ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Comparison between Sybil Attack Detection Techniques: Lightweight and Robust

RoopaliGarg[1],Himika Sharma[2]

Coordinator, Dept. of IT, UIET, PanjabUniversity, Chandigarh, India[1]

PG Student, Dept.of IT, UIET, PanjabUniversity, Chandigarh, India[2]

ABSTRACT: Mobile ad-hoc network (MANET) is an independent network which consists of many nodes and these nodes uses wireless links to communicate with each other. The infrastructure less nature of MANET makes it vulnerable to various attacks. There is an attack which causes many serious threats to the network and it is known as Sybil attack. In Sybil attack, attackers or malicious nodes uses many identities or IP addresses to gain control over the network and creates lots of misconception among nodes present in the network. In this paper two approaches are discussed to detect the Sybil Attack, one is Lightweight Sybil Attack Detection Approach and other is Robust Sybil Attack Detection Approach.

KEYWORDS: MANET-Mobile ad-hoc network, RSS-Received Signal Strength, UB-Upper bound.

I.INTRODUCTION

MANET is a wireless mobile ad-hoc network. Due to its wireless nature it is exposed to several attacks. Among those attacks there is a Sybil attack which very badly ruins the communication among the nodes of the network. The name of the Sybil attack comes from the name of patient i.e. Sybil (Shirley ArdellMarson) who is suffering from multiple disorder personality. The name itself explains the meaning of Sybil attack. Sybil attack is an attack which uses several identities at a time and increases lot of misjudgments among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. Like this, it disturbs the communication among the nodes of the network. To have secure communication it is necessary to eliminate the Sybil nodes from the network [1] [2].

The following goals must be fulfilled by security algorithm used to detect the attack [3]:

1. Authentication:It means that each and every node, participating in communication must be genuine and legitimate node.
2. Availability: All services should be available all the time to all the nodes for the proper functioning and security of the network.
3. Integrity: It gives the assurance that the data received by the receiver will be same as the data send by the sender.
4. Confidentiality: It means that some data is only accessible by the authorized users.
5. Non-repudiation:It means sender and receiver cannot deny that they didn't send or receive the data.

In this paper comparison is done between two approaches i.e. Lightweight and Robust Algorithm which are used to detect the Sybil attack.

II.LIGHTWEIGHT SYBIL ATTACK DETECTION

It is used to detect Sybil nodes. It does not require any extra hardware or antennae to implement it. So its cost is very less [4, 5, 6].

1. Distinct Characters of Sybil Attack: It has two characters, one is Join and Leave or Whitewashing Sybil attack and other is Simultaneous Sybil Attack. In Join and Leave or Whitewashing Attack, at a time, it uses its one identity only and discards

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

all its earlier identities. In this, its main purpose is to remove all its previous malicious tasks performed by it. It also increases the lack of trust in the network. In Simultaneous Sybil Attack, at the same time, it uses all its identities. Its main motive is to create confusion and congestion in the network by utilizing more number of resources and make efforts to collect more information about the network.

2. Enquiry Based on Signal Strength: In this step, each node collects the information about the RSS value of neighboring nodes. On the basis of RSS value, distinction can be made between legitimate and Sybil nodes. If the RSS value of the new node which joins the network is low, then that node is considered as legitimate node otherwise it is considered as Sybil node. Each node saves RSS information about neighbor nodes in the form of

<Address, Rss-List <time, rss>>, as displayed in Table1.

3. Exposure of Sybil Nodes: In this, assumption is made that no legitimate node can have speed greater than 10m/s which is called as threshold value or threshold speed [4]. On the basis of speed, RSS value is calculated and if the RSS values of nodes are greater than or equal to threshold value than those nodes are detected as Sybil nodes otherwise as legitimate nodes.

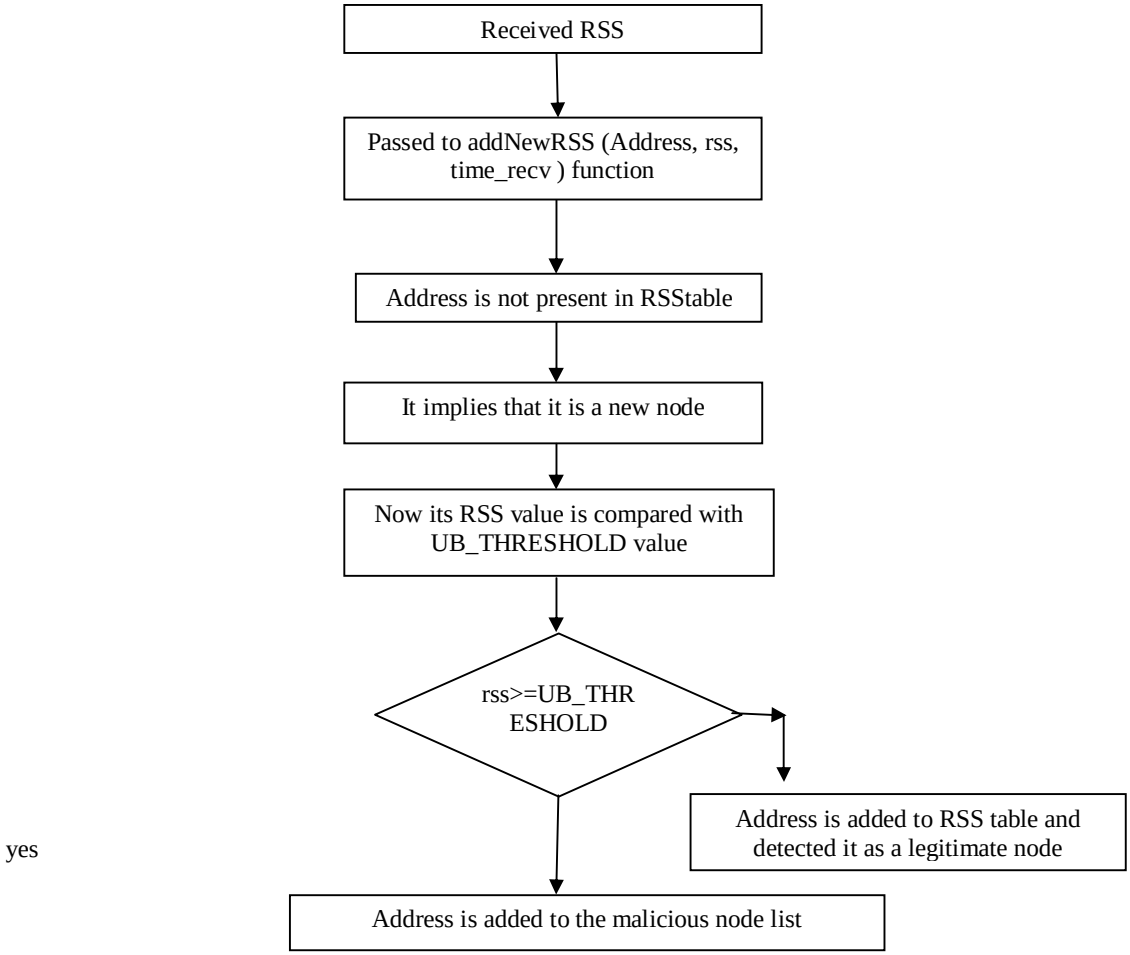

Fig1: Flowchart of Lightweight Sybil Attack Detection Algorithm

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Table1
RSS value of Neighbor nodes.

Node ID	RSS-List
Node 1	R1, T1 → R2, T2 → Rn, Tn
Node 2	
Node 3	
	. . .
Node n	

Explanation of fig1, in this the received RSS value of node is passed to the addNewRSS function and then address of that node is checked that if it present in RSS table or not, if it does not present in RSS table then node is considered as new node. Now RSS value of new node is compared with the upper bound threshold value, if RSS value of new node is greater or equal to upper bound threshold value then it is detected as malicious node otherwise detected as legitimate node.

III. ROBUST SYBIL ATTACK DETECTION

This is another technique used to detect the Sybil nodes. To implement this technique, some methods are required for the correct observation of traffic. These methods are discussed below [7, 8, 9]:

1. Robust Sybil Attack uses the authentication mechanism for the traffic observation. In this, each packet is signed by the sender's private key and also signed by the nodes which are traversed by it to reach the destination and in the end receiver authenticate it by its public key. So, it gives the proof that at what time and location sender sends the packet and in which direction the packet is send by the sender, so that it will reach to the destination.
2. To check the similarity of the path, it uses the novel location based Sybil attack detection mechanism. The nodes whose path is exactly similar to each other are detected as Sybil nodes.

The similarity of the node's path is checked by their overlapping components that how much they are overlapped. The similarity of the path is checked as follows [7]:

$$\text{Sim}(L_1,L_2)=\left(\frac{\sum_{i=1}^{k} T_{bobi}}{\max(T_{obs1},T_{obs2})}\right) * \left(\prod_{i=1}^{j} \frac{T_{coi}}{T_{bobi}}\right)$$

Here L_1, L_2 are nodes

T_{obs1}= It is a duration when each node is observed.

T_{bobi}= It is a duration when both nodes are observed in the observation table.

T_{coi}= It is a duration when both nodes are observed at the same time and they co-exist in same area.

j= It is the number of times when both nodes are observed commonly.

The first part of equation $\left(\frac{\sum_{i=1}^{k} T_{bobi}}{\max(T_{obs1},T_{obs2})}\right)$ is used to calculate that till what time both nodes are observed commonly and second part of equation $\left(\prod_{i=1}^{j} \frac{T_{coi}}{T_{bobi}}\right)$ is used to determine the overlap region of the nodes.

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

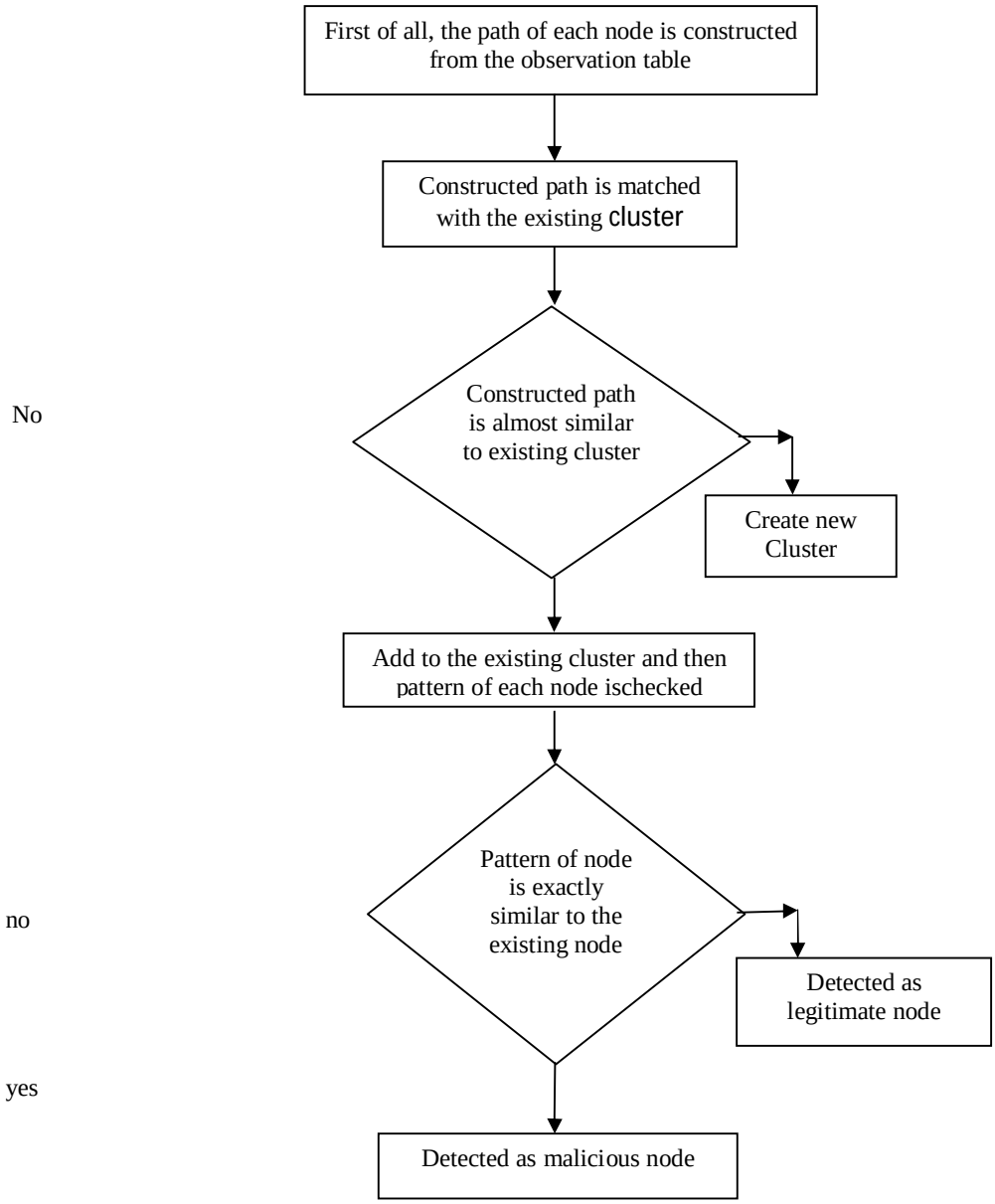

Fig2: Flowchart of Robust Algorithm used to detect the Sybil attack

In fig2, firstly the path of each node is constructed from the observation table and then path of each node is matched with the existing cluster. If path of node is almost similar to the existing cluster then add that node in the existing cluster and if path of node is not matched with any cluster present in the network, then new cluster is created for that node. After this the pattern of each node is checked present in almost similar cluster, the nodes having exactly similar pattern are detected as malicious node otherwise detected as legitimate nodes.

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

IV. COMPARISON

TABLE 2
COMPARISON OF SYBIL ATTACK DETECTION TECHNIQUES: LIGHTWEIGHT AND ROBUST

Algorithm	Parameters	Directional Antennae	Cost	Results*	Summary
Lightweight Sybil Attack Detection Technique	Speed, RSS	Not required	Cheap	90% true positive,10% false negative	The nodes entering in the network with RSS greater than the threshold value are detected as Sybil nodes.
Robust Sybil Attack Detection Technique	Time, Location	Required	Costly	80% true positive,20% false negative	The nodes having exactly the same path or pattern are detected as Sybil nodes

*True Positive: It detect Sybil node as Sybil node.
* False Positive: It detect legitimate node as Sybil node.

V. CONCLUSION

MANET is vulnerable to various attacks due to its infrastructure less or wireless nature. To have safe communication it is must be secure 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 two techniques are discussed i.e. Lightweight Sybil attack detection algorithm and Robust Sybil Attack Detection Algorithm and Comparison is done between these two techniques. In Robust Sybil attack detection technique; there is requirement of directional antennae to check the location of the nodes, so it is costly whereas in Lightweight Sybil attack detection technique there is no requirement of any extra hardware or directional antennae, therefore it is called as lightweight and it is also cheap in cost than robust technique. Parameters used in robust technique are time and location and parameters used in lightweight technique are RSS and speed.Robust technique, 80% detects the Sybil node as Sybil node and 20% detects the legitimate node as Sybil node whereas lightweight technique, 90% detects the Sybil node as Sybil node and 10% detects the legitimate node as Sybil node. So on the basis of comparison Lightweight Sybil attack detection technique is better than the Robust technique.

REFERENCES

[1]Adnan Nadeem and Michael P. Howarth,``A survey of MANET Intrusion Detection & Prevention Approaches for Network layer Attacks," IEEE Communication Surveys & Tutorials, pp.1-19, 2012.

[2] Jin-HeeCho,AnanthramSwami,andIng-Ray Chen,``A Survey on Trust Management for Mobile Ad Hoc Networks for Mobile Ad-Hoc Networks," IEEE Communication Surveys & Tutorials, Vol.13, No.4, pp.562-583, 2011.

[3] LoayAbusalah,AshfaqKhokar,and Mohsen Guizani,``A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE Communication Surveys & Tutorials, Vol.10, No.4, pp.78-93, 2008.

[4] Sohail Abbas, MadjidMerabti, David Llewellyn-Jones, and KasifKhifayat,``Lightweight Sybil Attack in MANETs," IEEE System Journal , Vol.7, No.2, pp.236-248, June 2013.

[5] J. R. Douceur,``The Sybil Attack," presented at the Revised Papers from the first Int. Workshop on Peer-to-Peer Systems, pp.251-260, 2002

[6] J. Wang, G. Yang, Y. Sun and S. ChenSyil Attack Detection Based on RSSI for Wireless Sensor Network " In Proc. WiCom, Sept, 2007.

[7]AthichartTangpong, George Kesidis, Hung-yuanHsu,AliHurson,``Robust Sybil Detection for MANETs "In proc. Of 18th International Conference on Computer Communications and Networks: IEEE, pp.1-6, 2009.

ISSN (Print) : 2320-3765
ISSN (Online): 2278-8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

[8] T.Zhou, R. R. Choudhury, P. Ning and K. Chakrabarty``Privacy –Preserving detection of Sybil attacks in vehicular ad hoc networks " In Proc. MobiQuitous, Philadelphia, 2007.

[9] C Piro, C. Shields, and B. N. Levine ``Detecting the Sybil attack in mobile ad hoc networks " In Proc. IEEE/ACM Secure Comm, August, 2006.

[10]IETF Mobile Ad-hoc Networks Group (MANET), IETF website www.ietf.org/dyn/wg/charter/manet-charter.html.

BIOGRAPHY

Roopali Garg is Coordinator of department of Information Technology Engineering at UIET, Panjab University, Chandigarh. She has an experience of 10 years in academics. She has done M. tech in Electronics and B. Tech in Electronice& Electrical Communication from Punjab Engineering College. She has been awarded Administrator's Gold medal by Chandigarh Administration in 2000 for her supreme performance in curricular, co- curricular and extra-curricular activities. There are more than twenty research papers to her credit which have been published in good indexed international journals and presented in reputed international conferences. Her focussed research area is Wireless communication and has guided more than a dozen M. thesis in this area.

HimikaSharma is a Research Scholar of department of Information Technology at UIET, Panjab University, Chandigarh. She is pursuing her M.E. in Information and technology from UIET, Panjab University, Chandigarh and has done her B.Tech in Computer Science from Punjab Technical University. Her main research interests are in ad hoc networks and wireless networks and currently involves improvement of security in Mobile Ad hoc Networks.