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 5, May 2014

Proposed Lightweight Sybil Attack Detection Technique in MANET

Roopali Garg[1], Himika Sharma[2]

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

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

ABSTRACT: 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 misinterpretation 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 disturb the communication among the nodes present in the network. Sybil attack is very much destructive for mobile ad-hoc network. In this research, we implemented the Lightweight Sybil Attack Detection technique which is used to detect the Sybil nodes in the network and also discussed the proposed work with implementation which is used to improve the existing Lightweight technique. Simulation tool used for the implementation is MATLAB.

KEYWORDS:MANET: Mobile Ad hoc Network, DCA: Distributed Certificate authority, RSS: Received Signal Strength, UB: Upper bound

I.INTRODUCTION

MANET is an autonomous system consists of numerous 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 [1] [2]. In Sybil attack attackers spoof the identities of other nodes or create its own identity. Like this it creates false relation with other nodes and decreases the trust of legitimate nodes present in the network. It does not allow the packets to reach its destination, misuse the information which it get from legitimate nodes and many more damages which it cause to a network. It has a great effect on normal functioning of the network. So it is very much necessary to eradicate this attack from the network.

There are some security goals to check whether MANET is safe or not [3]. These are discussed following:

1. 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.
2. Confidentiality: Some important data is only accessed by authorized authorities. This can protect the non-disclosure data from attackers.
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 important part of any network. If there is security then only there is secure communication and good output of network. The work done to remove Sybil attack in MANET is following:

Piro et al. [4] proposed a scheme to detect the Sybil nodes by examine the behaviour of nodes. According to this scheme, the nodes which move freely, independently in different directions are considered as legitimate nodes and the nodes which moves together are suspected as Sybil nodes and it keeps observing these suspected nodes. This scheme gives high false positives results when group of nodes move in same direction. In [4] [5] two approaches are discussed to detect the Sybil attacks. First is proactive approach which includes economic incentives [6] [7] and pre key distribution [8] [9] techniques. Second is reactive approach which is based on testing of resources and location of nodes.

J. Newsome et al. [10] proposed a scheme in which radio resource testing and randomly pre key distribution is done to detect the Sybil nodes.

In [11] [12] authors proposed DCA scheme. In this scheme, certificates are distributed to all nodes present in the network and nodes use these certificates as a proof of their identities. It helps to prevent the Sybil attacks.AthichartTangpong et al. [13] proposed a technique known as Robust Sybil attack detection technique. In this technique the behaviour of the nodes are examined. The nodes having the similar path are detected as the Sybil nodes.Hongbo Zhou [14] proposed a secure prophet address allocation scheme. In this scheme unique address is distributed to all nodes present in the network. If some new node enters a network, then unique address is provided to that node which does not match with address of any node present in the network. This helps to prevent the Sybil attack.

III.LIGHTWEIGHT SYBIL ATTACK DETECTION TECHNIQUE

This technique is known as lightweight as it does not use any extra hardware or antennae for its implementation. It is used to detect Sybil Attacks [15].

It includes three steps:

1) Types of Sybil nodes: There are two types of Sybil nodes. In first type it simultaneously use many identities at a time either by spoofing others identities or by creating its own identities. In second type it uses one identity at a time.
2) Threshold value: In this authors supposed that normal nodes do not have speed greater than 10m/s. The nodes whose speed is greater than 10m/s are detected as Sybil nodes.
3) Comparison: In this RSS (Received Signal Strength) upper bound threshold value is calculated. The upper bound value is calculated as average of RSS value when nodes are moving at 10m/s speed. When new node enters in a network then its RSS value is compared with RSS upper bound value, if it is greater or equal to upper bound RSS value then it is detected as Sybil node.

```
Algorithm 1:
1) Set Threshold Value of Speed = 10m/s.
2) Calculate RSS UB_THRESHOLD value
3) Address of the node is checked in table.
4) Node address is not present in table
   THEN
   If RSS (node)>= RSS UB_THRESHOLD
          {
            Add it into malicious list
          }
     Else
          {
            Add its address in table of legitimate nodes
          }
   End
```

In Algorithm1, First of all network is created which consists of nodes. Then the threshold value of speed is set to 10m/s. The nodes moving with speed greater than 10m/s are considered as Sybil nodes otherwise as legitimate nodes. After this RSS upper bound threshold value is calculated and it is calculated by taking average of RSS values of nodes which are moving at speed of 10m/s. When some node enters in a network then its address is checked in the table that whether it is present in the table or not. If it is not present in the table then its RSS value is compared against RSS upper bound value. If its RSS value is greater or equal to upper bound value then it is considered as Sybil node otherwise as legitimate node.

IV.PROPOSED LIGHTWEIGHT SYBIL ATTACK DETECTION TECHNIQUE

It is the improved version of Lightweight Sybil Attack detection technique. In above lightweight technique, sometimes there is Sybil nodes whose speed is less than 10m/s and these nodes are detected as legitimate nodes. To remove this drawback of above technique, it is modified. In above lightweight technique only one parameter is used i.e. speed. Here we added two more parameter i.e. energy and frequency. By using these two parameters it is giving better results than previous. In this threshold value of speed is taken as same i.e.10m/s and threshold value of energy and frequency are set as average energy of network and average frequency of network.

```
Algorithm 2:
1)  Set threshold value of Speed= 10m/s
2)  Set threshold value of Energy= avg_energy of network.
3)  Set threshold value of Frequency= avg_frequency of network.
4)  Node enters in a network.
5)  Node address is checked in table.
6)  Address is not present in table
    Then
          If node speed>= 10 | node energy >=avg_energy of network | node frequency >= avg_frequency of network
             {
              Add address of node in malicious list
             }
            Else
             {
    Add address of node in malicious list
    }
          End
```

In Algorithm2 three parameters are taken i.e. Speed, energy and frequency. Threshold value of speed is set to 10m/s whereas threshold value of energy is set to average energy of network and threshold value of frequency is set to average frequency of network. In this, if new node enters a network then its Speed, Energy and frequency value should be less than threshold value, only then that node is considered as legitimate node otherwise as Sybil node. When node enters in a network, firstly it is checked whether its address is present in the table or not. If it is not present in the table then its Speed, Energy and frequency parameters values are checked. And if Speed, Energy and frequency parameters values are less than threshold values then it is considered as legitimate node otherwise as Sybil node.

V. RESULT AND DISCUSSION

The simulation tool used for implementation is MATLAB R2010a. In this we implemented the proposed lightweight Sybil attack detection technique i.e.Algorithm2 by using parameters mentioned in Table 1 and also used energy and frequency parameters.

Parameters used for performance measurement are following:

1. Throughput: It is calculated as ratio of delivered packets to total number of sent packets.
2. BER (Bit error rate): BER is calculated as number of bit errors divided by total number of bits sends by sender.

Table 1: Simulation Parameters

Parameters	**Level**
Area	1000*1000
Speed	2 to 16 m/s
Pause Time	4s
Radio Propagation model	First order radio model
Number of nodes	100
Data Packets	100

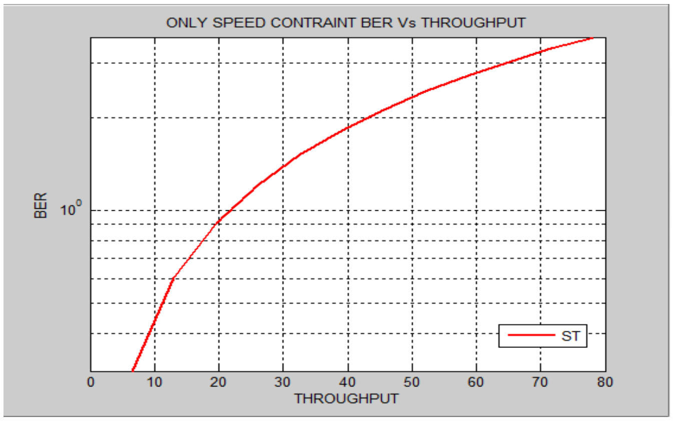

Fig1: BER vs Throughput (only speed parameter)

ST: Speed throughput

In Fig1 graph is plot between BER vs Throughput, when only speed parameter is used. Threshold value of speed parameter is set to 10m/s.When BER= $10^{0.5599}$ then throughput is coming 78.22.

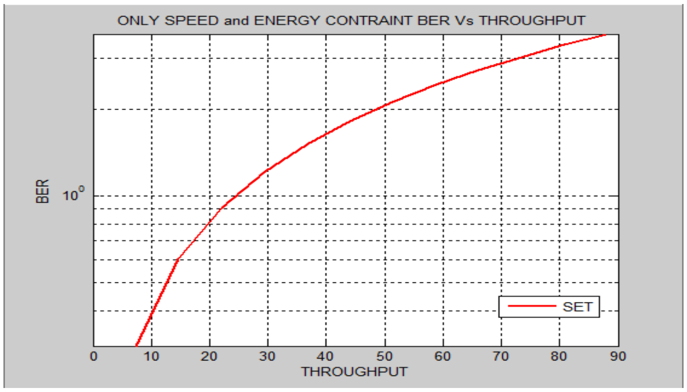

Fig2: BER vs Throughput (Speed and energy parameters)

SET: Speed Energy Throughput

In Fig2 graph is plot between BER vs Throughput when two parameters are used i.e. Speed and energy. Threshold value of speed is set to 10m/s and of energy is set to average energy of network. In this graph when BER= $10^{0.5599}$ then throughput= 88.12. By using one more parameter i.e. energy, performance or throughput is improved by 12.65% with respect to fig 1 in which only speed parameter is used.

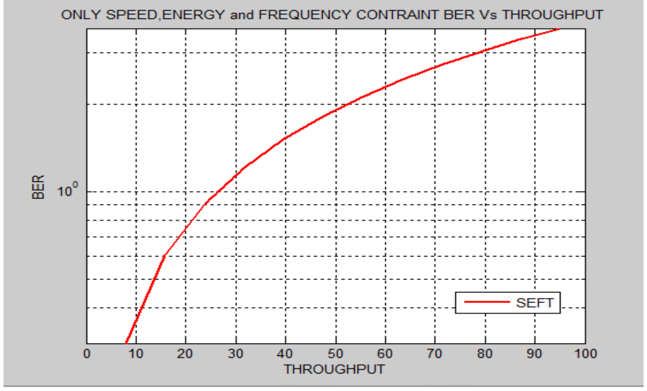

Fig3: BER vs Throughput (Speed, energy and frequency parameters)

SEFT: Speed Energy Frequency Throughput

In Fig3 graph is plot between BER vs throughput when three parameters are taken i.e. speed, energy and frequency.In this, when BER is $10^{0.5599}$ then throughput is coming 95.05. When three parameters are used then performance is improved by 21% with respect to Lightweight Sybil attack technique where only one parameter is used i.e. speed.It shows that by increasing the constraints i.e. parameters, the number of malicious nodes decreasein the network. As a result network security increases.

VI.CONCLUSION

In lightweight Sybil attack detection technique only one parameter speed is used to detect the malicious node but sometimes there is Sybil nodes whose speed is less than 10m/s are also detected as legitimate nodes. To provide more security, technique is proposed in which two more parameters are used i.e. energy and frequency. In proposed technique 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 otherwise as Sybil node. It improves the performance or throughput of network by 21% than lightweight Sybil attack detection 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] Roopaligarg andHimika Sharma, “Comparison between Sybil Attack Detection Technique: Lightweight and Robust,” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol.3, issue.2, pp.7142-7147, February, 2014.

[4] C. Piro, C. Shields, and B. N. Levine, “Detecting the Sybil attack in mobile ad hoc networks,” in ProcSecurecomm Workshops, pp.1–11,2006.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks : Analysis &defenses. In Proc. IPSN’04, Berkeley, Apr. 2004.

[6] N. Margolin and B. Levine. Informant: Detecting sybils using incentives.Financial Cryptography, Feb. 2007.

[7] N. B. Margolin and B. N. Levine. Quantifying sybil attacks againstnetwork applications. Technical Report 67, Dept. of Com. Sci., U. Mass-Amherst, Dec. 2005.

[8] P. Traynor, H. Choi, G. Cao, S. Zhu, and T. La Porta.Establishing pair-wise keys in heterogeneous sensor networks. In Proc. IEEE INFOCOM,Apr, 2006.

[9] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning.Defending against Sybil attacks in sensor networks.In Proc. IEEE ICDCS, June 2005.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis &defenses," in Proceedings of the third international symposium on Information processing in sensor networks. Berkeley, California, USA: ACM, 2004.

[11] SaroshHashmi, John Brooke,``Towards Sybil Resistant Authentication in Mobile Ad-hoc Networks “FourthInternational Conference on Emerging Security Information,System and Technologies, pp.17-24, 2010.

[12] SaroshHashmi, John Brooke,``Authentication Mechanisms for Mobile Ad-hoc Networks and Resistance to Sybil Attack " The Second International Conference on Emerging Security Information,System and Technologies, pp.120-126, 2008.

[13] AthichartTangpong, George Kesidis, Hung-yuanHsu,AliHurson,``Robust Sybil Detection for MANETs " IEEE, 2009.

[14]HongboZhuo,``Secure Prophet Address Allocation for Mobile Ad-hoc Networks" IFIP International Conference on Network and Parallel Computing, pp.60-67, 2008.

[15] 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

BIOGRAPHY

RoopaliGargisCoordinatorofdepartmentofInformationTechnologyEngineeringatUIET, Panjab University, Chandigarh. She has an experience of 10years in academics. She has done M. Tech in Electronics and B.Tech in Electronics &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 inreputed international conferences. Her focussed research area is Wireless communication and has guide more than a doze nM. The sis 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 adhoc networks and wireless networks and currently involves improvement to fsecurity in Mobile Adhoc Network.