ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

Survey on Literature Detection Methods of Sybil Attack In WSN

Omar Badeea Baban
Department of Computer Engineering
Sinhgad College of Engineering, Pune-41, Pune, India

Abstract:- **A wireless Sensor Network (WSN) is a distributed network of small sensor nodes deployed in large numbers to monitor the environment or other systems by the measurement of physical parameters such as temperature, pressure, or relative humidity. These nodes by monitoring collect detailed information about the physical environment in which they are installed, and then transmit the collected data to the Base Station (BS). BS is a gateway from sensor networks to the outside world. It passes the data it receives from sensor nodes to the server from where end-user can access them. Security in WSN is a greater challenge due to the processing limitations of sensor nodes and nature of wireless links. Extensive use of WSNs is giving rise to different types of threats. To defend against the threats proper security schemes are required. Traditionally security is implemented through hardware or software and is generally achieved through cryptographic methods. Limited area, nature of links, limited processing, power and memory of WSNs leads to strict constraints on the selection of cryptographic techniques. The Sybil attack is one of the dangerous attacks against sensor and ad-hoc networks, where a node illegitimately claims multiple identities. A Sybil attacker can cause damage to the ad hoc networks in several ways. For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or paths. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic.**

Keywords : **Wireless Sensor Network, Sybil Attack, Sensor, illegitimately, Clusters, Cluster Head, Vulnerable, Base Station.**

1. INTRODUCTION

1.1 Motivation

A wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, the traditional technique requires Geographical positioning system and Hardware like antennas, so the cost of the initial setup is very high. This paper describes, differentiation of legitimate user and illegitimate user or Sybil attacker even in the high mobility because, now a days the QOS is necessary in the network. This proposed scheme detects Sybil identities and legitimate identity even in high mobility. In particular, proposed scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First, we demonstrate the entry and exit behavior of legitimate user and Sybil user using simulation and real world test bed experimentation. Second, the threshold is defined to distinguish between the legitimate node and the Sybil node based on nodes' entry and exit behavior. Third, the threshold is detected by the getting average of all the nodes received signal strength values.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

1.2 Definitions of WSN

A WSN can generally be described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment.

WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area (sensor field), form networks through self-organization. Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multichip routing, and finally reach the management node through the internet or satellite. It is the user who configures and manages the WSN with the management node; publish monitoring missions and collection of the monitored data.

As related technologies mature, the cost of WSN equipment has dropped dramatically, and their applications are gradually expanding from the military areas to industrial and commercial fields. Meanwhile, standards for WSN technology have been well developed, such as Zigbee, Wireless Hart, ISA 100.11a, wireless networks for industrial automation – process automation (WIA-PA), etc. Moreover, with new application modes of WSN emerging in industrial automation and home applications, the total market size of WSN applications will continue to grow rapidly.

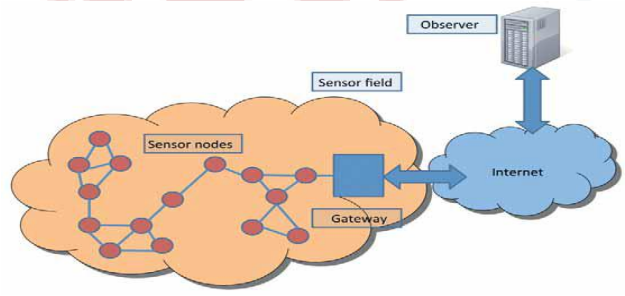

Figure 1.1 Wireless Sensor Networks [5]

The sensor node is one of the main parts of a WSN. The hardware of a sensor node generally includes four parts: the power and power management module, a sensor, a microcontroller, and a wireless transceiver, see Figure 1.2.

The power module offers the reliable power needed for the system. The sensor is the bond of a WSN node which can obtain the environmental and equipment status. A sensor is in charge of collecting and transforming the signals, such as light, vibration and chemical signals, into electrical signals and then transferring them to the microcontroller. The microcontroller receives the data from the sensor and processes the data accordingly. The Wireless Transceiver (RF module) then transfers the data, so that the physical realization of communication can be achieved. It is important that the design of the all parts of a WSN node consider the WSN node features of tiny size and limited power.

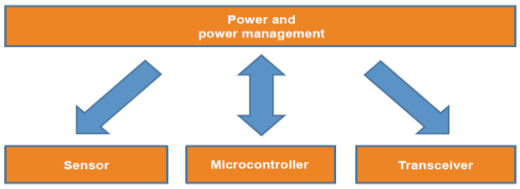

Figure 1.2 Hardware Structure of a WSN sensor node [5]

Sybil Attack Definitions

Sybil node is the process of creating two or more duplicate nodes with similar identity i.e. same node id as shown in Fig.1.3. Particularly, wireless sensor networks are more prone to Sybil attack because of the open and broadcast communication medium and the same frequency is being shared among all nodes. In Sybil attack, attacker makes multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. So the base station cannot distinguish the legitimate and the forged node. This confuses the base station and other nodes and the network performance degrades.

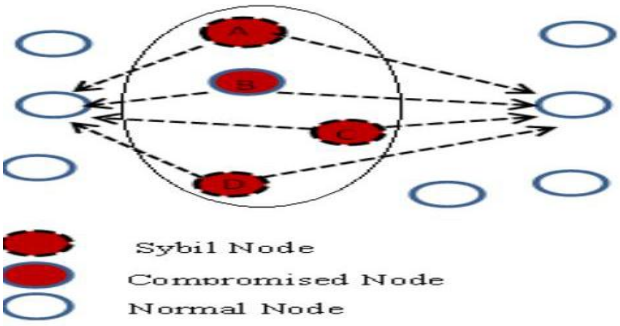

Figure 1.3 Sybil Node [17]

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

In Wireless sensor networks, mechanisms for redundancy are identity-based. It is assumed that each node is distinguished as one entity and presents only one single abstract concept of an identity. Hence, WSNs. and nodes are vulnerable to any method which allows identities to be forged or falsified. Such a malicious method is the Sybil attack. In Sybil attack, a single node intentionally, illegally presents many false or forges identities to other nodes in the network by either new (false) identities, or stealing legal identities from others. A Sybil node is a misbehaving node's extra identity. Therefore, a single entity may get selected many times (depends on number of identities) to participate in an network operation that relies on redundancy, thereby controlling the outcome of the operation, and defeating the redundancy mechanisms. Doueceur introduced the Sybil attacks on P2P architecture first time [7].

2. LITERATURE REVIEW

2.1 Literature Detection methods of Sybil Attack in WSN

Still now there exists no such well accepted technique to detect the Sybil attack. A number of methods have been proposed associated with different environments. Some of them are effective to reduce the threat to a satisfactory level. In this section different approaches proposed to prevent and mitigate the attack are discussed.

A. Message Authentication and Passing Method According to authors in [30], the Sybil attack is a massive destructive attack against the WSN, in which numerous genuine identities with forged identities are used for getting an illegal entry into a network. The existing method Random Password Comparison has only a scheme which is to just verify the node identities by analyzing the neighbors. In this paper authors, proposed a scheme of assuring the security for wireless sensor network, to deal with the attacks of these kinds in unicasting and multicasting. In this paper the message authentication and passing method is applied in order to check the trustworthiness or otherwise for a Sybil node. Verification of node needs the application of CAM-PVM. Instead of wasting time for CAMPVM to check each node, the message authentication and passing procedure is to be applied for authentication prior to communication. If a node does not have any authorization from the network or from the base station, it can't communicate with any other node in the network. The message authentication and passing method is known for more time consuming as compare to any other method.

B. TDOA method Authors emphasize on sybil attack and proposed an algorithm for sybil attack detection based on Time difference of Arrival (TDOA) localization method in [26]. This method detects the malicious behavior of head node and member nodes in a cluster based network. In this paper, authors, proposed a method to detect the head node and member node of cluster in WSN as sybil. Authors claim that in comparison to the conventional sybil attack detection methods, their TDOA based approach is better as it does not require any computational overhead to sensor nodes. According to authors, TDOA has achieved a detection rate of 96% along with very low false positive rate of 4%. The paper also analyze the consumption of energy of nodes before and after attack. In order to minimize the consumption of energy, an energy efficient algorithm has been suggested in the paper.

C. Random password comparison method A Random Password Comparison [RPC] method is proposed in [18]. This method facilitates deployment and control of the positions of the nodes and thereby it prevents the occurrence of sybil attack in WSN. According to authors, the RPC method is dynamic as well as accurate in detecting the sybil attack. The method also helps in improving data transmission in the network along will increase in the throughput. RPC algorithm discovers a valid route in the sensor network by checking each node is a trustable node or a sybil node so that the data can be transmitted very safely. The authors claim that, the sybil nodes are detected and data leakage is avoided completely by using RPC. As the sybil nodes are detected in the discovery stage of finding initial route, this enables continuation of the for further transmission without any fear of attack.

D. Neighborhood RSS based approach Investigation of Sybil attack which is one of the most disrupting attacks in context of wireless sensor networks is done in [31]. A lightweight scheme is proposed in this paper to detect the new identities of sybil nodes, this scheme does not use centralized trusted third party, it makes use of neighborhood RSS to differentiate between the legitimate and Sybil identities. RSS based process is used in this paper to detect Sybil attacks in a wireless sensor network. According to authors, it is verified that a detection threshold is used to make the distinction

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

between legitimate new nodes and new malicious identities.

Throughput, packet loss ratio, true positive rates, end-to-end delay, false positive rates are used to analyze the performance of the system. According to authors, the simulation results show that this scheme has a high level of accuracy with detection process gives us the high true positive rates up to 80% with low false positive rates that range to 16%.

E. SYBILSECURE technique An energy efficient algorithm named Sybil Secure is proposed in [1]. According to the authors, experimental results show that Sybil secure consumes less energy as compare to the existing defense mechanisms. Sybil secure is based on sending and acknowledging the query data packets. Social network based schemes that are involved in random routes of data consume more energy in order to detect a sybil node. But in Sybil secure , less energy is used for detection of Sybil node. The proposed solution is basically based on sending to and responding from the query sent by the cluster head. The Cluster head has a list of its sub nodes parameters, these parameters are identities and their locations. The Cluster head broadcasts query packet to all sub-nodes in such a way that it expects a reply from all the sub nodes, so that they must send their id and location.

2.2 Survey Conclusion

In this section different proposed approaches to prevent and mitigate the Sybil attack are discussed and their comparative study is represented in Table 2.1.

Technique to mitigate Sybil attack	Disadvantages / Limitations
Message Authentication and Passing Method	• The message authentication and passing method is applied in order to check the trustworthiness or otherwise for a Sybil node or otherwise for a Sybil node. • If a node does not have any authorization from the network or from the base station, it can't communicate with any other node in the network. • The message authentication and passing method is known for more time consuming as compare to any other method.
TDOA method	• It is an algorithm for Sybil attack detection based on Time difference of Arrival (TDOA) localization method. • This method detects the malicious behavior of head node and member nodes in a cluster based network. • TDOA has achieved a detection rate of 96% along with very low false positive rate of 4%. • It doesn't require any computational overhead to sensor nodes. • Minimize the nodes consumption of energy during an attack.
Random password comparison method	• This method facilitates deployment and control of the positions of the nodes and thereby it prevents the occurrence of Sybil attack in WSN, the RPC method is dynamic as well as accurate in detecting the Sybil attack. • RPC algorithm discovers a valid route in the sensor network by checking each node is a trustable node or a Sybil node so that the data can be transmitted very safely. • The Sybil nodes are detected and data leakage is avoided completely by using RPC.
Neighborhood RSS based approach	• This lightweight scheme use of neighborhood RSS to differentiate between the legitimate and Sybil identities. • This scheme has a high level of accuracy with detection process gives us the high true positive rates up to 80% with low false positive rates that range to 16%.
SYBILSECURE technique	• Experimental results show that Sybil secure consumes less energy as compare to the existing defense mechanisms. • Sybil secure is based on sending and acknowledging the query data packets. • The proposed solution is basically based on sending to and responding from the query sent by the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

	cluster head. The Cluster head has a list of its sub nodes parameters, these parameters are identities and their locations. The Cluster head broadcasts query packet to all sub-nodes in such a way that it expects a reply from all the sub nodes, so that they must send their id and location.

3.1 Leach-E Protocol

LEACH-E protocol improves the CH selection procedure. Sensor node's residual energy is the main concern, which decides whether the node become a CH or not after the first round (BaniYassein .M et al2009). Like LEACH protocol, LEACH-E is divided into rounds (Shankar .M et al. 2012). In the first round, all the nodes have the same probability of being a CH. At the end of the first round, the node, which has more residual energy, is elected as CH. LEACH–E protocol improves the cluster head selection procedure. [19]

3.2 Leach-E-GA (Leach-Energy-Genetic Algorithm)

This methodology uses the LEACH-Genetic algorithm (GA) that would enhance the WSN response time, network life and minimize the delay. The Genetic algorithm proposed by (Goldberg et al in 1975;Wu Xinhua and Wang Sheng. 2010) improves the cluster heads selection process. Selecting the minimum number of cluster heads in the WSN is determined based on the square root of the total number of sensor nodes, to minimize the total energy consumption. The LEACH-E Genetic algorithm is shown in figure 3.1 selects an unsupervised node, which allows the network to achieve maximum coverage distance with minimum energy consumption. Genetic algorithm optimizes the behavior of the node based on its request and response, energy level, mobility and comparison with its record of previous transmissions. A node, whose behavior is changed and not fit to the fitness function, is considered to be the Sybil node. The node is dropped from the network to improve the quality of the network for future communication.

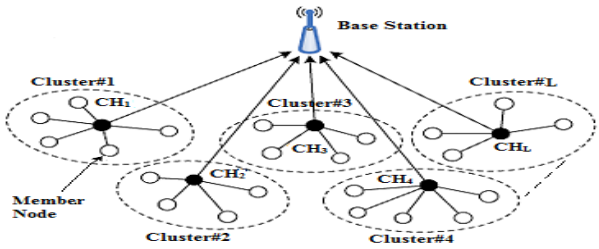

Figure 3.1 GA Hierarchical Clustering [19]

Genetic_Algorithm ( )
{

- Initialize population and Objective Function Value-[OFV].
- Define the Fitness function.
- Selection.
- Cross over.
- Mutation.
- Repeat the above steps until reaching the solution.

}

A population contains a group of individuals named chromosomes, which represents a finished solution for a derived problem. Each chromosome is a sequence of values of the attribute [node-energy, node-trust value, and node-distance].

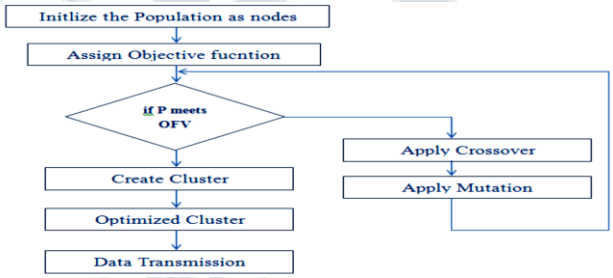

Figure 3.2 GA Flowchart used for WSN [19]

Once an initial population is randomly generated, the algorithm evolves through three operators:
1. Selection: This equates to survival of the fittest.
2. Crossover: This represents mating between individuals.
3. Mutation: This introduces random modifications.

4. CONCLUSION

The applications of wireless sensor network are increasing along with the need for more effective security mechanisms. The security concerns of the WSNs should be addressed from the beginning of designing of the system, since sensor networks interact with sensitive data and they usually operate in hostile unattended environments. A thorough understanding of the capabilities and limitations of each of underlying technology is required for the secure working of wireless sensor networks. In Sybil attack, a node illegitimately claims multiple identities or claims fake IDs in order to collapse the sensor network. A thorough study of limitations of available techniques will help in the design

of novel, robust, and secure mechanism against Sybil attack, so that the sensor network applications can be extended to other fields.

The aim of the cluster based Hierarchy routing protocol LEACH-E (Low Energy Adaptive Clustering Hierarchy-Energy) is to provide secure routing and to preserve the functionalities of the original protocol. This energy efficient protocol always elects a Cluster Head (CH) based on high energy among the cluster group. Here we propose a LEACH-E-GA for Intrusion detection (ID) in Wireless Sensor Nodes. The Genetic Algorithm is deployed into LEACH-E to provide prevention for Sybil attacks. The objective of this Genetic Algorithm (GA) is to identify its best trusted neighbors for communication using its optimization capability. LEACH-E-GA reduces an inside Sybil attack in WSN and shows reliable transmission with improved network efficiency, reduced delay and increased packet delivery ratio. In LEACH-E-GA algorithm the node behavior is controlled and network prolong lifetime is improved. With this algorithm we can extend the work to monitor the network using Intrusion Detection Protocol using Cryptography.

REFERENCE

[1] A. Babu Karuppiah and A. Raja Prakash, "SYBILSECURE: an energy efficient sybil attack detection technique in wireless sensor network," International Journal of Information Sciences and Techniques (IJIST) Vol. 4, No. 3, May 2014.

[2] Dr. Shu Yinbiao, Dr. Kang Lee, Mr. Peter Lanctot," Internet of Things: Wireless Sensor Network " White Paper 2014 International Electrotechnical Commission-IEC, China (http://www.iec.ch).

[3] John R. Douceur, The attack, (2002), 251–260. http://shodhganga.inflibnet.ac.in/bitstream/10603/22912/7/07_chapter_01.pdf

[4] Prabhjotkaur, Aayushi Chada, Sandeep Singh," Review Paper of Detection and Prevention of Sybil Attack in WSN Using Centralizedids", International Journal of Engineering Science and Computing (IJESC), July 2016, Volume 6 Issue No. 7

[5]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 Technology, September 2014, Vol. 67, No.1, ISSN: 1992- 8645.

[6]R. Amuthavalli & R. S. Bhuvaneswaran, "Genetic Algorithm Enabled Prevention of Sybil Attacks for LEACH-E", in Modern Applied Science Vol. 9, No. 9; 2015, Published by Canadian Center of Science and Education.

[7]Raed, M. B. H., &Abdalraheem, A. I. (2013). A Survey on LEACH-Based Energy Aware Protocols for Wireless Sensor Networks. Journal of Communications, 8(3).

[8]Sweety Saxena and Prof. Vikas Sejwar, " Sybil Attack Detection and Analysis of Energy Consumption in Cluster Based Sensor Networks," International Journal of Grid Distribution Computing Vol. 7, No. 5 (2014), pp.15-30, ISSN: 2005-4262.

[9] Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method," Scientific World Journal, 2015.

[10] V. Sujatha and E. A. Mary Anita, "Detection of Sybil Attack in Wireless Sensor Network," Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 202-206, 2015, ISSN 1990-9233.