DETECTION OF SYBIL ATTACK USING NEIGHBOURING NODE MESSANGING USING WIRELESS SENSOR NETWORK

A.V.Vibi[1], GV.Padmasree[2], P.Nithya[3], C.Geetha[4]

[1,2,3,4] *CSE Department, RMK Engineering College, (India)*

ABSTRCT

The wireless sensor network is ad hoc network used to monitor and record the physical conditions of the environment. This network is attacked by many attackers like denial of service, wormhole, clone, Sybil etc. Sybil attack is harmful attack which affects the sensor network. It is a malicious device and it takes multiple 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. Each and every node in the sensor network will maintain the observation table for storing node id and location to detect the Sybil node. The simulation results shows that the detection of Sybil attack is high in sensor network and the communication overhead is less compared with other existing algorithms.

Keywords*: *Sybil attack, Wireless sensor network, Security path tracing, Time-To-Time message

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 [4].

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.

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 Smith it represented as John or Alden 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 [5], 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 [6], have proposed scheme in which the node identities are verified simply by analyzing the neighboring node information of each node.

Bin et al [7] 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[8] 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 [9] 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. From this paper we proposed 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.

III.EXISTING MODEL

The sequential testing hypothesis is efficient method to detect the Sybil node in wireless sensor network. In Existing model, two Hypotheses is used to detect Sybil attack .the author used observation and location table and using XOR function detect Sybil node in network. The main disadvantage of this model is, Memory space is more because the observation and location table is maintained by each and every node in wireless sensor network.

IV.PROPOSED MODEL

In this section the network model and methodology explains about the proposed model.

4.1 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 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. We proposed detection of Sybil attackers in static. A static routing table contains information entered manually. However a node maybe replaced or relocated manually in case of node failure in each sensor network.

4.2 Performance Metrics

4.2.1 Set distance between each sensor nodes.

4.2.2 Set specific interval time to send the messages to other nodes.

4.2.3 Create table for each nodes to store id and location.

4.3Path Tracing Algorithm

The nodes in a certain network send the message to all its neighboring nodes. Then the node which receives the message from the neighboring nodes will maintain an observation table for each sender node with its respective node identity and location. The next time when the message is received, the observation table is comparing the previous node identity and location. 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.

4.3.1 In this model, we are using the path tracing algorithm to detect Sybil node in a sensor network.

4.3.2 The message is transfer from source to sink using AODV reactive protocol to find the shortest paths.

4.3.3 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.

4.3.4 Whenever the sensor node receiving the packets from other nodes it will compare node id and location of that particular node. This comparison is made by path tracing algorithm. If the id and location is same then its normal node otherwise it is a Sybil node. So we can detect accurate misbehave node.

4.3.5 If the comparison return true the second message will be deleted else the node contains the corresponding id and location will consider as a Sybil node.

4.3.6 Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

V SIMULATION PARAMETERS AND SYSTEM ARCHITECTURE

5.1Simulation Parameters

Table1

Simulator	Ns-2.35
Examined protocol	Path tracing with TTM
Mac	802.11
Area	1000*1000
Nodes	23
Packet size	64 bytes
Attack	Sybil attack
Maximum connections	25

Simulation time	10min
Bandwidth	200kbps
Antenna	Omni antenna
Queue	Drop tail
Topology	Flat grid

5.2 System Architecture

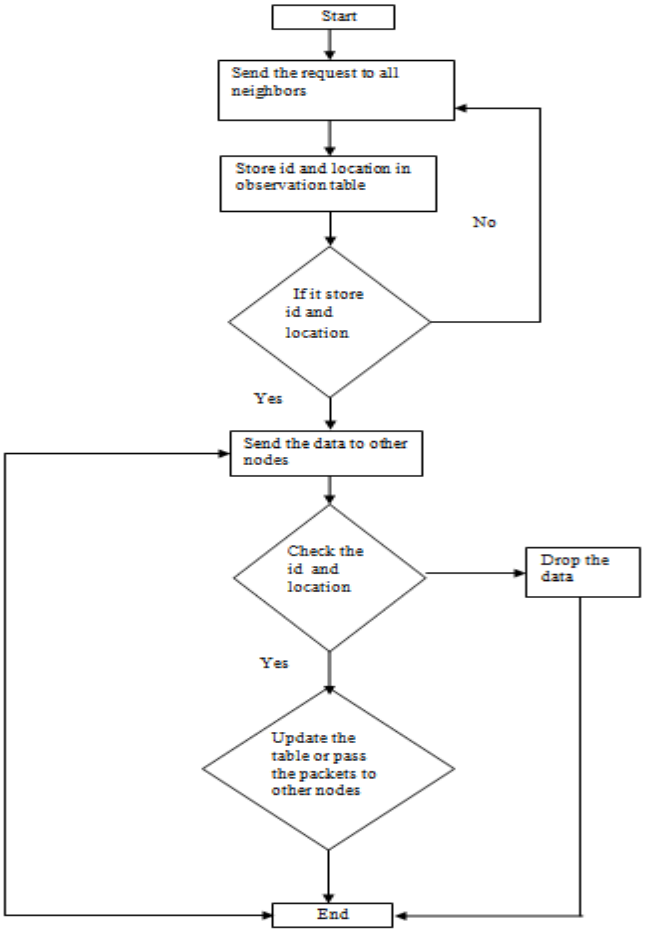

Fig 5.1.System Architecture

VI.SIMULATION STUDY

The approach is simulated in NS2 under 25 nodes to accept the TTM. The average no of samples shows that the packet rate is increased in proposed model compare to existing model. The simulation results shows that the detection of Sybil attack average rate is high in sensor network and the communication overhead is less compared with other existing algorithms.

The fig2 and fig3 shows the average rate of detection of Sybil attack in existing and proposed system. The comparison result is given below,

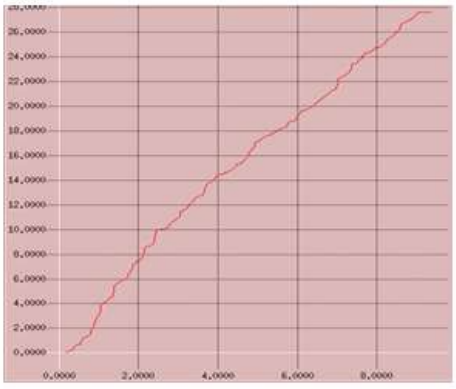

Fig2. S Existing System SHT Average Rate

Fig3. Proposed System TTM Average Rate

VII.CONCLUSION AND FUTRUE WORK

In this paper, time to time message model based technique to detect the Sybil attack has been proposed and applied. In addition, the present model detects the Sybil nodes accurately by using observation table. The simulation results are compared with other existing methods and it shows that TTM approach shows a good efficiency in terms of detection time and speed. The main advantage of this algorithm is while receiving the packets each node store the id and location other nodes to detect the packets.

VIII. ACKNOWLEDGEMENT

We take immense pleasure in thanking our respectable Founder and chairman Thiru.R.S.Munirathnam and vice-chairman Mr.R.M.Kishore for giving us this opportunity.

We express our gratitude to our principal Dr.Elwin Chandra Monie for his whole hearted and kind co-operation.

We are highly thankful to our Head of the Department, professor Dr.K.L.Shunmuganathan who took interest on us and encouraged we throughout the course of study are noteworthy.

REFERENCES

[1 Vijaycuyyuru, Prateekarora & Terrygriffin http://www.powershow.com/view/21ba3-ZmJjZ/Denial_of_Service_DoS_powerpoint_ppt_presentation http://www.cse.unt.edu 28 July 2009

[2] Chris, Karlo , Davidwagner http://web.cs.wpi.edu/~rek/Adv_Nets/Fall2009/Secure_WSN09a.pdf University of California, Berkeley December 01, 2009

[3] Harsh Kishore Mishra M.Tech. Cyber Security Centre for Computer Science & Technology http://www.slideshare.net/HarshMishra3/ieee-80211ac-stanfdePublished on Apr 30, 2008

[4] J.R. Douceur,"The Sybil attack," in Peer-to-peer Systems, pp. 251-260,Springer, 2002.

[5] Sajid Hussain and Md Shafayat Rahman, “Using Received Signal Strength Indicator to Detect Node ReplacementAnd Replication Attacks in Wireless Sensor Networks”,school of computer science, acadia university wolfville, ns, canada b4p 2r6computer networks journal homepage: www.elsevier.com/locate/comnet

[6] kuo-feng ssu , wei-tong wang, wen-chung chang ,”detecting sybil attacks in wireless sensor networks using neighboring information”.department of electrical engineering, national cheng kung university, tainan, taiwan, roc. IEEE icbnmt2013

[7] Bin TIAN, Yizhan YAO, Lei SHI, Shuai SHAO, Zhaohui LIU, Changxing XU "A Novel Sybil Attack Detection Scheme For Wireless Sensor Network"

[8] Wen mi, li hui, zheng yanfei, chen kefei."TDOA-based sybil attack detection scheme forwireless sensor networks" cryptography & information security lab, shanghai jiaotong university, shanghai,

[9] P. Raghu Vamsi and Krishna Kant,"Sybil Attack Detection using Sequential HypothesisTesting in Wireless Sensor Networks", department of computer science and engineering jaypee institute of information technology, noida, india. Paper 2014 IEEE.

[10] H. Wymeersch, J. Lie n, a nd M. Z. Win, "Cooperative localization i nWireless networks", Proceedings of the IEEE, vol. 97, no. 2, pp. 427- 450, 2009.