iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3124

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

A Detecting Mechanism for Sybil Attack in Wireless Sensor Network

Rajeswari. M[1], Sharmila. S[2]
[1]*Assistant Professor, Dept.of Information Technology, Panimalar Institute of Technology*
[2]*UG Scholar, Dept. of Information Technology, Panimalar Institute of Technology*

Abstract: Security has become a most important issue for several significant applications provided by wireless sensor networks (WSNs). The intrinsically susceptible features of WSNs employ them susceptible to a diversity of attacks. This paper has centered on how to protect from a principally destructive type of attack called Sybil attack. A Sybil node using only one physical device may produce an random number of extra node identities and can be used to interrupt standard performance of the WSNs, like multi-hop routing which is utilized to discover numerous disjoint paths among source and destination. Recently, there has been a increasing attention in leveraging WSNs to mitigate Sybil attacks. Digital certificates are a way used to show individuality, however, it is not feasible in sensor networks. This paper has proposed a Trust Based Sybil Detection (TBSD) technique to detect Sybil nodes in WSNs. The TBSD scheme is based on manipulative trust values of adjacent sensor nodes and the nodes with the trust values less than a threshold value are detected as Sybil node [4]. The feasibility of TBSD method is demonstrated systematically, while experimental results of TBSD in exposing Sybil attacks is expansively assessed equally mathematically and numerically. The acquire consequence show that the TBSD attains significant attack detection rate than existing techniques.
Keywords: Trust based Sybil detection; threshold values.

I. INTRODUCTION

WSNs is defined as a self-configured and infrastructure-less wireless networks which is used to monitor environment or physical conditions, such as temperature, sound, wind direction, humidity, pressure, illumination intensity, speed, chemical concentrations, vibration intensity, sound intensity, pollutant levels, power-line voltage, etc. WSNs considerately send the information collected from the sensors to a center position or sink [1].

This information is processed for more processing and to take different decisions. WSNs have limited capacity of processing speed, communication bandwidth, and storage. The WSNs due to limitations are inherently resource constrained and are vulnerable to various attacks.

The inbuilt complexity of the applied security algorithms also adds to the complexity of providing security to WSNs. The proposed security techniques for WSNs in the history supposed that almost all sensor nodes are cooperative as well as trustworthy, but the same is not true for most of the case for various sensor network advantages presently. A large number of attacks has been feasible in WSN which contains tampering, jamming, hello flood, exhausting, wormhole, collision, sinkhole, Sybil, flooding, denial-of-service, cloning etc. .

Sybil attack in WSNs is the important attacks in this malevolent sensor node intentionally and illegally presents many forge or false identities to other sensor nodes. This is done by either creating new (fake) identities or by stealing the legal identities from other sensor nodes. A variety of countermeasures against Sybil attack have been proposed in the literature that we discussed in our previous work [8].

Each of the countermeasures has its own limitations and needed improvement in producing more efficient one. In this paper we identify the Sybil attack, trust based system and related works. In this, we describe our TBSD (Trust Based Sybil Detection) technique for countermeasure against Sybil attack in wireless sensor networks [5]. The proposed scheme is based on calculating trust values of adjacent nodes and the nodes with the trust values less than threshold value are detected as malicious (Sybil) nodes. The proposed technique is designed and implemented in NS-2 tool.

It refers to the Trust Based Sybil Detection (TBSD) technique to detect Sybil nodes in WSNs. The TBSD scheme is based on manipulative trust values of adjacent sensor nodes and the nodes with the trust values less than a threshold value are detected as Sybil node. The feasibility of TBSD method is demonstrated systematically, while experimental results of TBSD in exposing Sybil attacks is expansively assessed equally mathematically and numerically. The acquire consequence show that the TBSD attains significant attack detection rate than existing techniques [6].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

II. LANGUAGE SPECIFICATION

This chapter describes the requirement analysis in accordance with the input and the resources and it also describes the implementation of the project with the technology used. Requirement analysis determines the requirements of a new system. This project also analyze the product and resource requirement, which is required for the successful system. The product requirements includes input and output requirements it gives the needs in term of input to produce the required output. The resource requirements provides brief about the software and hardware that are required to achieve the required functionality.

A. Network Simulator

Network simulator is an object-oriented discrete event simulator. It is a package of tools that simulate of networks. It is primarily UNIX based. It creates topologies of network. It is written in C++ and OTCL languages (TCL scripting with object-oriented extensions). NS is primarily used to simulating local and wide area networks. It will be used to simulate a variety of IP networks. It implements networking protocols such as TCP and UDP, then traffic behaviors such as Telnet, FTP, Web, CBR and VBR, also router queue management mechanism such as RED, Drop Tail and CBQ, routing algorithm which includes Dijkstra, and more. NS also providing implementations for multicasting and some of the MAC layer protocols for LAN simulations. A simplified view of NS2 is shown below in figure 1.

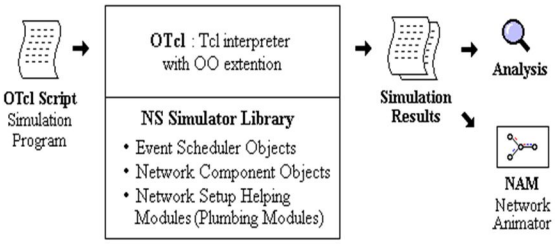


Figure 1. Simplified user view of NS2

NS is Object-oriented TCL (OTCL) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object). In other words, to use NS, you program in OTCL script language. To setup and run a simulation network, a user should write an OTCL script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler[7]. The C++ and OTCL duality is shown below in figure 2.

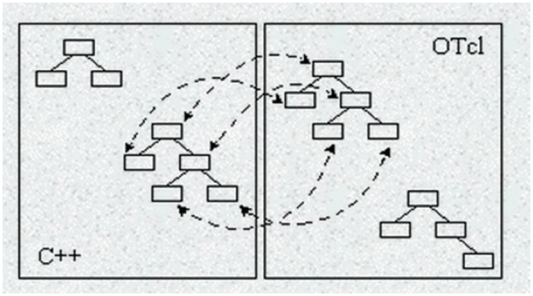


Figure 2.C++ and OTCL- The duality

NS is written not only in OTCL but in C++ also. For efficiency purpose, NS separates the data path implementations from control path implementation. In order to decrease the packet and event processing time (not simulation time), the event schedulers and the basic network component object in the data path are written and compiled using C++. Likewise, an object (not in the data path) can also be entirely implemented in OTCL. Figure.2 show an object hierarchy example in C++ and OTCL.

The event scheduler and most of the network component are implemented using C++ and available at OTCL through an OTCL linkage that is implemented using TCL. The whole concepts together makes NS, which is a Object Oriented extended TCL interpreter with network simulator library. When the simulation is completed, NS produce one or more text-based output files that contain detailed simulation information, if specified to do so in the input TCL (or more specifically, OTCL) script. Figure.3 gives a broad idea about the architecture of NS. This information can also be used for simulation analysis or as an input to a graphical simulation display tool called Network Animator (NAM).

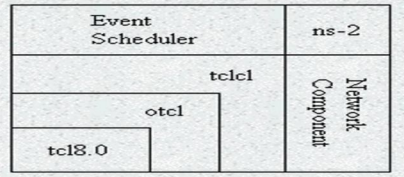


Figure 3. Architectural View of NS

B. Network Animator

NAM is a TCL based animation tool for viewing network simulation traces and real world packet trace data. The design theory behind NAM was to create an animator that is able to read large animation data sets and be extensible enough so that it could be used indifferent network visualization situations. The members of wireless sensor networks are Base Station(BS), Cluster Head (CH), and resource-constrained nodes, which are deployed in a geographical area to perform some special monitoring functions. In most of the applications, especially for large scale deployment, the sensors are arranged in multiple static clusters, as shown in Figure 1. The members' changing makes the authentication and key management always a key research point in wireless network. Considering the resource-constrained essence of WSN, a lightweight scheme is badly needed, which keeps the key changeless to save the limited energy [3]. Many applications, however, require the mobility of network nodes to support.

In a mobile sensor network, there will always be the condition that a node from an existing cluster moves into another cluster dynamically. The separated nodes can be the cluster heads or cluster members. The major reason causing the changes in cluster heads and cluster members will be the mobility. The mobility of nodes together with the transient nature of the wireless media will always leads to a highly dynamic network topology. In this case, security protection with mobile sensors must be incorporated into wireless sensor network. The process when these malicious nodes communicate with their neighboring nodes, by making use of any one of fake identities. This result becomes confusion in the network and it may collapse the entire network. In stolen identities case, the attacker first identifies legitimate existing identities and steal it. This type of Sybil attack may go unidentified in the network in the case of destroying the node whose identity has been stolen.

III. THE PROPOSED SYSTEM

A. Network construction using mesh topology:

In this paper, first we have to construct a network which consists of 'n' number of Nodes. So that the nodes can request data from the other nodes in the network. In a network, nodes are registered with the separate Cluster of network then only select coordinate provides a Node id for each node and also assigns random key pairs with time stamp for all its mobile sensor nodes. Each Network is monitoring for all the Mobile Sensor Nodes [2]. All nodes are sharing their information with each nodes and elects the neighbor node connection establishment using neighborhood forwarding algorithm.

While a legitimate node will faithfully report its neighbors, an attacker will manipulate the list to avoid being detected. For example, a malicious physical device may claim to have a route to an indirect Sybil node so that more traffic will be attracted to it. However, it will not report the Sybil node as its neighbor to the controller. To prevent the 53 manipulation and its impacts on Sybil detection, we require every neighbor list that is transmitted to the controller to be authenticated by the Message Authentication Code (MAC) of the nodes in the list.

The nodes that are not in the list will not be adopted by the neighbors in routing or other network activities. Therefore, a Sybil node cannot be hidden from the controller.

B. Active Nodes For Visualization Approach Using Chord Algorithm

In this module, can verify the Neighbor nodes information of the Requested Node like Predecessor Node Id with key and Successor Node Id with key using Chord Ring Merger Algorithm [9]. These are verifying the Node Id's and Location Id's then we can detect the easy to direct Sybil Node. For this purpose we have to create the List of the Neighbor Nodes information for each node updated to that the Cluster Head Node can verify the each network of the node located.

C. Cluster Head Node Distribution And Verification Of Node Status Using Hashing

Cluster Head node is used for verification process for each network. In our project base station elects the cluster head for trust level value assigned into initial formation then it means first its broadcast trust data manipulate goes to Cluster Head node then only data moves via neighbor cluster head to the base station if one Cluster to another Cluster of network process occurred. So source node

sends all its detail to Cluster Head node like source node id, source node Cluster id, predecessor node id, and successor node id, random key with time stamp, destination node id, and destination node Cluster id with encrypted data (using Hashing). Cluster Head node verifies the details of the source and destination status for secure data transmission.

D. Inner And Outer Nodes Of Network Using False Positives Algorithm

In this module, each node is assigned a key randomly with Time Stamp from Co coordinator node. Then those will also transmit Random key which was generated with respect to that Time Stamp to the Cluster Head node. Cluster Head node will now check the Random number from the distributed hash table which is generated with the node status for active or suspicious nodes. If active nodes of the data's are matched at present global network then the Cluster Head node will confirm that this node is Genuine or not using False Positive or False Negative Algorithm.

WSNs consist of huge numbers of sensor nodes, and since this number is huge, the nodes have to be very cheap[12]. This further implies that they possess very limited power and computation resources, small memory size and limited bandwidth usage. Furthermore, the incorporation of any tamper-resistant hardware would assume unacceptable costs. All of this makes the security of these networks very challenging, as the resource limited devices cannot support the execution of any complicated algorithms.

Moreover, WSNs use a radio band that is license-free, so anybody with appropriate equipment can listen to the communication. Finally, due to their deployment in areas that are difficult to reach makes them prone to node failures and adversaries.

E. Sybil Attack Detection And Data Transfer In Mswn

Only the Cluster Head node confirms the Sender node, the data is send to the Destination, which is genuine using TDMA mechanism. If user specified information and the internal information are varied then the Cluster Head node will identify that attacks or some Mal practice has occurred for too long time period using Event Scheduling Time Advance Algorithm and the Packets are discarded by the Cluster Head node and those attacker or misbehaving nodes are put into the idle mode status.

IV. FUTURE ENHANCEMENT

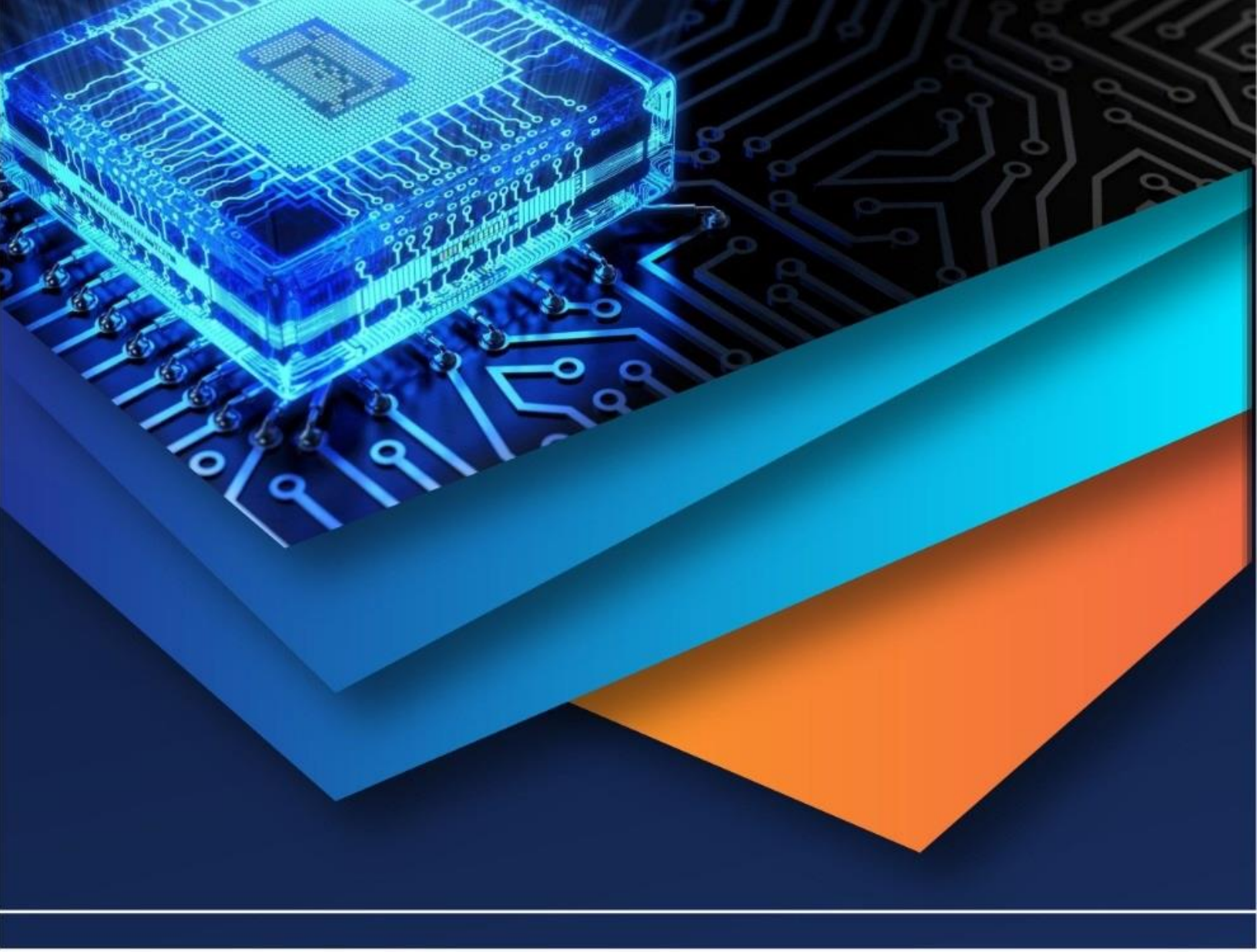
There are number of nodes to be consumed the energy status improved which depends on the network lifetime improvement and detects the node location for filter the same group cluster message harvesting when buffered occurred using localization algorithm and it fetches the unknown node also to outside of the network**.**

V. CONCLUSION

In this paper, we propose an approach for detecting Sybil attack in wireless networks, which is a particular harmful attack for many network functions. This approach concentrates on visualizing, organizing and detecting significant abnormal patterns from network topology information. We have designed security methods to locate suspicious nodes and validate their behaviors using topology geometry information [2]. The results using these intelligent algorithms demonstrate that Sybil Belief performs orders of magnitudes better than existing Sybil classification.

REFERENCES

[1] Rupinder Singh, Jatinder Singh, Ravinder Singh "TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks", IJCSNS 2016.
[2] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in WWW, 2009.
[3] J. R. Douceur,"The Sybil attack," in IPTPS, 2002.
[4] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defenses," in SIGCOMM, 2010
[5] P. L. Fong, "Preventing Sybil attacks by privilege attenuation: A design principle for social network systems," in IEEE S & P, 2011.
[6] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman., "Sybil Guard: Defending against Sybil attacks via social networks," inSIGCOMM,2006.
[7] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time url spam filtering service," in IEEE S & P,2011.
[8] Rupinder Singh, Dr. Jatinder Singh, Dr. Ravinder Singh "Sybil Attack countermeasures in wireless sensor", IJCNWC, ISSN: 2250-3501 Vol.6, No 3, May - June 2016.
[9] Shunli Ding, Xiuhong Zhao, "Analysis and improvement on Chord protocol for structured P2P", Communication Software and Networks (ICCSN) 2011 IEEE 3rd International Conference on, pp. 214-218, 2011.
[10] RezaRafeh and Mozhgan Khodadadi, "Detecting Sybil Nodes in Wireless Sensor Networks using Two-hop Messages," Indian Journal of Science and Technology, Vol. 7(9), 1359–1368, September 2014.
[11] Weichao Wang, Di Pu, and Alex Wyglinski, "Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding," IEEE IIFIP International Conference on Dependable Systems & Networks (DSN), 2010.
[12] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol. 29, No. 3, March 2011.
[13] Philip W. L. Fong, "Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems," IEEE Symposium on Security and Privacy, 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY