Detection of SYBIL Attack using Neighbour Nodes in Static WSN

[1]C. Geetha, [2]M. Ramakrishnan
[1]Research Scholar, Manonmaniam Sundaranar University, Tirunelveli
[2]Professor & Chairperson, School of IT, Madurai Kamaraj University, Madurai

Abstract:- As wireless sensor network is an emerging technology nowadays, it is prone to many attacks like denial of service, wormhole, clone, Sybil etc. Sybil attack is a harmful attack which affects the sensor network in routing the information. It is a malicious device that it takes multiple fake identities. This malicious device make the sensor node into Sybil node and get the information from other sensor node and send the different information to receiver or it keep the information with itself and delay the information to reach the receiver. To detect the Sybil node, we proposed a TIME-TO-TIME MESSAGE (TTM) model to detect the Sybil attack in wireless sensor network. In this method, each and every node in the sensor network will maintain an observation table for storing node id and location which is useful to detect the Sybil attack. The approach is simulated in a sensor network and the result shows a very good detection rate comparing with other existing algorithms.

Keywords: *Path Tracing, Sybil Attack, Time-To-Time Message, Wireless Sensor Network.*

*****

I. INTRODUCTION

Wireless sensor network is an interconnection of sensor nodes used to monitor and record the physical conditions of the environmental object such as pressure, temperature, pollution etc. Wireless networks comprised of low cost, high security and limited radio transmission range.WSN nodes have limited storage and computational resources. The wireless sensor network is attacked by two mechanisms they are against security mechanism and against basic mechanism (like routing).The major attackers are denial of service (DoS), sinkhole attack, wormhole attack, selective forwarding attack, passive information gathering: hello flood attack acknowledgement spoofing. The denial of service occurs when a computer or a network user is unable to access resources like e-mail and the Internet. An attack can be directed at an operating system or at the network [1].The sinkhole attack is Adversary tries to attract traffic from a particular area to pass through a compromised node, thereby creating sinkhole with adversary at the center. A node may be made to look attractive to neighbors in some routing algorithm [2]. The wormhole attack makes nodes fake a route that is shorter than the original one within the network. This can confuse routing mechanism which relies on the knowledge about distance between nodes [3]. Each sensor node has identity and location to uniquely identify them in WSN. Each node can maintain the connectivity in the nodes outside the broadcast range .Sybil attack is a harmful attack on geographic and ad hoc routing in which an adversary captures and tempers the node for the purpose of converting them as malicious. In the Sybil attack, a single node presents multiple identities to others nodes in the network. The lack of a central authority allows a malicious user to create many fake identities.

Sybil attack was first addressed in peer to peer system. The attacker subverts the reputation system of peer to peer network by creating a large number of misrepresents identities. The different types of Sybil attacks[4] are as follows:

Direct and indirect, legitimate nodes communicate directly with Sybil nodes or through malicious nodes[6]. Fabricated and Stolen Identities, creates several new ids of same length or stole the ids of other nodes. Simultaneous and non-simultaneous, uses all ids at the same time or use different ids at different times.

Redundancy mechanisms are id-based. They assume that each physical node is distinguished as one entity and presents only one single abstract concept of an identity[8]. Sybil attack allows ids to be forged or falsified.

The remaining part of the paper is organized as follows. Section II explains the literature survey, section III deals with network model and assumptions, section IV describes the proposed methodology, section V discusses the results and performance analysis and section VI concludes the paper.

II. RELATED WORKS

In this section related works on the detection of Sybil nodes are presented in static network. A Sybil node uses multiple network identities simultaneously. For an example if a node named as kava it represented as virat or anush to other nodes for retrieving data or location information. This leads to the

amount of Sybil attackers increase in the network .It will affect the network traffic and data packet will never reach the destination. In this literature there are various methods to detect the Sybil node.

Sajid et al [2], have proposed node replication, replacement, and man-in-the-middle attacks. They analyzed the feasibility of using received signal strength indicator (RSSI) values measured at the receiver node to detect the Sybil attacks. Kuo et al [3], have proposed scheme in which the node identities are verified simply by analyzing the neighboring node information of each node. Bin et al [4] have proposed a Sybil detection methods based on ranging in wireless sensor networks. They proposed to detect Sybil attacks by anchor nodes location. Wen Mi et al[5] have proposed an efficient and lightweight solution for Sybil attack detection based on the Time Difference of Arrival (TDOA) between the source nodes and beacon nodes and not only detect the existence of Sybil attacks but also locate the Sybil nodes. Raghu et al [6] have proposed a method to detect Sybil attacks using Sequential Hypothesis Testing. The proposed method has been examined using a Greedy Perimeter Stateless Routing (GPSR) protocol with analysis and simulation.

A newly proposed method to detect the Sybil nodes using time to time message model with observation table. This model is very efficient to detect the Sybil node and to also reduce the memory space in wireless sensor network[7].

Redundancy mechanisms are id-based. They assume that each physical node is distinguished as one entity and presents only one single abstract concept of an identity(8). Sybil attack allows ids to be forged or falsified.

In RRT, assume that each node can transfer via one channel at a time. To check the Sybil node, assign each node a unique channel and asks them to send an ack at a particular time. If no ack is received from a particular node, that is the Sybil node [9].

In random key pre-distribution, each node selects some k number of keys from a large pool. ID of each node is associated with set of keys of that node. By verifying the keys we can identify the Sybil node[9].

In Merkle hash tree approach, each node authenticates the IDs of all the other nodes. The Finger print approach verifies the finger prints of all neighbor nodes. Malicious nodes can't have valid finger print(8). By checking the Received Signal Strength Indicator (RSSI), identify the Sybil node. Having the assumption that probability of two nodes having the same set of neighbors is very low. The Sybil node has same set of neighbors for all its faked IDs(10).

A swarm agent collects the information about the routes(11). Sybil node is detected by energy variation. Clock skew is verified for all sensor nodes. Sybil node has same clock skew for all its falsified IDs(12).

III. PROPOSED METHODOLOGY

In this paper a method has been proposed to detect the malicious nodes which misrepresent the identity and location using TIME-TO-TIME MESSAGE MODEL (TTM). Each node in the network runs TTM to identify the Sybil node. We are using observation table to store the identity and location information for each node.

A. Network model and assumptions

Let S be a set of n sensor nodes in the network. S = {S1, S2.. Sn} deployed in a geographical region (Xi, Yi). These nodes interact directly with each other within communication range to forward the packets. In this model, it is assumed that each node has a unique identity and aware of its own location. The nodes will store each and every node identities and location in observation table. Normally location information will be obtained by using global positioning system (GPS)[10].Every node will communicate using bidirectional transceiver. A node can observe all packets.

The nodes are deployed in 1000X1000m area. Once deployed, nodes can't change their location. Each node can communicate using wireless radio channel and transfer the packets using Omni-directional mode.

The scope of our paper is to detect Sybil attacks in static wireless sensor network. To find the Sybil node, we are using observation table to store the location and id of other nodes by using path tracing algorithm.

B. Performance Metrics

Detection Rate: time taken to detect the clone and Sybil attacker.
Storage Overhead: Amount of extra space required for storing the messages
Communication Overhead: Extra messages transmitted and increase in size of these messages

 ISSN: 2321-8169
2428 - 2432

C.SYSTEM ARCHITECTURE

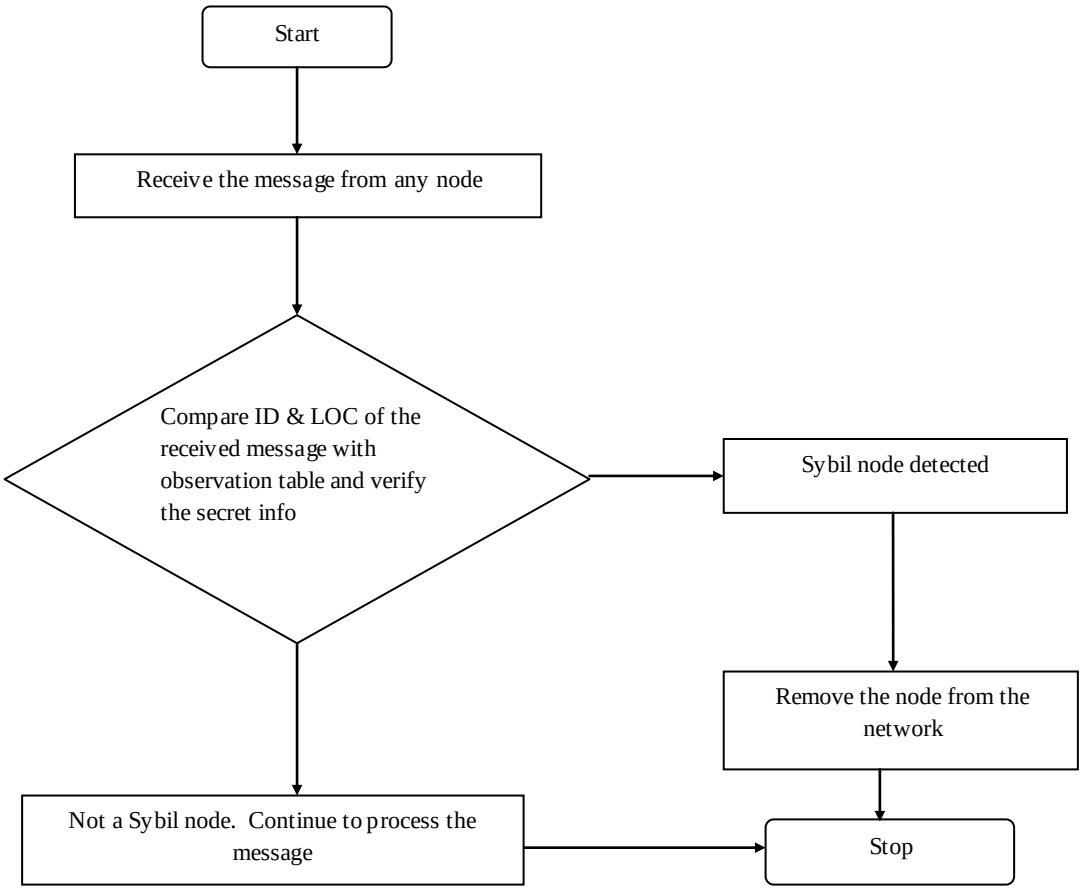

Fig1. System Architecture

D.PROPOSED MODEL

The nodes in the network send the Hello message which contains its ID, Location and secret information, which is generated and distributed by a server during deployment of each and every node to all its neighboring nodes. It is part of registration process. All the nodes which receive the Hello message from the neighboring nodes will maintain an observation table and store node identity, location and the secret information. Next time when a message is received, the observation table entries are compared with the previous information stored in the table. If it matches then it's a normal node else it is a Sybil node. Then the corresponding node and message will be destroyed from the network. In this model, we are using the path tracing algorithm to detect Sybil node in a sensor network. The message is transfer from source to sink using AODV reactive protocol to find the shortest paths. When the message is passed from one node to another node the receiver node will maintain the observation table to store the id and location.

When a sensor node receives the packets from other nodes, it will compare node id and location of that particular node. If the id and location is same then its normal node otherwise it is a Sybil node. If the node is an ordinary node, the received message will be processed further. Otherwise it is deleted and the ode is blocked further from processing.

Step 0: During the node deployment each sensor node gets secret information of size 1 byte which is generated and assigned by a server.

Step 1: Each node sends a Hello Message to all its neighbors. This Hello message contains the information like id, location and secret information.

Step 2: Each and every node maintains an observation table which stores the entries received from the neighboring

nodes. Since all the nodes are static, after deployment, they won't change its location.

Step 3: After this registration process, when a new message is received by any node from any other node, it finds the distance from the traveling time and verifies the id, location and distance. The secret information is extracted from the received message and compared with the available information in the observation table.

Step 4: If the message is received from a Sybil node, every time it will act as different id and so with different secret information. Comparing this information, we can easily find the malicious nodes.

Step 5: If id is different with same Loc and distance or multiple messages, one with unique id and same location is received then the source node is considered as Sybil node. The node is removed from the network.

Step 6: If the malicious node is determined, then received message is discarded otherwise the message will be stored and processed.

The TTM model is frequently executed in the network to find the malicious nodes. This model will find all the malicious nodes because the verification is performed by each and every node when it receives the message. Suppose this verification is done by a Sybil node, the outcome of the verification will not be correct. Some of such Sybil nodes will not be determined by this method.

IV. RESULTS & DISCUSSION

This approach is simulated in NS2 in a sensor network consists of 100 nodes and among this some nodes are Sybil nodes. The TTM model is executed for a number of iterations and the detection rate is taken every time. These data is used to plot the graph. Comparing with existing algorithms detection rate is high but the storage space is little bit high because every sensor node is maintaining an observation table which contains one entry for each neighboring node.

The figure shows the average rate of detection of Sybil attack in existing and proposed system. The comparison shows that when time goes on during the coming iterations the detection rate is high. About 99% of the Sybil nodes were detected. In the existing system the 90% detection rate is achieved in the 25th iteration but the same rate is achieved in the proposed TTM model in the 18th iteration itself.

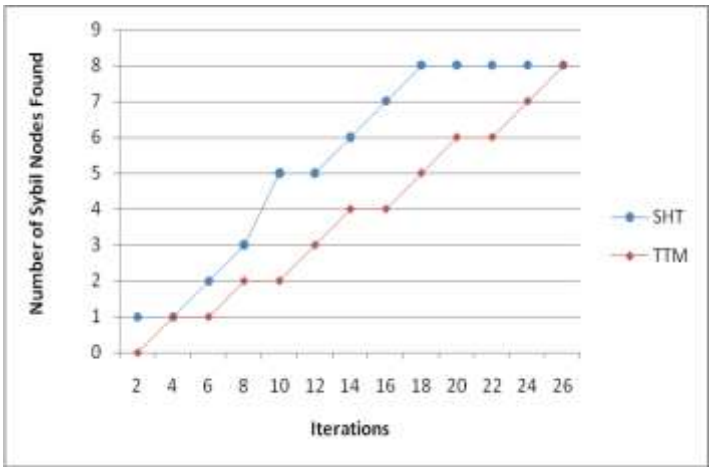

Figure 1 Detection of Sybil Nodes

V. CONCLUSION

The proposed method is detecting the Sybil nodes in a fast manner. Without any special hardware support, this scheme finds the multiple fake identities with high efficiency. To detect the Sybil nodes it uses the identity and location of the each sensor node along with neighboring information and secret information assigned by a server. This method shows 99% detection rate and very less false detection rate. Since every node is maintaining the observation table, at point the Sybil node is exactly determined and blocked from the network. There is not even a 1% of false identification rate, because the network is static and moreover every node is registering themselves to all its neighbors with id, location and secret information.

REFERENCES

[1] Douceur J R "The Sybil attack In:Proc. of First International workshop on Peer-to-peer systems (IPTPS' 02). 7-8March 2002•Cambridg M US Volume 2429 of LNCS 200 25 1 260.

[2] Sajid Hussain and Md Shafayat Rahman, "Using Received Signal Strength Indicator to Detect Node Replacement and Replication Attacks in Wireless Sensor Networks" Proc. SPIE 7344, Data Mining, Intrusion Detection, Information Security and Assurance, and Data Networks Security 2009, 73440G (13 April 2009); doi: 10.1117/12.824207

[3] Kuo -Feng Ssu, Wei-Tong, Wang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information" Computer Networks 53 (2009) 3042–3056.

[4] Bin TIAN, Yizhan YAO, Lei SHI, Shuai SHAO, Zhaohui LIU, Changxing XU, "A NOVEL SYBIL ATTACK DETECTION SCHEME FOR WIRELESS SENSOR NETWORK", Proc. Of IEEE IC-BNMT 2013 978-1-4799-0094-7/13.

[5] Wen Mi, Li hui, Zheng Yanfei, Chen Kefei, "TDOA-based Sybil Attack Detection Scheme for Wireless Sensor Networks", Journal of Shanghai Univesity 12 (1) (208) 66-70.

[6] Vamsi, P.Raghu, Kant, Krishna, "Sybil attack detection using Sequential Hypothesis Testing in Wireless Sensor Networks", Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on 12-13 July 2014.

[7] A.V.Vibi, GV.Padmasree, P.Nithya, C.Geetha, "DETECTION OF SYBIL ATTACK USING NEIGHBOURING NODE MESSANGING USING WIRELESS SENSOR NETWORK", IJATES, Volume No.03, Issue No. 03, March 2015, pg 221-226.

[8] Qinghua Zhang, Raleigh, Wang, P.; Reeves, D.S.; Peng Ning,(2005) "Defending against Sybil attacks in sensor networks", Distributed Computing Systems Workshops. 25th IEEE International Conference, pp 185-191.

[9] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, (2004)"The Sybil Attack in Sensor Networks: Analysis & Defenses", Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium, pp. 259 – 268.

[10] Kuo-Feng Ssu, Wei-Tong Wang, Wen-Chung Chang,(2009) "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information", Computer Networks, Volume 53, Issue 18, 24, Pages 3042-3056.

[11] R. Muraleedharan, X. Ye, L.A. Osadciw, (2008)," Prediction of Sybil attack on WSN using Bayesian network and Swarm intelligence", in: Proceedings of Wireless Sensing and Processing, March 2008.

[12] D.-J. Huang, W.-C. Teng, C.-Y. Wang, H.-Y. Huang, J.M. Hellerstein,(2008)," Clock skew based node identification in wireless sensor networks", in: Proceedings of the IEEE Global Telecommunications Conference, pp. 1–5.