Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 11, November 2015, pg.173 – 180

RESEARCH ARTICLE

Lightweight Sybil Attack Detection Technique "An Overview"

Vrushali Kelatkar[1]
P.G Student: Electronics and telecommunication
Alamuri Ratnmala Institute of Engineering and Technology.
Mumbai, India
e-mail: kelatkar.vrushali@gmail.com

Prof. Pravin Dere[2]
Assistant Prof: Electronics and Telecommunication
Terna Engineering College
Nerul, Navi Mumbai, India
e-mail: pravindere@rediffmail.com

Abstract:
A set of mobile nodes which can communicate directly with other nodes within its transmission array and use multihop routing for nodes outside its transmission range is called Mobile Ad hoc Network (MANET). The infrastructure less nature (bandwidth, memory and battery power) of MANET makes it susceptible to various attacks. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions. Since MANETs require a unique discrete and persistent identity per node in order for their security protocols to be workable, Sybil attacks create a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a synchronized attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of responsibility in the network. It is strongly desirable to detect Sybil attacks and eliminate them from the network. This paper proposes a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any additional hardware, such as directional antennae or a geographical positioning system.

Keyword: MANETs, Sybil attack, RSS, Legitimate

I. Introduction

MANET is an autonomous system consists of several nodes. These nodes communicate with each other through wireless links. Due to infrastructure less nature of MANET and as there is no central authority to maintain and control the network makes it vulnerable to various attacks. There is an attack which causes so much destruction to a network Called Sybil attack. In Sybil attack, attackers use several identities at a time or they take-off identity of some trustworthy node present in the network. This attack can create lots of false impression in the network like decrease the trust of legitimate node by using their identities, disturbs the routing of packets so that they cannot reach to its desired destination, and many more. Like this it disturbs the communication among the nodes present in the network. Sybil attack is very much destructive for mobile ad-hoc network. In this paper, we propose the Lightweight Sybil Attack Detection Technique which is used to detect the Sybil nodes in the network.

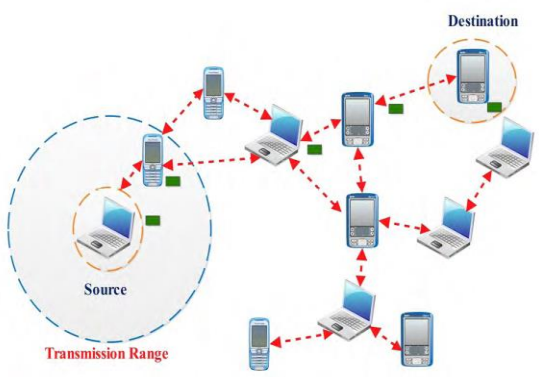

Figure 1: MANETs Example

There are some security goals to check whether MANET is safe or not. These are discussed following:

1. Confidentiality: Some important data is only accessed by authorized authorities. This can protect the nondisclosure data from attackers.
2. Availability: It means all services should be provided to all nodes at proper time. So that they can do secure communication with other nodes present in the network.
3. Integrity: It provides the assurance that data which is transferred from sender to receiver will not be degraded. Receiver receives the same data as it is send by the sender without any modifications.
4. Non repudiation: In this, receivers and senders do not refuse that they didn't get or delivered the data.
5. Authentication: This goal is used to check that participants or nodes which are performing or participating in a network are authenticated or fake.

II. Related Work

Security is vital section of any network. If there is security then only there is a secure communication and good output of network. The work done to remove Sybil attack in MANET is following:

Kanni Selvam, Mr.C. Karthikeyan M.E,(4) in which they sense the Sybil attacker with different transmission power by using lightweight scheme, without using centralized trusted third party or

any extra hardware such as directional antenna and global positioning system. Himika Sharma, Roopali Garg (5), presented Enhanced lightweight Sybil attack detection technique, which is used to detect the Sybil attack, they used three more parameter i.e energy, frequency and latency. In this detection throughput is increased and tool used for simulation is MATLAB. Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat (3) Presented, in this research, a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. P.Kavitha, C.Keerthana, V.Niroja, Vivekanandhan(1), proposed to use passive ad hoc identity technique and key distribution. Detection can be done by a single node, or multiple trusted nodes can join to improve the accurateness of detection. The proposed NDD algorithm-based detection mechanism to Sybil attacks. Use these algorithms to transfer the data in source to destination without any harm or loss as well as each node to have the neighbor's node address. Being subject to on the address the data will be transmitted in to correct endpoint. Roopali Garg, Himika Sharma (6) Proposed To provide more security, two more parameters are used in this method i.e. energy and frequency. In this procedure when node enters a network, then it's all three parameters are checked i.e. speed, energy and frequency and if value of all these parameters are less than threshold value then node is considered as legitimate node else as Sybil node. It improves the performance or throughput of network by 21% than lightweight Sybil attack detection technique and the Simulation tool used for the operation is MATLAB.

III. Lightweight Sybil Attack Detection Technique

This technique is also termed as lightweight as it does not use any extra hardware or antennae for its operation. It is used to detect Sybil Attacks [8].

There are three steps in this process:

1) Types of Sybil nodes: Sybil nodes consist of two types. In the first type it simultaneously use many identities at a time either by deceiving others identities or by crafting its own identities. In the second type it uses only one identity at a time.

2) Threshold value: In this step we assume that normal nodes do not have speed greater than 10m/s. The nodes whose speed is greater than 10m/s are termed as Sybil nodes.

3) Comparison: In this step the RSS (Received Signal Strength) upper bound threshold value is calculated. The upper bound value is calculated as an average of RSS value when nodes are moving at 10m/s speed. When a new node enters in a network then its RSS value is compared with RSS upper bound value. If the value is greater or equal to upper bound RSS value then it is detected as Sybil node.

IV. Existing System

The Sybil attacks will have a serious influence on the normal process of wireless ad hoc networks. It is effectively necessary to detect Sybil attacks and remove them from the network. The traditional approach to avert Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not appropriate for mobile ad hoc networks because it usually requires inflated initial setup and incurs overhead related to maintaining and distributing cryptographic keys.

A. Disadvantage

- Existing approach uses extra hardware to provide security
- Cryptographic techniques consume more resources for computation.
- Reduce the energy level of the mobile node.

V. Proposed System

In Sybil attack, an attacker attains several identities and uses them simultaneously or one by one to attack network operation. Such attacks cause a serious risk to the security of Mobile Ad hoc Networks (MANETs) that require distinctive and unchangeable identity per node for detecting routing misconduct and reliable computation of node's reputation.

A Sybil attacker can either generate more than one identity on a single physical device in order to launch a coordinated attack on the network or can shift identities in order to deteriorate the detection process, hereby promoting lack of responsibility in the network. In this research, we suggest a lightweight scheme to sense the new identities of Sybil attackers without using centralized trusted third party or any additional a hardware, such as directional antenna or a geographical positioning system. According to the previous researches, our projected scheme detects Sybil identities with good accuracy even in the presence of mobility and also the nodes with variable transmission power.

A. Advantages

- The proposed scheme provides security against Sybil attack with less energy consumption.

B. Network Configuration

The mobile nodes in the MANET are supposed to move by using the random way point mobility model. Let be considered that each mobile node using Omni antenna for transmission and reception of signals. The Two ways ground is used as the path loss model in our simulation scenario. The nodes are having the connection with the node switch are present inside its communication range. The AODV routing protocol is used as the routing protocol to route the data packets to the indented terminus.

C. System Architecture and flow chart of Sybil attacker

A method was suggested using the Light weight scheme to confirm the physical identity for avoiding multiple-identity attacks. The multiple-identity attacks usually use a single malicious node to confuse neighbor nodes, causing misperception among them, and finally the entire network is hindered and thus cannot function properly.

In order to sense new identities spawned by a Sybil attacker, the following algorithm checks every received RSS by passing it to the add New RSS function, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been intermingled with before, i.e. it is a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an UB−THRESHOLD (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e., whitewasher). If it is superior than or equal to the threshold, signifying that the new node lies near in the neighborhood and did not enter normally into the neighborhood; the address is added to the malicious node list. Else, the address is added to the RSS table and a link list is created for that address in order to store the newly received RSS along with its time of reception in it. Lastly, the size of the link list is checked, if it is greater than the LIST−SIZE, the oldest RSS is removed from the list.

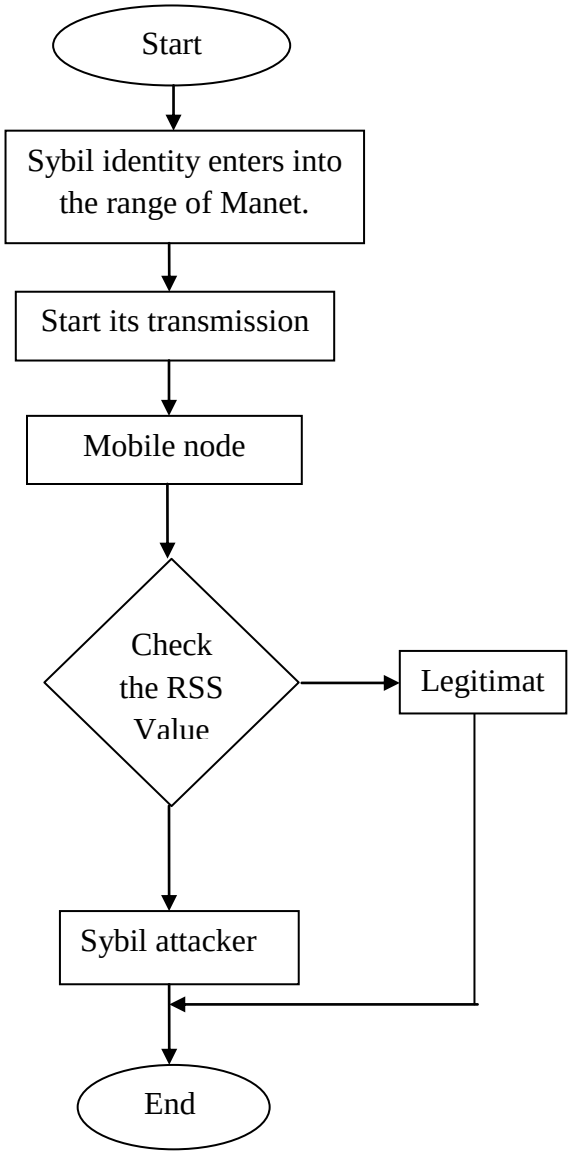

Figure 2: Flow chart

VI. Received Signal Strength Analysis

The distinction between a new legitimate node and a new Sybil identity can be made based on their neighborhood joining conduct. For example, new legitimate nodes become neighbors as soon as they enter inside the radio range of other nodes; hereafter their first RSS at the receiver node will be low enough. In contrast a Sybil attacker, which is already a neighbor, will cause its new identity to appear abruptly in the neighborhood. When the Sybil attacker creates new identity will be high enough to be illustrious from the newly joined neighbor. In order to investigate the difference between a legitimate newcomer and Sybil identity entrance behavior. Each node preserves a list of neighbors in the from <Address,Rss-List<time,rss>>,and records the RSS values of any directly received or overhead frames of 802.11 protocol, i.e. RTS, CTS, DATA, and ACK messages. In other words, each node will capture and store the signal strength of the transmissions received from its neighboring nodes. This can be done when a node either takes part in the communication directly with nodes acting as a source or a destination or when a node does not take part in the

direct communication. In the latter case it will capture the signal strength values of other communicating parties through overhead the control frames. Each Rss- List in front of the corresponding address comprises Rn RSS values of newly received frames along with their time of reception, Tn. where n is the figure of elements in the Rss-List that can be increased or decreased depending upon the memory requirements of a node(3).

Node ID	RSS List
1	R1-T1---R2-T2---R3-T3------R_NT_N
2	
3	: : :
N	

TABLE 1: Neighbor List Based on RSS

A. Sybil Attack

There are two flavors of Sybil attacks. In the first one, an attacker generates new identity while dumping its previously created one, hence only one identity of the attacker is up at a time in the network. This is also known as a join-and –leave or whitewashing attack and the inspiration is to clean out any bad history of malicious activities. This attack potentially encourages lack of accountability in the network. In the second type of Sybil attack, an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack. The motivation of this attack is to cause disturbance in the network or try to increase more resources, information, access etc. than that of a single node deserves in a network

B. Block diagram

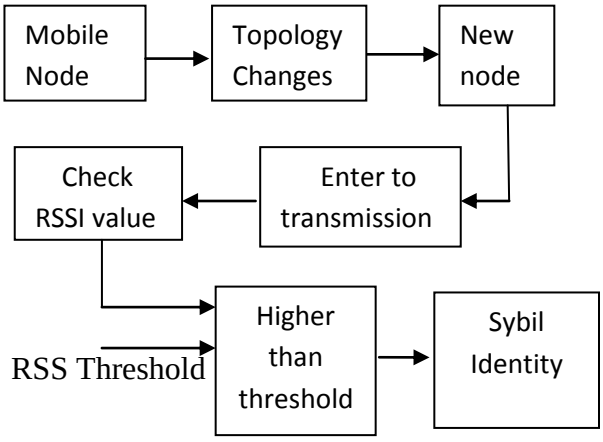

Fig 4.Identification Sybil identity

There may be so much of mobile nodes. To identify the new node the RSSI value is compared with that threshold value. If the RSS value is more than the threshold value the new node is the Sybil node otherwise it is a normal node. Then remove the Sybil path and transfer the data in a

new path. The Network Inter phase layer serves as a hardware interface which is used by mobile node to access the channel.

In this paper, we are going to differentiate the legitimate node with the Sybil attacker node by its Received Signal Strength (RSS) value. The RSS value the transmission contains the transmission power of the node. In this project, we take in account each and every node has the different transmission power in the wireless network. In our project, we are going to differentiate the legitimate node with the Sybil attacker node by its Received Signal Strength (RSS) value. The RSS value the transmission includes the transmission power of the node. In this paper, we consider each and every node has the different transmission power in the wireless network. The RSS and Threshold value of new node is compared with our fixed RSS value. If the new node value is superior than our value, it is a Sybil node otherwise it is a normal node. After the identification of Sybil node eliminates the Sybil path. The significant parameter of proposed systems is packet delivery ratio, packet loss ratio, Bandwidth consumption and energy consumption.

Conclusion

To have safe Communication it is must be safe network. There are various attacks in MANET and there is one attack which is very dangerous called Sybil attack, it uses multiple identities or uses the identity of another node present in the network to disrupt the communication or reduce the trust of legitimate nodes in the network. In this paper we have given RSS based detection mechanism as Lower-bound detection threshold is used and compared with Received Signal Strength (RSS) value, if the comparison is greater than or equal to RSS value, then it's a Sybil identity otherwise it's a legitimate node in the network

REFERENCES

[1] P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan, "Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network" International Journal of Communication and Computer technologies Volume 02 – No.02 Issue: 02 March 2014 ISSN NUMBER: 2278-9723

[2] S.Abbas, M.Merabti, and D.Llewellyn-Jones "Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks" School of Computing and Mathematical Sciences Liverpool John Moores University Byrom St. Liverpool, L3 3AF, UK

[3] Sohail Abbas,Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat Presented "Lightweight Sybil Attack Detection in MANETs". IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013

[4] R. Kanni Selvam , Mr.C.Karthikeyan M.E "Identifing The Sybil Node By Using Lightweight Scheme In Mobile Ad hoc Network" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 5, May 2014

[5] Himika Sharma, Roopali Garg "Enhanced lightweight Sybil attack detection technique" 978-1-4799-4236-7/14/$31.00 2014 © IEEE

[6] Roopali Garg, Himika Sharma "Proposed Lightweight Sybil Attack Detection Technique in MANET" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 5, May 2014

[7]K.Kayalvizhi1,N.Senthilkumar,G.Arulkumaran"Detecting Sybil Attack by Using Received Signal Strength in Mantes" International journals of Innovative research in science and engineering (IJIRSE) (Online) 2347-3207

[8]Roopali Garg, Himika Sharma "Comparison between Sybil Attack Detection Techniques: Lightweight and Robust" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 2, February 2014 Copyright to IJAREEIE www.ijareeie.com 7142

[9] Rakesh G.V, Shanta Rangaswamy, Vinay Hegde , Shoba G "A Survey of Techniques to Defend Against Sybil Attacks in Social Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014 Copyright to IJARCCE www.ijarcce.com 6577
[10] A. Amalorpava Preethi and R. Boopathiraj "Detection of Sybil Attack using Received Signal Strength and Masquerade Attack using Mutual Guarding" International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 11 No. 2 Nov. 2014, pp. 520-526
[11] K.Vaijayanthi, M.Baskar, M.Sc., M.Phil. "Detecting And Resolving The Sybil Attack In Manet Using Rss Algorithm" IJCSMC, Vol. 3, Issue. 11, November 2014, pg.233 – 24.

