International Journal of Grid Distribution Computing
Vol.7, No.5 (2014), pp.15-30
http://dx.doi.org/10.14257/ijgdc.2014.7.5.02

Sybil Attack Detection and Analysis of Energy Consumption in Cluster Based Sensor Networks

Sweety Saxena[1] and Prof. Vikas Sejwar[2]

Department of CSE/IT
Madhav Institute of Technology and Science, Gwalior, M. P, India
er.s.royal@gmail.com[1], vikassejwar@gmail.com[2]

Abstract

Wireless Sensor Network is an emerging new technology extensively used for large-scale real-time data processing due to its characteristics and is used in application areas such as in civilian and military domains. These networks are vulnerable to several security attacks. In this paper, we emphasize on Sybil attack, which is a harmful threat to sensor networks and proposed an algorithm for Sybil attack detection based on Time difference of Arrival (TDOA) localization method, which detects the malicious behavior of the head node and member nodes in a cluster based network.

Keywords- *Localization algorithm, TDOA, RSSI, Sybil attack, LEACH*

1. Introduction

In the present scenario, wireless sensor networks are a promising new technology to allow economically possible solutions to a range of applications, for example structural integrity monitoring, pollution sensing and traffic monitoring. Sensors incorporated into machines, structures, and the environment, capable of delivering the sensed information; provide great benefits to the society. Potential benefits include: less catastrophic failures, improved manufacturing productivity, conservation of natural resources, improved emergency response, and enhanced homeland security [1]. A large number of sensor network applications require security, especially if the sensor network protects or monitors critical infrastructures.

Security is the major concern in these networks. Design and nature of WSNs makes them vulnerable to security attacks. Wormhole, Sinkhole, Sybil, Jamming and selective forwarding are the attacks which cause threat to the functioning of the network. Focusing on one of the issues of these networks, *i.e.*, security, this paper aims at proposing an algorithm to detect Sybil attack which is one of the particularly harmful attacks for WSNs.

In this paper, we simulated Sybil attack in WSNs and evaluated its damage in the network. We have considered a cluster based network and proposed an algorithm to detect the Sybil identities of the head node and member nodes of the cluster based WSNs. We make use of Localization algorithm in our work. Time Difference of Arrival is one of most efficient localization algorithms, which is used for estimating the node as malicious. Detection Rate and false positive rate is calculated and then energy consumption of each node before and after attack is calculated.

Energy consumption is also one of the main issues in WSN since the sensor motes have the limited battery because of the size of the sensors. Hence an energy minimization algorithm is suggested for reducing the variation between the energy differences obtained during the simulation.

ISSN: 2005-4262 IJGDC

The rest of the paper is organized as follows. Section 2 gives the Overview of WSN, including its issues and Applications. Section 3 describes the security attacks in WSN. Section 4 includes the Routing Protocols used in WSN. Localization techniques are presented in section 5.The basic algorithm is presented in section 6. Simulation results are described in section 7. Finally concluding remarks are made in Section 8.

2. Wireless Sensor Network

Wireless Sensor Network (WSN) is the one that has emerged as a recent application obtained from the combination of wireless Communications and embedded computing technologies. These are the network which consists of mobile nodes; those have self-organizing and self-managing capabilities [2]. Nodes join or leave the network at any instant of time, as a result of which topology changes frequently. As nodes have limited communication range, they use multi-hop transmission to communicate within the network. Sensor nodes have limited storage and computational resource.WSN is used in some time critical applications like fire detection, nuclear reactor control, military applications for area monitoring and traffic monitoring, *etc*.

Wireless sensor networks consist of a large number of small nodes that are used to measure some physical or environmental aspect of the hostile environment such as temperature, sound, vibration or motion. These nodes are resource-constrained units that communicate via a wireless medium and forward sensed data to the gateway node. The gateway node, so called base station, is the only connection with the other world apart from the network itself.

Wireless sensor networks act as a bridge between the physical world and the computer system by providing measurements of physical properties of the real world. Although wireless sensor networks were originally designed for the purpose of military application, nowadays their field of application is much wider and they are being used in civilian and industrial areas as well.

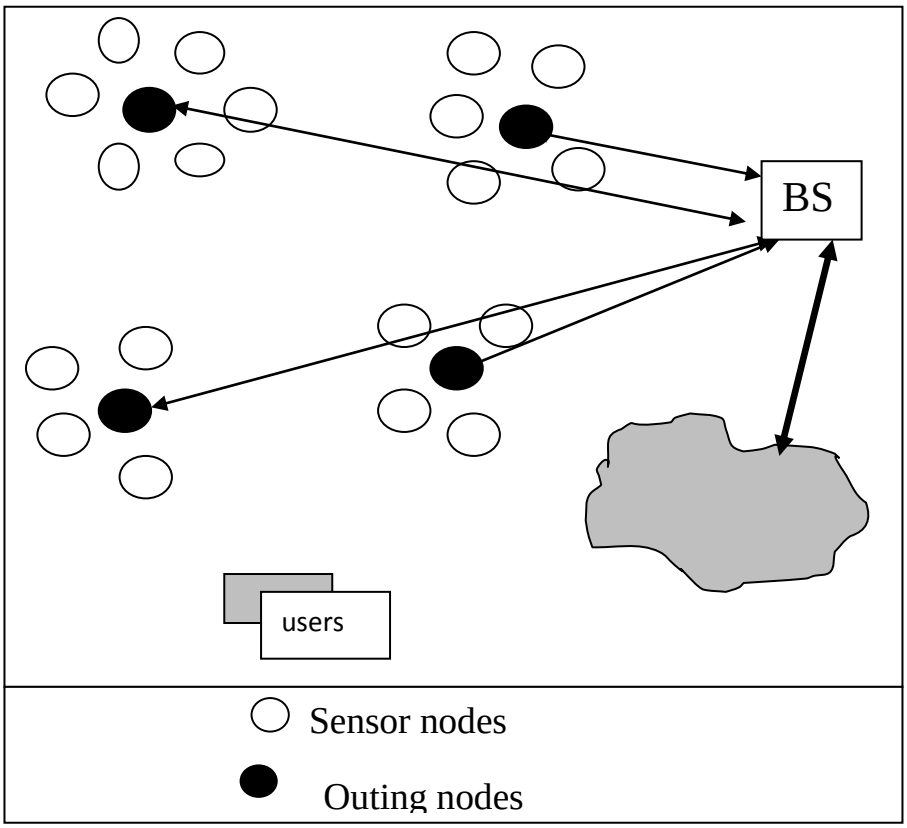


Figure 1. Wireless Sensor Network Architecture

2.1 Issues of Wireless Sensor Networks

Although WSNs evolved from wireless adhoc networks, there exist some important differences between them, which greatly affect the system designs including security designs. The system design is also affected by most of the issues .Some of the issues is as follows [8]:

1. Energy efficiency – In Wireless sensor networks, nodes have limited battery size and these nodes use battery for various functions like sensing, computation and communication purpose. Hence energy is one of the important issues that are to be considered while designing the sensor networks.
2. Size of the network – The number of nodes in the sensor network can be much larger than that in a typical adhoc wireless network.
3. Density of Deployment – The density of nodes in the sensor network varies with the domain of application .For example, military applications require high availability of the network, making redundancy a high priority.
4. Data/Information fusion – The limited bandwidth and power constraints demand aggregation of bits and information at the intermediate relay nodes that are responsible for relaying. Data fusion refers to the aggregation of multiple packets into one before relaying it. This mainly aims at reducing the bandwidth consumed by redundant headers of the packets and reducing the media access delay involved in transmitting multiple packets. Information fusion aims at processing the sensed data at the intermediate nodes and relaying the outcome to the monitor node.
5. Traffic Distribution – The communication traffic pattern varies with the domain of

application in sensor networks.

2.2 Applications of Wireless Sensor Networks

The applications can be categorized into three main classes: environmental data collection, security monitoring, and sensor node tracking [17].

2.1.1 Environmental Data Collection

An environmental data collection application is the one where a sensor reading is collected from a set of points in an environment over a period of time in order to detect trends and interdependencies. The data is collected from hundreds of points spread throughout the area and then the data is analyzed. For the data to be meaningful it would have to be collected at regular intervals and the nodes would remain at known locations. At the network level, the environmental data collection application is characterized by having a large number of nodes continually sensing and transmitting data back to a set of base stations that store the data using traditional methods. These networks generally require very low data rates and extremely long lifetimes.

2.1.2 Security Monitoring

Security monitoring is the second class of sensor network application. These networks are composed of nodes that are placed at fixed locations throughout an environment that continuously monitor one or more sensors to detect an anomaly. A main difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a major impact on the optimal network architecture. Each node has to regularly check the status of its sensors but it only has to transmit a data report when there is a security violation. The instant and trustworthy communication of alarm messages is the primary system requirement. Additionally, it is necessary that it is confirmed that each node is still present and functioning. If a node were to be disabled or fail, it would represent a security violation that should be reported. For security monitoring applications, the network is configured so that nodes are responsible for confirming the status of each other. One technique is to have each node be assigned to peer that will report if a node is not functioning.

2.1.3 Node Tracking Scenarios

A third usage, commonly discussed for sensor networks is the tracking of a tagged object through a region of space monitored by a sensor network. There exist several situations where one would like to track the location of valuable assets or personnel. Current inventory control systems try to track objects by recording the last checkpoint that an object passed through. Though, with these systems it is not possible to determine the current location of an object. For example, every shipment is tracked by UPS, scanning it with a barcode whenever it passes through a routing center. When objects do not flow from checkpoint to checkpoint, the system breaks down. With wireless sensor networks, objects are tracked by simply tagging them with a small sensor node. The sensor node is tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations.

3. Security Attacks in Wireless Sensor Networks

Although WSNs evolved from wireless adhoc networks, there exist some important differences between them, which greatly affect the system designs including security designs. The differences are [7]:

- Sensor nodes are limited in memory, power resources, computation and bandwidth.
- The topology of these networks changes frequently due to node failure, joining or mobility.
- Sensor nodes are deployed densely.
- The total number of nodes in WSNs is higher in magnitude than adhoc networks.
- Sensor nodes are easily compromised.

Due to these differences, security in WSNs is more complicated. WSN is vulnerable to several types of security attacks. Attacks such as wormhole, sinkhole, black hole, Sybil and selective flooding are possible, but Sybil attack is one of the particularly harmful attacks for WSNs.

3.1 Wormhole Attack

Wormhole attack [21] is an attack in which the malicious node records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of packets can be done selectively. Wormhole attack is a major threat to wireless sensor networks, because this kind of attack does not require compromising a sensor in the network rather, it might be performed even at the initial phase when the nodes start to discover the neighboring information. Figure 2 (a and b) shows a wormhole attack situation. When a node B (for example, the base station or any other sensor) broadcasts a route request packet, the malicious node receives this packet and replays it in its neighbor. Each neighbor node receives the replayed packet and considers itself to be in the range of Node B, and will treat this node as its parent. Hence, even if the legitimate nodes are multihop away from B, attacker will convince them that B is only a single hop away from them and thus create a wormhole.

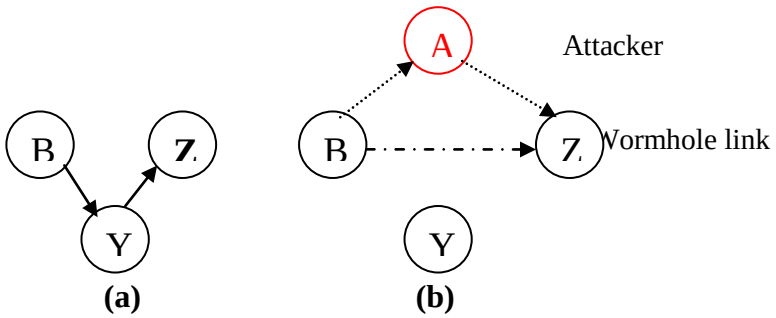


Figure 2. A Wireless Sensor Network Structure

3.2 Black Hole Attack

In this attack, a malicious node acts as a black hole [21] and receives all the traffic in the sensor network. Specially in a flooding based protocol, the attacker listens to the route request, then replies to the target nodes that it contains the shortest path to the base station. Once the malicious device is able to introduce itself between the communicating nodes (for

example, sink and sensor node), it can do anything with the packets passing among them. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure shows the conceptual view of a black hole/sinkhole attack.

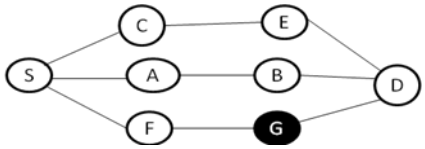


Figure 3. A Wireless Sensor Network Structure

3.3 Node Replication Attack

In this attack, an attacker first physically captures only one or few of the legitimate nodes, then replicates or clones the nodes fabricating those replicas having the same identity (ID) with the captured node, and finally deploys a unpredictable number of clones throughout the network. The clones or replicas are selectively reprogrammed to threaten the network by launching further insider attacks like falsifying sensor data or extracting data from the network, suppressing legitimate data, and disconnect the network by triggering correct execution of node revocation protocols that rely on threshold voting schemes and staging denial of service (DoS) attacks. Clone nodes may initiate a wormhole attack with a collaborating adversary, create a black hole, or may also leak data in an environment in which sensed data must be kept private [21]. If these replicated nodes or clones remain undetected or unattended for a long time, they can further initiate the changes in protocol behavior and intrusion into the systems security.

3.4 Sybil Attack

Douceur [2] first introduced the Sybil attack problem in the peer-to-peer distributed systems. According to Douceur, the Sybil attack is an attack in which a single entity can control a substantial fraction of the system by presenting multiple identities (Figure 4). In the Sybil attack, a node illegitimately claims various identities. A malicious node behaves as if it is a large number of nodes, for example by impersonating legitimate nodes or simply by claiming false identities. In the worst case, an attacker may create a random number of additional node identities, using one physical device. The Sybil attack is a particularly harmful threat to sensor networks. If a single malicious node is able to convince its neighbors by presenting several identities, it will have control over the large portion of the network and can adversely affect the functioning of the network.

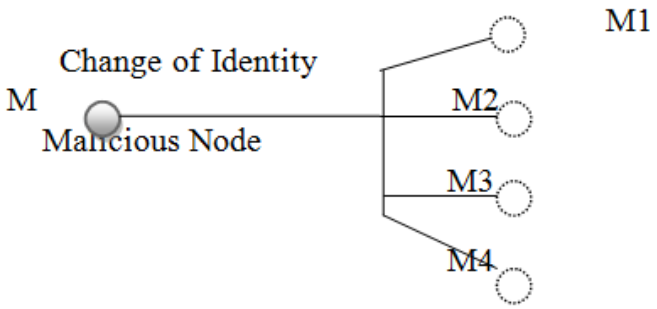


Figure 4. A Wireless Sensor Network Structure

Newsome, *et al.*, [1] established a classification of different types of Sybil Attacks:

3.4.1. Data Aggregation- A single Sybil node with multiple fake identities can participate in the aggregation process many number of times and can affect the result of the data aggregation[14].

3.4.2. Fair Resource Allocation- Some network resources may be allocated for each node. For example, neighbor nodes sharing a single radio channel might each be assigned a fraction of time per interval during which they are permitted to transmit. In this case a malicious node can have a larger share of resource by presenting multiple identities. This both denies service to legitimate nodes by reducing their share of the resource, and provides the attacker more resources to perform other attacks [5].

3.4.3. Voting- WSN could use voting for a number of tasks. The Sybil node is capable of changing the result of a voting scheme. For example, in a vote based intrusion detection system, a malicious node with various Sybil identities can expel a legitimate node from the network by voting against this node. Also, to win the trust of the legitimate nodes in the network, a Sybil attacker can acquire advantage of its multiple Sybil nodes that will vote in its favor [6].

3.4.4. Distributed Storage- Douceur observes that the Sybil attack can defeat replication and fragmentation mechanisms in peer-to-peer storage systems [1]. The similar problem exists for distributed storage in wireless sensor networks. Suppose the system may be designed to replicate or fragment data across several nodes, it could in reality be storing data on Sybil identities generated by the same malicious node.

3.4.5. Routing- Sybil attacks can affect the functioning of certain routing protocols such as geographic based routing protocols and multi-path routing protocols. In geographic routings, the nodes exchange their location information with their neighbors, to route the packets in an efficient manner. Here, a single malicious node can present various identities with different fake coordinate positions. Thus the legitimate nodes will have false routing information in their tables and will lead to disruption in the routing process. In multipath routing protocol, if the Sybil attacker has presented several Sybil identities among the legitimate nodes, then for the sender nodes which is legitimate it may appear that the route request packets are being forwarded through different paths, whereas they are being actually passed through a single malicious node [6]. There are different types of routing protocols in WSN that comes under the category of proactive, reactive and hybrid, on the basis of their functioning mode and the type of the application they target. Some of these protocols are LEACH, TEEN, APTEEN [9], *etc.*

4. Routing Protocols for WSNs

Routing techniques are essential for communication between sensor nodes and the base stations. Several routing protocols are proposed for wireless sensor network. These protocols are categorized on the basis of different parameters. Protocols are classified as proactive, reactive and hybrid, on the basis of their mode of functioning and type of applications they target. In case of proactive protocols the nodes switch on their sensors and transmitters, sense the environment and send the data to a BS by the predefined route. The Low Energy Adaptive Clustering hierarchy protocol (LEACH) comes under this type of protocol [9]. In reactive protocols, if there are sudden changes in the sensed attribute beyond some pre-determined threshold value, the nodes reacts immediately. This type of protocol is used in time critical applications. The Threshold sensitive Energy Efficient sensor Network (TEEN) is an example of a reactive routing protocol. Hybrid protocols like Adaptive Periodic TEEN (APTEEN)

include the characteristics of both proactive and reactive protocols. They compute all routes first and then improve the routes at the time of routing.

LEACH (Low Energy Adaptive Clustering Hierarchy)

We have used LEACH routing protocol in our algorithm, because it is one of the most efficient routing algorithm for wireless sensor network. It is an adaptive, self-organizing clustering protocol. Randomization is used for distributing the energy load among the sensor nodes in the network. According to this protocol, the base station is at fixed place and is located far from the sensor nodes and the nodes in the network are energy constrained and homogeneous. In the network, one node called cluster-head (CH) is present which acts as the local base station [9]. LEACH randomly elects the high-energy cluster-head in the network so that the activities are evenly shared among the sensors and the sensors consume uniform battery power. LEACH also performs data fusion, when data is sent from the clusters to the base station it is compressed thus reducing energy dissipation and enhancing lifetime of the system. LEACH divides the total process into rounds—each round consisting of two phases: set-up phase and steady phase.

In the set-up phase, clusters of sensor nodes are formed and for each cluster, one CH is selected from the sensor nodes at a time with a certain probability. Each sensor node generates a random number between 0 to 1. If this number is lower than the threshold node T (n) then this particular node becomes a CH. T(n) is given by:

$$T(n) = \frac{p}{1-p}[r \bmod (1/p)], \; n \in G = 0, \text{otherwise}$$

Here p gives the percentage of nodes that are CHs, r is the existing round and G is the set of nodes that have not acted as a cluster head in the last 1/p rounds. Then the CH allocates time slots to nodes in its cluster. Clustering through LEACH is shown in Figure 5.

In steady state phase, nodes send data to their CH during their allocated time slot by means of TDMA. When the cluster head receives data from its cluster, the data is aggregated by the cluster head and then, the data compressed is send to the BS. High energy is needed for transmitting the data, since the BS is far-off from the CH.

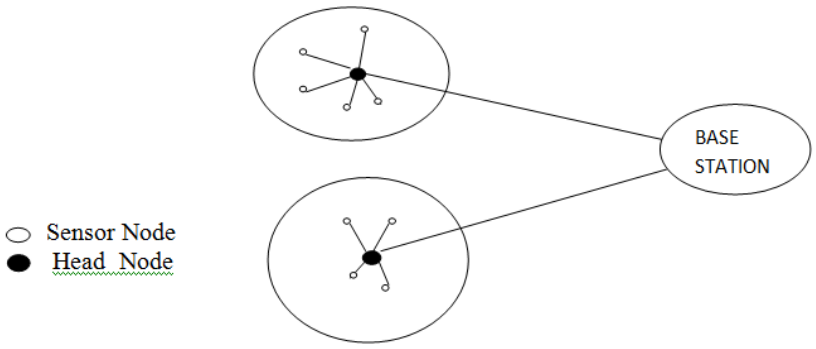


Figure 5. Clustering in LEACH Protocol

5. Localization Algorithms

Localization is a process of calculating a node's position either relative to other reference nodes/landmarks or its global position. In WSNs, these reference nodes are called anchors primarily because their position (whether it is relative or global) is known to the network/application. Usually, because of the specialized feature requirement of these nodes, they are either base stations or cluster heads. For the purposes of terminology, the nodes that need to be localized are called unknown nodes. The fundamental approaches to localization exploit geometric relationships between anchor nodes and unknown nodes to calculate the localization result. Received signal strength indicator, angle of arrival (AOA), time of arrival (TOA) and time difference of arrival (TDOA) are examples of localization techniques.

5.1. Received Signal Strength Indicator (RSSI) [4] is the technique that uses the spatial correlation between the signal strength and physical location to detect the presence of Sybil attacks. This method measures the received power associated with incoming message(s) from a node and relates this to a unique location and subsequently a unique ID. Usually, there are several nodes measuring this value in order to triangulate this position. In the event that another message is received having the same location but a claim to a different ID, the system will assume that this entity is a Sybil node. Usually a minimum of three nodes are required but there are claims that four nodes are required to locate a node using RSSI effectively. The choice of the frequency of RSSI calculations (i.e. on which transactions does the system need to verify a node's identity claim) varies for different solutions based on the researcher's goal. Sometimes, this value is calculated only if a new node sends a message or if the system is in bootstrap, while other solutions run this calculation on every message.

5.2 Angle of Arrival (AOA)

The angle is estimated by phase differences in the signal received by two or more individual sensors (microphones for acoustic signals or antennas for RF signals).With directional antennas, AOA estimation uses the RSS ratio between two (or more) directional antennas located on the sensor. Two directional antennas pointed in different directions, such that their main beams overlap, can be used to find the AOA from the ratio of their individual RSS values. The position of a sensor node is determined as an intersection of antenna sectors of different anchor nodes [10].

5.3 Time of Arrival (TOA)

TOA is the measured time at which the incoming message first arrives at a receiving node. The measurement is the time of transmission plus a propagation-induced time delay. The assumption is that the time delay, $T_{i, j}$, between transmission from node i and reception at node j, is the distance between them divided by the propagation velocity v_p . Generally, a free-space wave propagation model is used for the models. In free space, $v_p \approx 3 \times 10^8$ m / s. A critical success factor for TOA is the receiver's ability to estimate the arrival time of the line-of-sight (LOS) incoming message accurately [15].

5.4 Time Difference of Arrival (TDOA)

The TDOA method is an improvement of the TOA method. In TOA, there is a requirement to know actual timestamps when messages are sent and when they arrive at the anchor node. Hence there is a crucial necessity for strict time synchronization of the whole network. The

TDOA method uses the time difference of signal propagation between anchor nodes (or beacons) and unknown nodes, but not propagation time itself. In doing so, TDOA techniques reduce the requirement for stringent time synchronization for the WSN [12].
Hence we have used TDOA in our algorithm to detect the node as Sybil [16].

6. Proposed Methodology for Sybil Node Detection based on TDOA

Algorithm to Detect Head Node of Cluster as Sybil in a Sensor Network

We consider a network with some nodes and a cluster is formed on the basis of LEACH protocol in which we have head node and member node .Head node communicate with its member node and performs certain malicious activity (if it is malicious). Our detecting principle is that one of the member nodes follows the algorithm and detects it as Sybil. The algorithm is as follows:

At session 1

- Head node (which acts as a Sybil) floods messages to the member nodes.
- To detect it as a Sybil node we will consider 4 member nodes (M_1, M_2, M_3, and M_4) within its cluster.
- Now at session1 Head node floods a message with H_1 as the first id of head node, to the member nodes is as follows:

  $H \rightarrow M_i$:{Data ,H_1} where i=1 to 4.
- These member nodes record their time at which the message has arrived from head node.
- Suppose the time be t_1, t_2, t_3 & t_4.
- Member node $M_{(i>1)}$ transmit their own ID & the arriving time of message as report (R1) to M_1.

  $M_{(i>1)} \rightarrow M_1$:{$M_{(i>1)}$,H_1,t_i}.
- M_1 will use it & will compute the TDOA value between $M_{(i>1)}$ & itself as :

  $d_{(i>1),1}^{H1} = t_i - t_1$
- Then M_1 computes the ratio $tr_1 = (d_{2,1}^{H1} / d_{3,1}^{H1})$.

At session 2.

- Head node (Sybil) floods another message to its member nodes with a different id H_2.

  $H \rightarrow M_i$:{Data ,H_2} where i=1 to 4.
- Member nodes performs the same process as in session 1 and report (R2) is generated which is send to M_1.

  $M_{(i>1)} \rightarrow M_1$:{$M_{(i>1)}$,H_2,t_i}.
- M_1 computes TDOA ($d_{i,1}^{H2}$) for all i>1 & then takes the ratio $tr_2 = (d_{2,1}^{H2} / d_{3,1}^{H2})$.
- Now M_1 test by comparing the ratio tr_1 & tr_2 at session 1 & 2.

If the ratios found to be equal, then it means the Head node is the Sybil node and Sybil attack has been performed.

Algorithm to Detect Member Node of Cluster as Sybil in a Sensor Network

To detect member node of the cluster as a Sybil, the algorithm takes place at head node.

- Member nodes (M_i) send the time of arrival (t_i) of message to its cluster head (C).
- C computes difference of arrival time of two simultaneously arriving messages from a particular member node (M_i).
- Again after certain interval of time, C performs the same function.
- If the difference, at both the sessions for the same message, found to be equal, then the member node is Sybil.

7. Experimental Results

TDOA-based algorithm has been implemented in MATLAB .We have considered LEACH routing protocol for generating clusters in the network. We have assumed a static network where the sensor nodes are deployed within a specific area. The simulation parameters are given in Table 1. If the head node of any cluster perform malicious activity *i.e.,* floods messages again and again then our algorithm is capable to detect it .Detection is done on member node .Some results on member node if head node act as sybil are shown in Table 2 [16].

Table 1. Simulation Parameters

Parameter	**Value**
Protocol used	LEACH
Simulation area	100m X 100m
No. of nodes	20,30,40,50
Transmission Range	30m
Transmitter Energy	50NJ
Reciever Energy	50NJ
Type of network	Static
Sink node at	(50,50)

Table 2. TDOA Measure of Sybil Node (Head Node) at its Member Node 1 for 30 Nodes

S. No.		**TDOA at session 1**	**TDOA at session 2**
1.	**At member node 1**	**0.012**	**0.013**
	At member node 2	**0.025**	**0.027**
	TDOA Ratio	**0.48**	**0.48**
2.	**At member node 1**	**0.017**	**0.018**
	At member node 2	**0.034**	**0.036**
	TDOA Ratio	**0.5**	**0.5**
3.	**At member node 1**	**0.012**	**0.013**
	At member node 2	**0.025**	**0.027**
	TDOA Ratio	**0.48**	**0.48**
4.	**At member node 1**	**0.009**	**0.010**
	At member node 2	**0.018**	**0.020**
	TDOA Ratio	**0.5**	**0.5**
5.	**At member node 1**	**0.017**	**0.018**
	At member node 2	**0.034**	**0.036**
	TDOA Ratio	**0.5**	**0.5**

Likewise we have performed the experiment 25 times and found that the detection rate comes to be 96% *i.e.*, if the node is Sybil then our algorithm can detect it to a greater extent. Few results with varying the no. of nodes in the network are given in Table 3. Detection Rate is given by the percentage of Sybil attack attempts that are determined to be under attack. If the Sybil attack is present, the detection rate corresponds to the probability of detection P_d, while under normal conditions it corresponds to the probability of false positive P_{fa} [13].

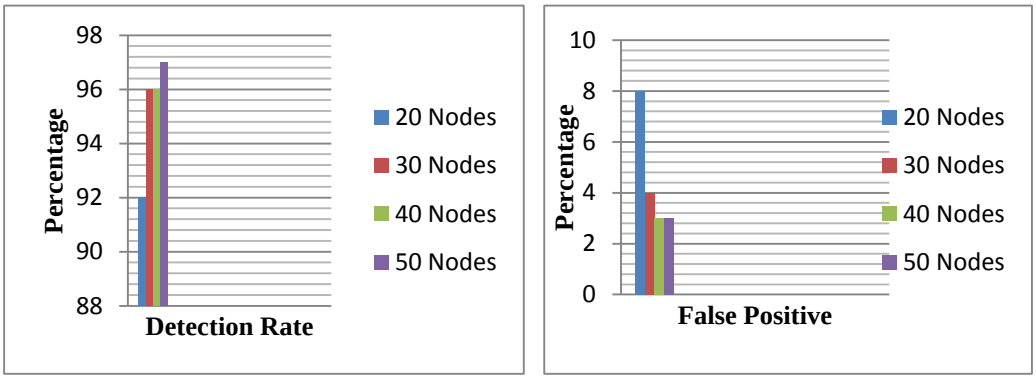


Figure 6. Detection Rate And False Positive

7.1 Analysis of Energy Consumption

Energy consumption is one of the most fundamental but crucial factor determining the success of the deployment of sensors and wireless sensor networks (WSNs) due to many severe constraints such as the size of sensors, the unavailability of a power source, and inaccessibility of the location and hence no further handling of sensor devices once they are deployed.

In our simulation we have check the energy performance of the network in the absence (Figure 7-a) and in the presence (Figure 7-a, b) of attack. The results are shown below. For calculating the initial energy of the nodes we have considered the distance between the node and the sink node and the transmitting and receiving energy of each node.

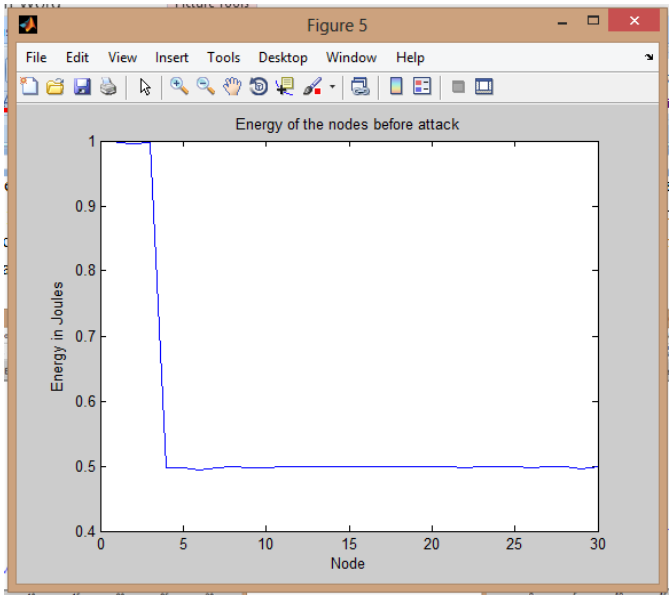
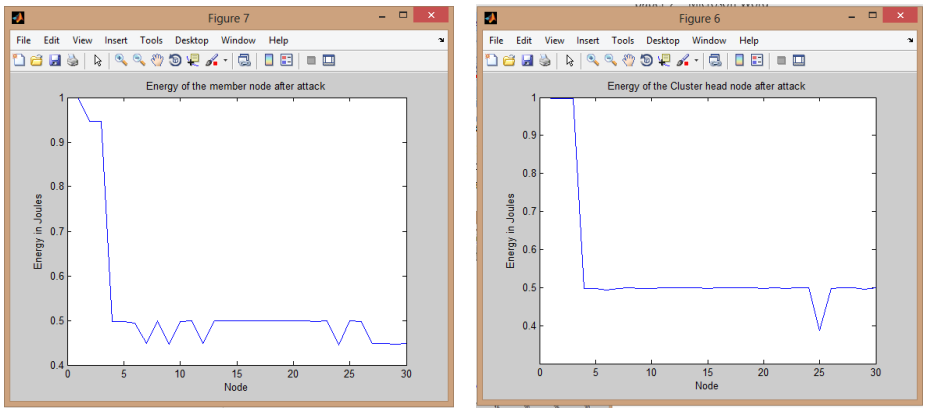


Figure 7: (a) Energy consumption before Sybil attack



(b) (c)

Figure 7. (b) Energy Consumption after Sybil Attack for Member Nodes (C) for Head Node

We can observe from the results that, there is drop in the value of energy, since the energy is consumed in doing some work. The energy consumed is calculated on the basis of the following [19]:

$$E_{consumed,i} = E_{initial,i} - E_{TR} \quad ...(1)$$

where "i" is the node of which energy is to be calculated. It can be head node or member node.

E_{TR} is the energy of the particular node, for transmitting and receiving unnecessary messages from the malicious node.

This energy consumed affects the network performance and its lifetime. Hence it can be minimized so that the network functionality remains the same. There are many algorithms available in the literature for minimizing energy consumption. We find two algorithms best which can be applied for minimization named MAP_Opt and MAP_CP. MAP (Mode Assignment with Probability) is the method where node can be assigned three modes: active, vulnerable and sleep mode .If the nodes have any of these mode ON then there energy can be minimized. MAP_Opt and MAP_CP follow this concept.

8. Conclusion and Future Work

In this paper, we proposed a method to detect head node and member node of cluster in WSN as Sybil .There are various algorithms present in the literature to detect Sybil attack. In comparison to the conventional Sybil attack detection methods, our TDOA based approach is better as it does not require any computational overhead to wireless devices and sensor nodes. Our method has achieved a detection rate of 96% and very low false positive rate of 4% and below. Hence our approach is effective in detecting Sybil attack in Wireless Sensor Network. We have also analyzed the energy consumption of nodes before and after attack. In order to minimize the energy consumption, a energy efficient algorithm has been suggested in the paper. In future, we are planning to implement the energy efficient algorithm and computing the results for reducing the consumption of energy, so that the network lifetime is not affected by the malicious activity of the Sybil nodes present in the network.

References

[1] J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in IPSN'04: Proceedings of the Third International Symposium on Information Processing in Sensor Networks, **(2004),** pp. 259–268.
[2] J. R. Douceur, "The sybil attack", In IPTPS'01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, **(2002),** pp.251–260.
[3] M. Demirbas and Y. W. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", International Workshop on Wireless Mobile Multimedia, **(2006),** pp. 564-570.
[4] J. Wang, G. Yang, Y. Sun and S. Chen, "Sybil Attack Detection Based on RSSI for Wireless Sensor Network", IEEE International Conference, **(2007),** pp. 684-687.
[5] H. N. Saha, D. Bhattacharyya and P. K. Banerjee, "Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack", International Journal of Computer Science & Emerging Technologies, vol. 1, Issue 4, **(2010)** December.
[6] A. Vasudeva and M. Sood, "Sybil Attack on Lowest ID Clustering Algorithm in the Mobile Adhoc Network", International Journal of Network Security & its Applications (IJNSA), vol. 4, no. 5, **(2012)** September.
[7] M. M. Patel and A. Aggarwal, "Security Attacks in Wireless Sensor Networks: A Survey", International Conference on Intelligent Systems and Signal Processing, **(2013)**.
[8] C. S. R. Murthy and B. S. Manoj, "Adhoc wireless Networks".
[9] D. Bhattacharyya, T.-H. Kim and S. Pal, "A Comparative Study of Wireless Sensor Networks and Their Routing Protocols", mdpi journals, pp.506-523, **(2010)**.
[10] P. Kułakowski, *et al.*, "Angle-of-arrival localization based on antenna arrays for wireless sensor networks", Journal of Computers and Electrical Engineering, elsevier, **(2010)**.
[11] Q. Zhang, P. Wang, D. S. Reeves and P. Ning "Defending against Sybil attack in sensor network", In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops(ICDCSW'05), **(2005)**.
[12] W. Mi, L. Hui, Z. Yanfei and C. Kefei, "TDOA-based Sybil Attack Detection Scheme for wireless Sensor Networks", Journal of Shangai University (English Edition), vol. 12, no. 1, **(2008),** pp. 66-70.
[13] J. Yang, Y. Chen and W. Trappe, "Detecting Sybil Attacks in Wireless and Sensor Networks Using Cluster Analysis", IEEE International Conference, **(2008).**
[14] S. Pal, A. K. Mukhopadhyay and P. P. Bhattacharya, "Defending Mechanisms against Sybil Attack in Next Generation Mobile Adhoc Networks", IETE Technical Review, vol. 25, issue 4, **(2008)** July-August.
[15] Z. Yang, Z. Zhou and Y. Liu, "From RSSI to CSI: Indoor Localization via Channel Response", ACM Computing Surveys, vol. 46, no. 2, Article 0, **(2014)** June.
[16] S. Saxena and V. Sejwar, "Sybil Attack Detection through TDOA-Based Localization Method in Wireless Sensor Network", International Journal of Emerging Technologies in Computational and Applied Sciences, vol. 9, no. 2, **(2014)** June-August, pp. 110-114.
[17] C. Townsend and S. Arms, "Wireless Sensor Networks: Principles and Applications, Micro Strain, Inc.
[18] Thesis, "System Architecture for Wireless Sensor Networks", Jason Lester Hill, **(2003)**.
[19] N. Kamyabpour, D. B. Hoang, "Modeling overall energy consumption in Wireless Sensor Networks".
[20] M. Qiu, C. Xue, Z. Shao and Q. Zhuge, "Efficient Algorithm of Energy Minimization for Heterogeneous Wireless Sensor Network", International Federation for Information Processing, **(2006),** pp. 25-34.
[21] A.-S. K. Pathan and H.-W. Lee, "Security in Wireless Sensor Networks: Issues and Challenges".

Authors

Sweety Saxena, she is born in India in 1990. She is currently M.Tech scholar in computer science and engineering department at Madhav Institute of Technology and Science, Gwalior, India. She has completed B.E in computer science and engineering from NRI-ITM, Gwalior, India in 2012. Her research area includes MaNets and Wireless Sensor Network.

Vikas Sejwar, he is presently Assistant Professor in computer science and engineering department at Madhav Institute of Technology & Science, Gwalior, India. He has got M.Tech degree from SOIT, RGPV, Bhopal in 2008. He has got B.E. degree from MITS, Gwalior in 2006. His research area includes Mobile Adhoc Network and Computer graphics.

