



Sybil Attack Detection through TDOA-Based Localization Method in Wireless Sensor Network

Sweety Saxena¹, Vikas Sejwar²

Department of CSE/IT, Madhav Institute of Technology and Science
Gwalior, M.P, India

Abstract: *Wireless Sensor Networks are being widely used for large-scale real-time data processing due to its characteristics and is used in application areas such as in military and civilian domains. These networks are more prone to several security attacks. In this paper, we emphasized on Sybil attack, which is a particularly harmful threat to WSNs and proposed an algorithm based on Time difference of Arrival (TDOA) localization method, which detect the malicious behavior of head node in a cluster based network.*

Keywords: *Sybil attack, LEACH, Localization algorithm, RSSI, TDOA.*

I. Introduction

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 [1][4]. 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 [8]. WSN is vulnerable to several types of security attacks. Attacks such as wormhole, sinkhole, black hole, and selective flooding are possible, but Sybil attack is one of the particularly harmful attack for WSN [7].

Sybil attack is the attack in which single node forge multiple identities in the network so as to disrupt the normal functioning of the network [2]. Nature of Sybil node in the network is flooding messages again and again in the network so as to affect the performance of the sensor network by proving harmful to many functions like group based decisions, routing, fair resource allocation, data aggregation and voting etc [3].

Sensors have limited bandwidth, computing power and memory size due to which use of conventional algorithms to detect Sybil attack is not suitable to use. Detection algorithms that use identity certificate methods & radio resource testing method require huge memory usage and energy consumption. We used a localization algorithm to detect Sybil node which does not require any computational overhead and it easily detect node as malicious. In this paper, we have proposed a method to detect Sybil attack in WSN on the basis of Time difference of arrival. This algorithm is applied on clusters i.e. we detect head node (Sybil) of clusters as malicious with the help of member nodes present in the network.

The rest of the paper is organized as follows. Section II gives the Overview of Sybil attack and its types. Section III describes the LEACH protocol. Section IV includes the localization algorithms. The basic algorithm is presented in section V. Simulation results are shown in section VI. Finally concluding remarks are given in Section VII.

II. Sybil attack

Douceur [1] 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. 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 only one physical device [11]. 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.

Newsome et al. [2] established a classification of different types of Sybil Attacks:

A. 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].

B. 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].

C. 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 favour [6].

D. 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.

E. 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 the protocols are LEACH, TEEN, APTEEN [9] etc.

III. 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 1.

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.

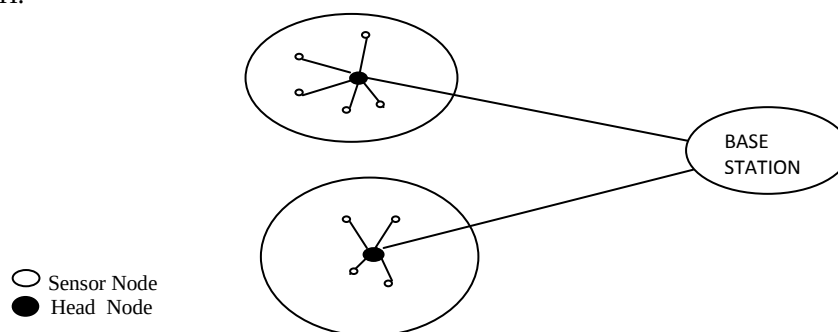


Figure 1: Clustering in LEACH Protocol

IV. 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 [15]. 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.

A. Received signal strength indicator (RSSI)

RSSI 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.

B. 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 [10]. 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.

C. 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.

D. 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 [12]. In doing so, TDOA techniques reduce the requirement for stringent time synchronization for the WSN.

Hence we have used TDOA in our algorithm to detect the node as Sybil.

V. Sybil Node Detection based on TDOA

A. Algorithm to Detect Head Node of Cluster as Sybil Node

Given a network 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

- Suppose a 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).
- Now a Head node broadcast a message with H_1 as the first id of head node, at session1 to the member nodes.

$$H \rightarrow M_i : \{ \text{Data}, H_1 \} \text{ where } i=1 \text{ to } 4.$$
- These member nodes record their time at which the message has arrived. Suppose the time be t_1, t_2, t_3 & t_4 .
- Now member node $M_{(i>1)}$ transmit their own ID & the arriving time of message as report₁ 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 :

$$d_{(i>1),1}^{H_1} = t_i - t_1$$

- 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 .
 $H \rightarrow M_i : \{ \text{Data}, H_2 \}$ where $i=1$ to 4.
- Member nodes performs the same process and $report_2$ 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.

VI. 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 table2 .

Table 1. Simulation Parameters

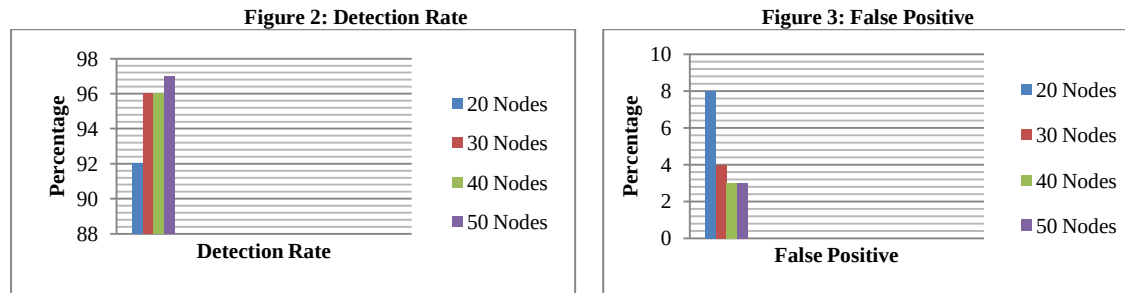
Parameter	Value
Protocol used	LEACH
Simulation area	100m X 100m
No. of nodes	20,30,40,50
Transmission Range	30m
Transmitter Energy	50NJ
Receiver Energy	50NJ
Type of network	Static
Sink node at	(50,50)

Table 2: TDOA measure of Sybil node (head node) at its member node1 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
6.	At member node 1	0.019	0.017
	At member node 2	0.037	0.036
	TDOA Ratio	0.51	0.47
7.	At member node 1	0.016	0.018
	At member node 2	0.035	0.035
	TDOA Ratio	0.45	0.51
8.	At member node 1	0.017	0.018
	At member node 2	0.034	0.036
	TDOA Ratio	0.5	0.5
9.	At member node 1	0.014	0.016
	At member node 2	0.028	0.032

	TDOA Ratio	0.5	0.5
10.	At member node 1	0.011	0.012
	At member node 2	0.022	0.024
	TDOA Ratio	0.5	0.5

Likewise we have performed the experiment 30 times and found that the detection rate comes to be 97% 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 shown in Fig.2 and Fig.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].



VII. Conclusion and future work

In this paper, we proposed a method to detect head 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 method, 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 97% and very low false positive rate of 4% and below. Hence our approach is effective in detecting Sybil attack in Wireless Sensor Network. In future, we are planning propose a method for reducing the effects of the attack and will check the performance of the network in the presence and in the absence of attack.

References

- [1] J. R. Douceur, "The sybil attack," In IPTPS'01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp.251–260, 2002.
- [2] 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, pp. 259–268,2004.
- [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,pp.564-570,2006.
- [4] JiangtaoWang, GengYang, YuanSun and Shengshou Chen, "Sybil Attack Detection Based on RSSI for Wireless Sensor Network," IEEE International Conference , pp.684-687, 2007.
- [5] Himadri Nath saha, Dr. Debika Bhattacharyya and Dr. P. K. Banerjee, "Semi centralized multi authenticated RSSI based solution to sybil attack," International Journal of Computer Science & Emerging Technologies, volume1, Issue 4, December 2010.
- [6] Amol vasudeva and Manu 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, September 2012.
- [7] Manish M Patel and Dr.Akshai Aggarwal, "Security Attacks in Wireless Sensor Networks: A Survey," International Conference on Intelligent Systems and Signal Processing, 2013.
- [8] Adhoc wireless Networks by C.Siva Ram Murthy and B.S.Manoj.
- [9] Debnath Bhattacharyya, Tai-hoon Kim, and Subhajit Pal, "A Comparative study of wireless sensor networks and their routing protocols," mdpj journals, pp.506-523, 2010.
- [10] Paweł Kułakowski , Javier Vales-Alonso, Wiesław Ludwin "Angle-of-arrival localization based on antenna arrays for wireless sensor networks," Journal of Computers and Electrical Engineering, Elsevier, 2010.
- [11] Qinghua Zhang,Pan Wang,Douglas S. Reeves, and Peng 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] Wen Mi,Li hui,Zheng Yanfei and Chen Kefei, "TDOA-based Sybil Attack Detection Scheme for wireless Sensor Networks," Journal of Shanghai University(English Edition), Vol.12, No. 1, pp.66-70, 2008.
- [13] Jie Yang, Yingying chen and Wade Trappe, "Detecting Sybil Attacks in Wireless and Sensor Networks Using Cluster Analysis," IEEE International Conference, 2008.
- [14] Sarit Pal,Asish k.Mukhopadhyay and Partha Pratim Bhattacharya, "Defending Mechanisms Against Sybil Attack in Next Generation Mobile Adhoc Networks," IETE Technical Review, Vol.25, issue 4,Jul-Aug 2008.
- [15] Zheng Yang, Zimu Zhou and Yunhao Liu, "From RSSI to CSI: Indoor Localization via Channel Response," ACM Computing Surveys, Vol. 46, No. 2, Article 0, June 2014.