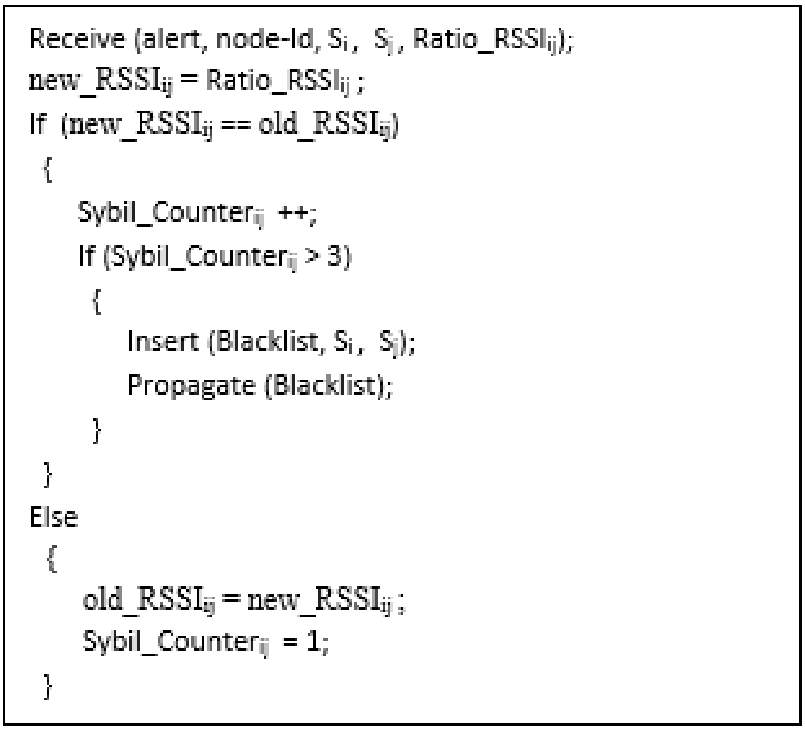
In order to formulate the detection rate in the proposed method, first, the geometric probability of the presence of a node to be within the communication range of node i must be determined.

According to Fig. 6, the geometric probability of the presence of a node within the neighborhood of the node i with the communication radius R is equal to:

$$\alpha = \frac{Area\ of\ favorable\ region}{Area\ of\ total\ region} = \frac{\pi R^2}{E}, \pi R^2 \leq E \tag{10}$$

With the aid of equation (10), the probability that node i has exactly x neighbors can be written in the form of equation (11), that has been determined based on probability density function (pdf) of a single node i with exactly x neighbors.

$$P^i(x) = Pr(X = x) = \binom{N-1}{x} \alpha^x (1-\alpha)^{N-x-1} \tag{11}$$



```
Receive (alert, node-Id, $S_i$, $S_j$, Ratio_RSSI$_{ij}$);
new_RSSI$_{ij}$ = Ratio_RSSI$_{ij}$ ;
If (new_RSSI$_{ij}$ == old_RSSI$_{ij}$)
 {
    Sybil_Counter$_{ij}$ ++;
    If (Sybil_Counter$_{ij}$ > 3)
     {
        Insert (Blacklist, $S_i$, $S_j$);
        Propagate (Blacklist);
     }
 }
Else
 {
    old_RSSI$_{ij}$ = new_RSSI$_{ij}$ ;
    Sybil_Counter$_{ij}$ = 1;
 }
```

Figure 5: Sybil attack detection pseudo-code in Cluster head

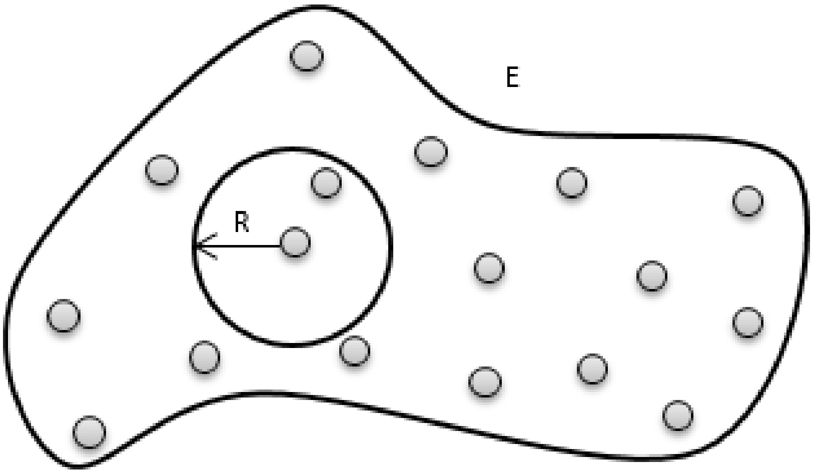


Figure 6: Wireless sensor network field

Where that $0 \le X \le N-1$ and N is the total number of nodes that have been uniformly distributed in a sensor network with area E.

As stated in the proposed algorithm, in order to detect the Sybil attack, a minimum of 3 neighboring nodes must create invasion alarm; therefore, in order to detect in node i, this node should have at least three neighbors, which its probability is presented in equation (12).

$$P^i = \sum_{x=3}^{N-1} P^i(x) \qquad (12)$$

Equation (12) actually specifies the probability of detecting a Sybil attack in a node of the network;

therefore, the probability of detecting a Sybil attack in the entire WSN with N nodes distributed in area E, it is obtained from equation (13).

$$P^{Detection} = (P^i)^N \qquad (13)$$

In the following, in order to formulate the false alarm rate, we need to consider situations in which the proposed intrusion detection method mistakenly identifies the normal state of the nodes as a Sybil attack.

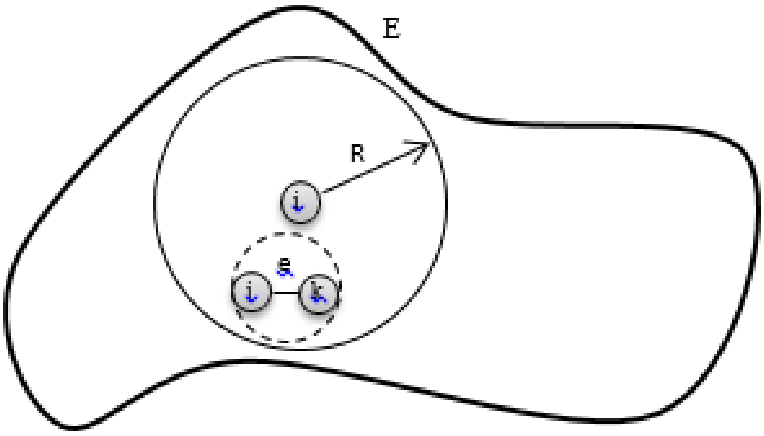


Figure 7: The distance between nodes in the wireless sensor network

As shown in Figure 7, this will happen when there are naturally two or more nodes in one place of the network. Of course, considering that the proposed algorithm estimates location of the Sybil nodes based on the received RSSI ratio, and due to the fact that its value changes under the influence of temperature, humidity, environmental conditions, and other factors, we must also consider a small amount of error.

$$if \begin{cases} d_{jk} < e, & then\ raise\ an\ alarm \\ d_{jk} \geq e, & else\ continue\ normal\ operation \end{cases} \qquad (14)$$

According to equation (14), if the distance between two nodes j and k, d_{jk}, is less than e, then the node i detects them in the same location based on the proposed algorithm and mistakenly identifies them as a Sybil attack. The parameter e here is the error value of the estimated distance by a sensor node.

To calculate the false alarm rate across the entire sensor network, we must calculate the probability that two or more nodes will be located at a distance less than e. In other words, the probability of having two nodes in a circle with radius $e/2$ must be calculated, that considering the geometric probability of the presence of a node in the neighborhood of the other node, we have:

$$\beta = \frac{Area\ of\ favorable\ region}{Area\ of\ total\ region} = \frac{\pi(e/2)^2}{E} \qquad (15)$$

With the aid of equation (15), the probability that node i has exactly x nodes at distance of e from itself is in accordance with equation (16) that has been determined based on probability density function (pdf) of a single node i with exactly x neighbors.

$$P^i(x) = Pr(X = x) = \binom{N-1}{x} \beta^x (1-\beta)^{N-x-1} \qquad (16)$$

Where that $0 \leq X \leq N - 1$ and N is the total number of nodes that have been uniformly distributed in a sensor network with area E.

With respect to equation (16), it is sufficient to calculate the probability that each node such as i in the sensor network has at least one node in less than equal distance e of itself.

$$P^i = \sum_{x=1}^{N-1} P^i(x) \qquad (17)$$

In fact, equation (17) specifies the false alarm probability in node i. therefore, the false alarm probability of detecting a Sybil attack in the entire WSN with N nodes distributed in area E, and the error value of the estimated distance e, it is obtained from equation (18).

$$P_{FalseAlarm} = 1 - (1 - P^i)^N \qquad (18)$$

In equation (18), the value of $(1 - P^i)$ is the true alarm probability at node i, and so, in order for in the entire WSN with N nodes, all nodes publish the true alarm, the value of $(1 - P^i)^N$ must be calculated. Finally, Equation (18) specifies the probability that at least one node in the network generates a false alarm, that is the same false alarm probability in the entire sensor network.

5. Simulation and results

This section first simulates WSNs and Sybil attacks. Then, the proposed IDS is simulated and the results are compared with the existing work.

5.1. Simulation of WSN and attacks

The evaluation of our IDS is performed using the network simulator NS2. The NS2 simulator is one of the most popular network simulators. The NS2 simulator is simply a discrete event simulation tool for studying the dynamic nature of communication networks and supports a wide range of protocols in all layers [25].

In this simulation, the basic network parameters are determined according to the nature of WSNs, existing requirements and the usual applications of these networks. In this scenario, our experimental model is built on a network containing 10-100 nodes in 2-5 clusters in an area of $100 * 100m^2$ with CBR traffic and packet size of 70 bytes. The simulation parameters used in our simulation model are summarized in the Table 1.

Given the fact that the Sybil attack is planned in various forms (we examined them in Section 1), We simulated it by relying on its main characteristic, that is common to all of its various forms. This main characteristic is the existence of multiple identities with the same location. So, in order to simulate it in NS2, we created several nodes with the same location in the network to indicates the Sybil attack on a wireless sensor network. Also, in terms of functionality (both for the facilities and for the traffic), we defined them the same as normal nodes. Table 2 presents the simulation parameters of the Sybil attack.

Table 1: Wireless sensor network simulation parameters

No	Parameters	Values
1	Number of nodes	10 / 20 / ... / 100
2	Size of network	$100 * 100m^2$
3	Routing protocol	AODV
4	MAC protocol	802.11
5	Type of traffic	CBR
6	Packet size	70 byte
7	Clustering method	Static / Dynamic (LEACH)
8	Number of Cluster	2 / 3 / 4 / 5
9	Queue Length	50
10	Type of nodes	Mica2
11	Sensing Power	0.015 w
12	Processing Power	0.024 w
13	Sleep Power	0.0001 w
14	RX Power	0.024 w
15	TX Power	0.036 w
16	Initial Energy of nodes	1 j
17	Antenna Model	Omni Antenna
18	Channel Type	Wireless Channel
19	Radio Propagation Model	Two Ray Ground
20	Interface Queue Type	Drop Tail
21	Antenna Range	30 m
22	Simulation Time	100 sec

Table 2: Attacks simulation parameters

No	Parameters	Values
1	Number of Sybil nodes	2 / 3 / 4
2	Type of nodes	Mica2
3	Initial Energy of nodes	10 j
4	Attacker location	Random / manual

5.2. Simulation of the proposed IDS

In order to evaluate the performances of the proposed IDS, the following criteria are considered:

Detection Rate (DR): The detection rate or the accuracy of detecting is the percentage of detected attacks relative to the total attacks.

$$DetectionRate = \frac{No.of\ Detected\ Attacks}{No.of\ Attacks} * 100\% \tag{19}$$

False Alarm Rate (FAR): This criterion shows an incorrect alarm rate in detecting attacks. In other words, it determines how much of the detected attacks was not attack, and the IDS mistakenly detected them.

$$FalsepositiveRate = \frac{No.of\ misdetected\ Attacks}{No.of\ Normal\ connections} * 100\% \tag{20}$$

Average energy consumption: This criterion shows the average energy consumption in network nodes.

$$Average\ energy\ Consumption = \frac{\sum_{i=1}^{nodes} Initial\ Energy_i - Residal\ Energy_i}{No.of\ nodes} \tag{21}$$

In Figures 8 and 9, the detection rate and the false alarm rate in detecting a Sybil attack are indicated as a function of the number of nodes. In this scenario, the network area is $E = 100*100m^2$, all nodes have the same communication range, $R = 30m$, and the average distance estimation error, $e = 30cm$ is considered. The number of nodes also changes from 10 to 100 nodes.

The most important finding in the curve of Figure 8 is that as the number of nodes increases, the false alarm rate also increases. The reason is the fact that by increasing the number of nodes, it is more likely that at least two nodes will be located at a distance less than average distance estimation error.

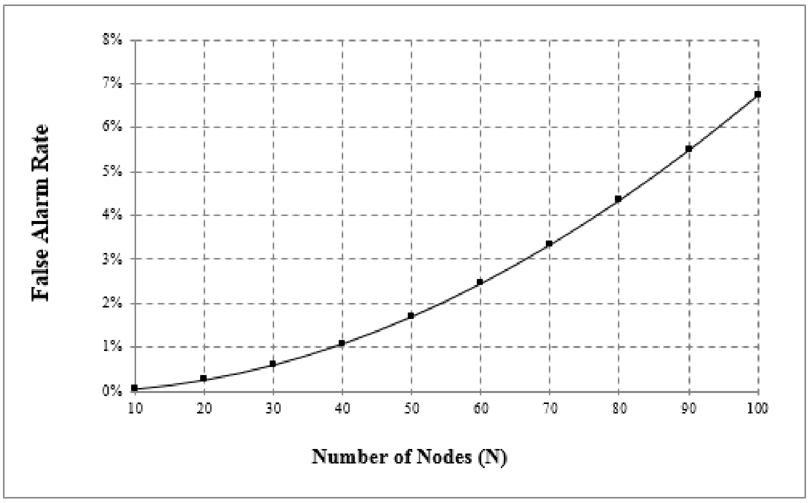


Figure 8: False alarm rate as a function of the number of nodes

Also, in the curve of Fig. 9, the detection rate is also increased by increasing the number of nodes in the sensor network. The reason for this is that with the increase in the number of nodes in the same deployment area, the number of neighboring nodes with a specific node increases, and subsequently the probability of detecting a Sybil attack also increases with increasing number of alarms generated.

Figure 10 shows the false alarm rate as a function of the distance estimation error e. In this scenario, the network area is $E = 100 * 100m^2$, all nodes have the same communication range, $R = 30m$, and the number of nodes in the network is $N = 50$. Also, the distance estimation error e is considered between $10cm$ to 60cm. As shown in the curve, with an increase in the distance estimation error, the false alarm rate also increases. The reason is that as the distance estimation error increases, the probability that the two nodes will be located at a distance less than that will increase, and consequently, the false alarm probability also will increase.

Figure 11 examines the effects of changing the deployment area of the sensor network on the false alarm rate of the proposed detection algorithm. In this scenario, the sensor deployment area changes from 4000 to 16000 m^2. All other parameters are also set with their default values (N=50; R=30 m, e=30 cm). As shown in the curve, the changes in the deployment area of the sensor network inversely correlate with the false alarm rate. In other words, by increasing the deployment area of the sensor

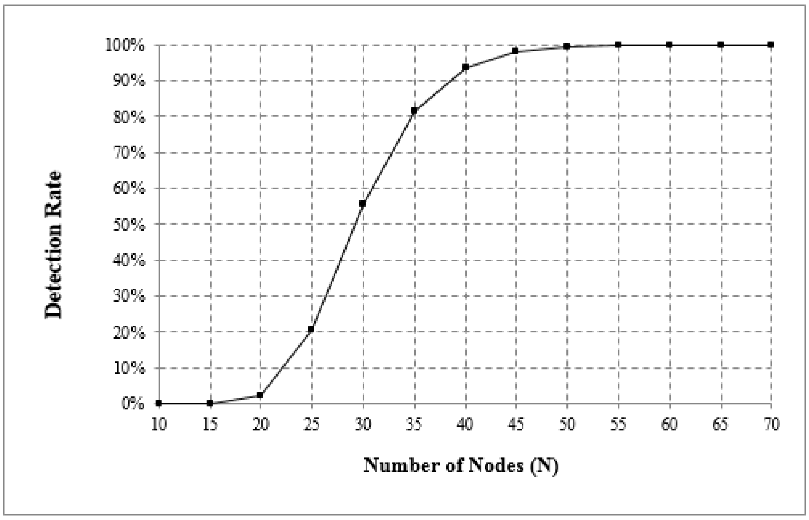


Figure 9: Detection rate as a function of the number of nodes

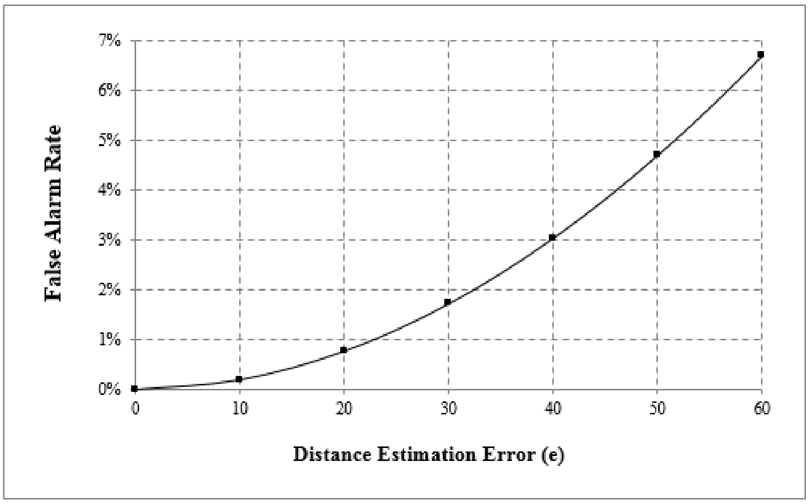


Figure 10: False alarm rate as a function of the distance estimation error e

network, the false alarm rate is reduced, which is due to the fact that in one larger deployment area of the network, the probability that the two nodes of the network will be located at a distance less than the average distance estimation error is reduced.

In the following, we will compare the proposed method with the existing works.

According to the results presented in Figures 12 to 14, the proposed system with a high detection rate of 99.44% and a low false alarm rate of 1.7%, as well as a low average energy consumption of 0.741 joules, is considered as an effective and lightweight method.

As can be seen in Figure 12, the reference methods [26] and [18] with a detection rate of 100% with a slight difference are better than the proposed method, but due to the false alarm rate of 6% in method [26] and Its high energy consumption, and also high false alarm rate of 11% in the method [18], the proposed system offers more favorable conditions. According to Figure 13, the false alarm rates in methods [10] and [5] are slightly better than the proposed method, but due to the low detection rates of 90% and 87% in them, the proposed system is more suitable.

In terms of energy consumption, according to Figure 14, the reference methods [5] and [20] are lighter than the proposed method, but due to the low detection rate of 87% of the method [5] and also

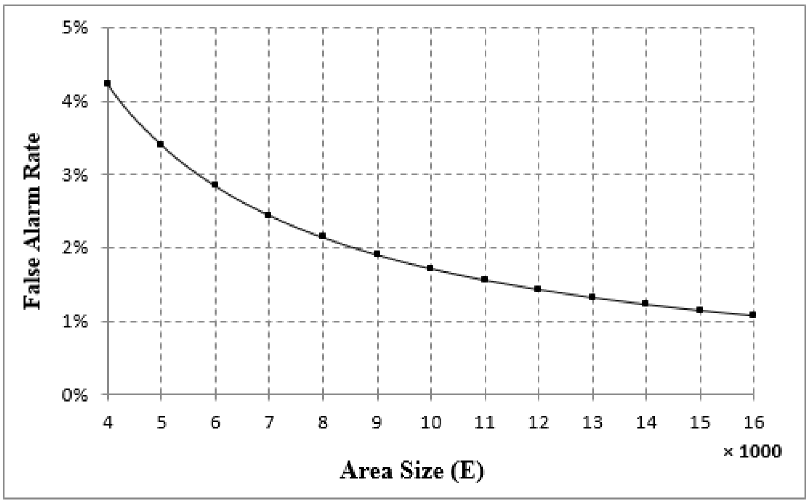


Figure 11: The false alarm rate as a function of changing the deployment area

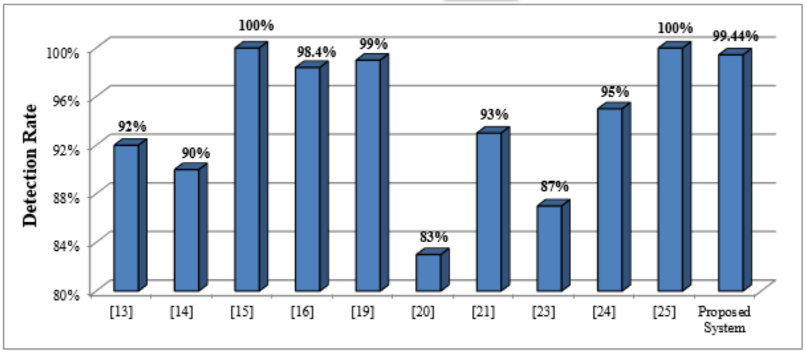


Figure 12: Detection rate of the proposed IDS compared to other references

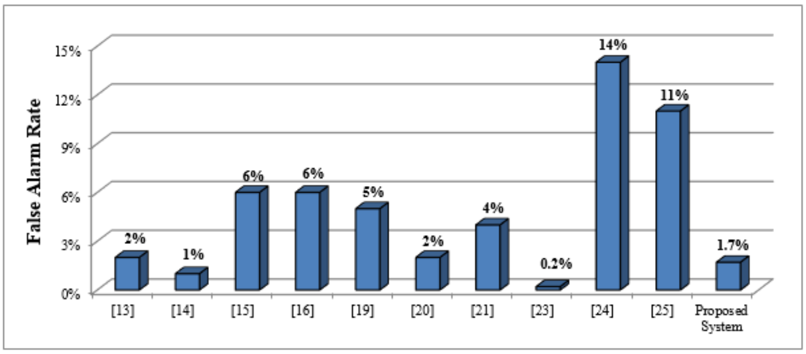


Figure 13: False Alarm rate of the proposed IDS compared to other references

the detection rate of 95% in the method [20] and a very high false alarm rate of 14%, the proposed system offers more favorable conditions.

6. Conclusion

In this paper, we proposed a lightweight intrusion detection system based on received signal strength indicator (RSSI) to detect Sybil attack according to its characteristics. The main idea of the proposed method is based on the local calculation (inside each node without the need for

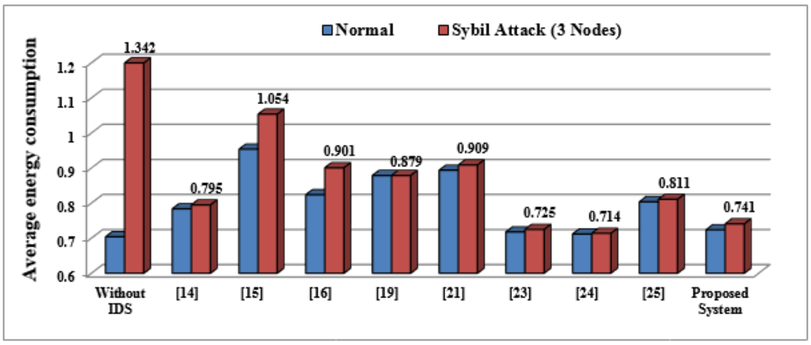


Figure 14: Average energy consumption of the proposed IDS compared to other references

communication) of the signal strength ratio received from the nodes suspected of Sybil attack, which is fully described in Section 3.

The results of simulation of the proposed intrusion detection system and comparison with the existing works presented in Figures 12 to 14, indicate that the proposed system with a high detection rate of 99.44%, and a slight false alarm rate of 1.7 %, and also (due to light calculations and low communication for detection) a low average energy consumption of 0.741 joules, is in a more favorable condition compared to the existing works. In general, according to the above, the proposed method is a lightweight and efficient method for detecting Sybil attacks.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, *A survey on sensor networks*, in IEEE Communications Magazine, 40 (8) (2020) 102-114.

[2] R. Amuthavalli and R. S. Bhuvaneswaran, *Detection and prevention of sybil attack in wireless sensor network employing random password comparison method*, Journal of Theoretical and Applied Information Technologygy, 67 (1)(2013) 236–246.

[3] A. Andalib, M. Jamshidi, F. Andalib and D. Momeni, *A Lightweight Algorithm for Detecting Sybil Attack in Mobile Wireless Sensor Networks using Sink Nodes*, International Journal of Computer Applications Technology and Research, 5 (7) (2016) 433-438.

[4] M. G. Ball, B. Qela and S. Wesolkowski, *A Review of the Use of Computational Intelligence in the Design of Military Surveillance Networks*, in Recent Advances in Computational Intelligence in Defense and Security, 621 (2015) 663-693.

[5] K. Butler, S. Ryu, P. Traynor and P. D. McDaniel, *Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems*, IEEE transaction on parallel and distributed systems, 20 (12) (2009) 1803-1815.

[6] S. Chen, G. Yang and S. Chen, *A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks*, in: Proc. of the International Conference on Communications and Mobile Computing, China, (2010) 142-146.

[7] M. Demirbas and Y. Song, *An RSSI-based scheme for Sybil attack detection in wireless sensor networks*, In: Proc. of the IEEE Computer Society International Symposium on World of Wireless, Mobile and Multimedia Networks, (2006) 570–574.

[8] A. Ghosal and S. Halder, *A survey on energy efficient intrusion detection in wireless sensor networks*, in Journal of Ambient Intelligence and Smart Environments, 9 (2) (2017) 239-261.

[9] D. He, N. Kumar, J. Chen, C. C. Lee and N. Chilamkurti, *Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks*, in Multimedia Systems, 21 (1) (2015) 49–60.

[10] A. Jangra and S. Priyanka, *Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS)*, in: Proc. of the International Conferences on Advances in ICT for Emerging Regions, (2011).

[11] A. Jiang and L. Zheng, *An Effective Hybrid Routing Algorithm in WSN: Ant Colony Optimization in combination with Hop Count Minimization*, Sensors, 18 (4) (2018) 1020.

[12] M. Li and H. J. Lin, *Design and Implementation of Smart Home Control Systems Based on Wireless Sensor Networks and Power Line Communications*, in IEEE Transactions on Industrial Electronics, 62 (7)(2015) 4430–4442.

[13] M. A. Moulavi, J. Nasiri, B. Bahmani, H. Parvar, M. Sadeghizadeh and M. Naghibzadeh, *DHA-KD: Dynamic Hierarchical Agent Based Key Distribution in Group Communication*, 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, (2008) 301-306.

[14] C. Pang, G. Xu, G. Shan and Y. Zhang, *A new energy efficient management approach for wireless sensor networks in target tracking*, in Defence Technology, 17 (3) (2021) 932-947.

[15] A. Rodríguez, C. Del-Valle-Soto and R. Velázquez, *Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks Based on Yellow Saddle Goatfish Algorithm*, Mathematics, 8 (9) (2020) 1515.

[16] M. Sadeghizadeh and O. R. Marouzi, *A Lightweight Intrusion Detection System Based on Specifications to Improve Security in Wireless Sensor Networks*, in Journal of Communication Engineering, 7 (2) (2018).

[17] M. Sadeghizadeh and O. R. Marouzi, *Securing Cluster-heads in Wireless Sensor Networks by a Hybrid Intrusion Detection System Based on Data Mining*, in Journal of Communication Engineering, 8 (1) (2019).

[18] P. Sarigiannidis, E. Karapistoli and A. A. Economides, *Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information*, Elsevier, Expert Systems with Applications, 42 (21) (2015) 7560-7572.

[19] P. Sarigiannidis, E. Karapistoli and A. A. Economides, *Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information*, Elsevier, Expert Systems with Applications, 42 (21)(2015) 7560-7572.

[20] W. Shi, S. Liu and Z. Zhang, *A Lightweight Detection Mechanism against Sybil Attack in Wireless Sensor Network*, KSII Transactions of Internet ad Information Systems 9 (9) (2015) 3738-3750.

[21] K. F. Ssu, W. T. Wang and W. C. Chang, *Detecting Sybil attacks in wireless Sensor Networks using neighboring information*, in: Proc. of the Computer Networks 53 (2009) 3042–3056.

[22] U. Suriya and R. Vayanaperumal, *Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method*, The Scientific World Journal, 2015(2015) 1-7.

[23] C. Wang, L. Zhu, L. Gong, Z. Zhao, L. Yang, Z. Liu and X. Cheng, *Accurate Sybil Attack Detection Based on Fine-Grained Physical Channel Information*, Sensors, 18 (3)(2018) 878.

[24] M. Wen, H. Li, Y.F. Zheng and K.F. Chen, *TDOA-Based Sybil Attack Detection Scheme for Wireless Sensor Networks*, Journal of Shanghai University (English Edition), 12 (1)(2008) 66-70.

[25] K. K. Waraich and B. Singh, *Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Adhoc Networks*, in International Journal of Advanced Science and Technology, 82 (2015) 63-70.

[26] S. Zhong, et Y. G. Liu and Y.R. Yong, *Privacy-preserving location based services for mobile users in Wireless Networks*, In: Proc. of the Technical Report, Yale Computer Science, (2004).