ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Discovering Sybil and Masquerading Attack Using Received Signal Strength of Nodes in MANET

Sivakumar B[1], Gracy Theresa W[2]

PG scholar, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, Krishnagiri (Dist), Tamilnadu, India[1]

Assistant Professor, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, Krishnagiri (Dist), Tamilnadu, India[2]

Abstract: Mobile ad hoc Networks (MANETs) is an autonomous assortment of mobile nodes that type form network with none existing network infrastructure or central access point. Since MANETs need a novel, distinct, and protracted identity per node so as for his or her security protocols to be viable, Sybil attacks cause a heavy threat to such networks. Sybil attacker will lawlessly claim multiple identities on single node and violate one-to-one mapping. Masquerading is an active attack where one node pretends to be another and giving false impersonation. Here by using RSS (Received Signal Strength) of nodes to find Sybil and masquerading identities on network with good accuracy even in the presence of mobility. This scheme detect Sybil identities while not exploitation centralized trusty third party or any further hardware, like directional antennae or a geographical positioning system.

Keywords: Mobile Ad hoc Networks (MANET), Received Signal Strength, Sybil Attack, Masquerading Attack, Security.

I. INTRODUCTION

MANETs is a self organized assortment of mobile nodes that kind a dynamic topology with none fastened infrastructure. Communication on Manet supported distinctive identity of every mobile nodes that forms the one to one mapping between associate identity and an entity which is sometimes assumed either implicitly or expressly by several protocol mechanisms; thus two identities implies two distinct nodes. however the malicious nodes will illegitimately claim multiple identities and violate this matched mapping of identity and entity philosophy.

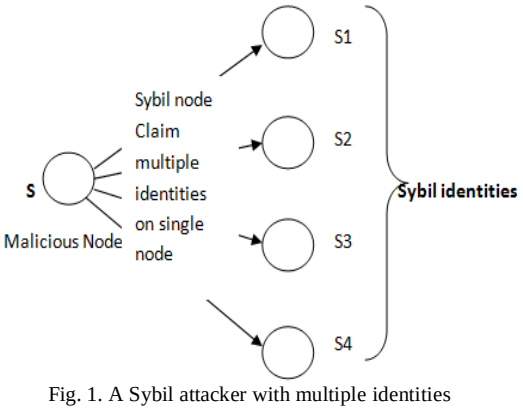

Fig. 1. A Sybil attacker with multiple identities

Figure 1 represents a malicious node S together with its four Sybil nodes (S1, S2, S3 and S4). If this malicious node communicates with any legitimate node by presenting all its identities, the legitimate node can have illusion that it's communicated with five totally different nodes. In actual, there exists just one physical node with multiple totally different Ids Masquerading attack is active attack during which user of the system lawlessly spoof the identity of another legitimate user [2]. Masquerade attacks will occur in many alternative ways. normally terms, a masquer might get access to a legitimate user's account either by stealing a victim's credentials, or through a possibility in and installation of keylogger. In either case, the user's identity is illegitimately noninheritable[13]. In MANETs communication supported distinctive id this sort of attacks are giving serious threat to network here by utilizing the Received Signal Strength of nodes to spot the Malicious nodes.

II. RELATED WORK

Levine et al. [4] surveyed countermeasures against Sybil attacks and categorised these techniques as follows.

Trusted Certification: it's thought-about to be one among a decent preventive resolution for Sybil attacks [3] during which a centralized authority is utilized for establishing a Sybil-free domain of identities. every entity within the network is guaranteed to one identity certificate [6]. However, trusty certification suffers from expensive initial setup, lack of quantifiability and a single point of attack or failure.

Resource Testing: during this approach [5], numerous tasks are distributed to any or all identities of the network so as to check the resources of each node and to work out whether or not each freelance node has spare resources to accomplish these tasks. These tests are disbursed to visualize the computational ability, storage ability and network information measure of a node. A Sybil attack won't possess a spare quantity of resources to perform the extra tests obligatory on every Sybil identity. the drawback of this approach is that an aggressor will get enough

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

hardware resources, like storage, memory, and network cards to accomplish these tasks.

Piro et al. [8] projected to find Sybil identities by observant node dynamics. Nodes are keeping track of identities that are usually seen along (Sybil identities) as opposition the honest distinct nodes that move freely in several directions. However, the scheme can manufacture high false positives wherever node density is high, such as a conference hall or nodes moves in an exceedingly same direction, like a bunch of soldier moving toward a target.

Abbas, M. Merabti et al. [11] reputation based schemes to find Whitewashing attack. A inconsiderate node will simply escape the implications of no matter misdeed it's performed by merely ever-changing identity to clear all its dangerous history, referred to as whitewashing

B. N. Levine et al. [4] Use the revenant price and charges approach this method may be a variation of the conventional resource testing, and might limit the amount of Sybil nodes an aggressor, with unnatural resources, will introduce in an exceedingly amount of your time. Charging a revenant fee for every participating identity is simpler as a deterrence against Sybil attacks.

Yingying chen et al. [9] as a result of the shared nature of the wireless medium, attackers will gather helpful identity information throughout passive observation and additional utilize the identity information to launch identity-based attacks. during this by exploitation the physical properties related to wireless transmissions to discover identity-based attacks. specifically, utilize the received signal strength (RSS) measured across a group of landmarks (i.e., reference points with better-known locations) to perform detection of identity-based attacks.

Capkun et al. [7] quality of nodes in a very wireless network are often accustomed discover and determine nodes that area unit a part of a Sybil attack. this accept the very fact that whereas individual nodes are unengaged to move severally, all identities of one Sybil attacker area unit certain to one physical node and should move along. The individual nodes that want to discover Sybil attackers monitor all transmissions they receive over several time intervals. These intervals area unit chosen long enough to capture behavior from all the Sybil identities of associate attacker, together with information transmissions, hello and keep alive messages, and routing requests and replies. The node keeps track of the various identities detected throughout the interval. By created several observations, the node analyze the information to search out identities that seem along usually which seem apart seldom. These identities are Comprise as Sybil attack.

Mohamed salah Bouassida et al. [10] Sybil detection approach, supported received signal strength variations, permitting a node to verify the credibility of different communication nodes, in step with their localizations. this system permits detecting malicious and Sybil nodes at intervals VANET by exploitation received signal strength variations, localization verification and nodes distinguishability degree analysis. Geometrical analysis, that an attacker mustn't increase its causing power. Then, by in turn measurement the received signal strength variations, will get an estimation of relative nodes localization.

III. PROPOSED WORK

It is used to detect Sybil nodes. It doesn't need any further hardware or antennae to implement it. thus it's referred as light-weight Sybil attack Detection. [12].

1. Distinct Characters of Sybil Attack: it's two characters, one is be a part of and Leave or Whitewashing Sybil attack and different is simultaneous Sybil Attack. In be a part of and Leave or Whitewashing Attack, at a time, it uses its one identity solely and discards all its earlier identities. In this, its main purpose is to remove all its previous malicious tasks performed by it. It conjointly will increase the lack of trust within the network. In simultaneous Sybil Attack, at identical time, it uses all its identities. Its main motive is create confusion and congestion within the network by utilizing additional range of resources and make efforts to gather additional info concerning the network.

2. Enquiry supported Signal Strength: during this step, every node collects the knowledge concerning the RSS value of neighboring nodes. On the idea of RSS value, distinction are often created between legitimate and Sybil nodes. If the RSS value of the new node that joins the network is low, then that node thought-about|is taken into account} as legitimate node otherwise it's considered as Sybil node. every node saves RSS information concerning neighbour nodes within the kind of

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

Table 1
RSS values of Neighbor nodes

Node ID	RSS List
Node 1	R1,T1 → R2,T2 → R3,T3 Rn,Tn
Node 2	
Node 3	
Node n	

3. Exposure of Sybil Nodes: during this, assumption is formed that no legitimate node will have speed larger than 10m/s that is termed as threshold value or threshold speed [4]. On the idea of speed, RSS value is calculated and if the RSS values of nodes are larger than or up to threshold value than those nodes are detected as Sybil nodes otherwise as legitimate nodes.

4. we logically partition the radio range of node A into two zones: a gray zone and a white zone as shown in figure 2.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

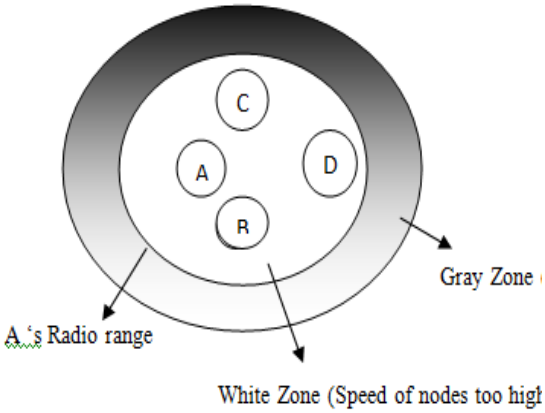

Fig. 2. Categorization of Radio Range

5. Node A can build a decision supported the RSS values of the nodes. If the primary RSS value captured is bigger than the threshold, i.e., a node is within the white zone, A can deem that identity as a brand new identity from a Sybil attacker, since no node will penetrate into white zone among the desired speed. If the primary RSS value received is a smaller amount than the threshold, i.e., a node is within the gray zone, it'll be thought of as a normal new entrant and can be more to the neighbor list.

It is necessary to regulate the dimensions of Table I, otherwise it might grow indefinitely. so as to regulate its size, the unused records need to be deleted. These unused records are as a result of certain reasons. First, when a malicious node changes its identity, its previous identity record stays within the RSS table. Second, nodes be a part of and leave the network at any time; therefore nodes that depart from the network, leave behind a record of their RSS histories. so as to regulate the dimensions, a global timer, referred to as RSS−TIMEOUT shown in algorithmic rule a pair of, is maintained to flush the spare records. once this timer expires, the rssTableCheck operate is called, that checks the time of the last received RSS against the TIME−THRESHOLD for each address of the RSS table. If the time obtained is bigger than this threshold, indicates that it's enough time past since it's not detected from this node.

RSS Finding Method

```
doublefindRSS(doublePt, doubleGt, double Gr, doubleht,
doublehr,
 double L, double d, double lambda)
{
/*
        * if d <crossover_dist, use free space model
        * if d >= crossover_dist, use two ray model
        * Two-ray ground reflection model.

                        Pt * Gt * Gr * (ht^2 * hr^2)
        Pr = ----------------------------------------
                        Assume L = 1.
        To be consistant with the free space equation,
L is added here.
        */
        doublePr;  // received power
        doublecrossover_dist = (4 * M_PI * ht * hr) /
lambda;
if (d <crossover_dist)
        {
                Pr = freespace(Pt, Gt, Gr, lambda,
L, d);
        }
        else
        {
Pr = Pt * Gt * Gr * (hr * hr * ht * ht) / (d * d * d *  d * L);
        }       returnPr; // It is returning the power
}
```

Here the detection of malicious node based on the RSS values that is calculated by using the Signal power Pr. Its based on Transmit power Pt, Transmit antenna gain Gt, Received antenna gain Gr, Transmit antenna height Ht, Received antenna height Hr and Received threshold lambda L.

IV. RESULT AND IMPLEMENTATION

In this entire scenario is simulated using JIST/SWANS (Java in Simulation Time/ Scalable Wireless Network Simulator). Here taken number of nodes as 50 and each of the nodes are connected with certain radio range while the nodes are communicating each entry is updated in the routing table. The messages send from source to destination via intermediate neighbour nodes by utilizing the RSS of nodes to detect the Sybil node with good accuracy even in the presence of mobility.

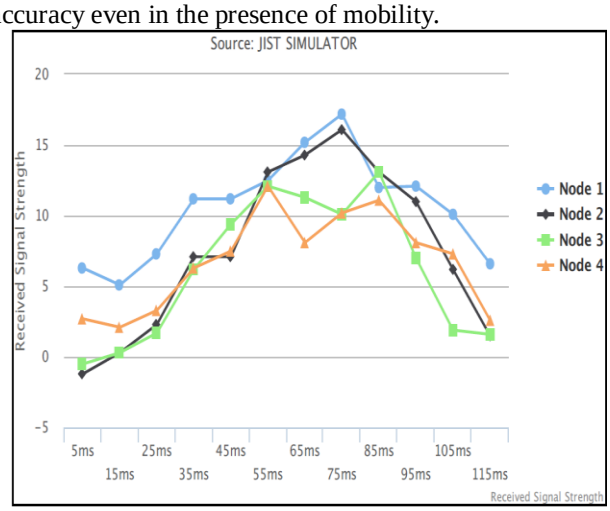

Fig.3. Received Signal Strength of nodes without Sybil identities

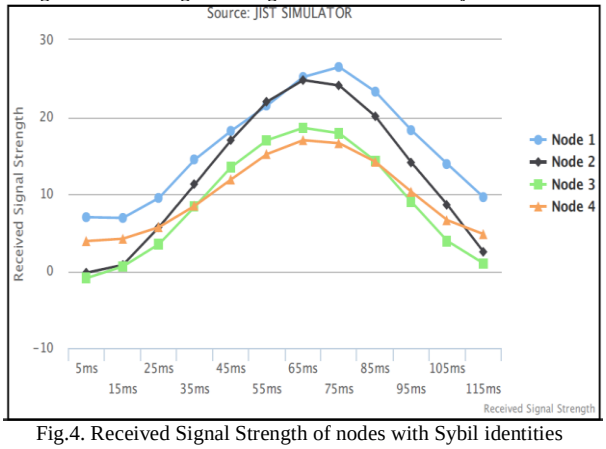

Fig.4. Received Signal Strength of nodes with Sybil identities

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

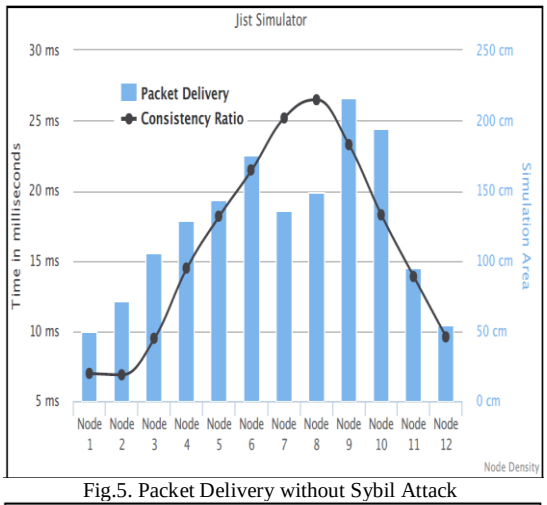

Fig.5. Packet Delivery without Sybil Attack

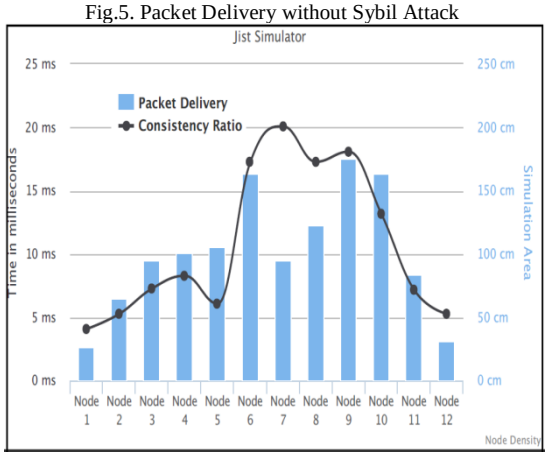

Fig.6. Packet Delivery with Sybil Attack

V. CONCLUSION

MANET is liable to various attacks due to its infrastructure less or wireless nature. To possess safe communication it's must be secure network. There are numerous attacks in MANET and there's one attack that is incredibly dangerous referred to as Sybil attack, it uses multiple identities or uses the identity of another node present within the network to disrupt the communication or reduce the trust of legitimate nodes within the network. And masquerading is another attack similar to Sybil cause damage to communication in network while giving false impersonation. In this paper mentioned regarding various techniques to detect Sybil nodes within the network. Also use Received Signal Strength of nodes to detecting the Sybil and masquerading nodes with good accuracy even within the presence of mobility.

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] Mukesh Barapatre and Vikrant Chole, "Spoofing Attack Detection and Localization in Adhoc network using Received Signal Strength," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2014.

[3] J. R Douceur, (2002), "The Sybil Attack", *IPTPS '01: Revised Papers from the FirstInternational Workshop on Peer-to-Peer Systems*, pp. 251–260, Springer Verlag, London, UK.

[4] Brian Neil Levine, Clay Shields, N. Boris Margolin," A Survey of Solutions to the Sybil Attack," Dept. of Computer Science, Univ. of Massachusetts, Amherst Dept. of Computer Science, Georgetown University

[5] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, "On the use of radio resource tests in wireless ad hoc networks," in *Proc. 3rd WRAITS*, 2009, pp. 21–26.

[6] H. Liming, L. Xiehua, Y. Shutang, and L. Songnian, "Fast authentication public key infrastructure for mobile ad hoc networks based on trusted computing," in *Proc. Int. Conf. WiCOM*, 2006, pp. 1–4.

[7] S. Capkun, J. P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," *IEEE Trans. Mobile Comput.*, vol. 5, no. 1, pp. 43–51, Jan. 2006.

[8] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in *Proc. Securecomm Workshops*, 2006, pp. 1–11.

[9] Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE, 2010 ' Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks', IEEE Transactions ON Vehicular Technology, VOL. 59, NO. 5.

[10] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, 2009 'Sybil Nodes Detection Based on Received Signal Strength Variations within VANET', International Journal of Network Security, Vol.9, No.1, PP.2233.

[11] Abbas, M. Merabti, and D. Llewellyn-Jones, 2010 'Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks,' in Proc. WD IFIP, pp. 1–6.

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

[13] Mukesh Barapatre, Prof. Vikrant Chole, "A Review on Spoofing Attack Detection in Wireless Ad hoc Network," in International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013, ISSN 2278-6856

BIOGRAPHY

B. Sivakumar received the B.Tech degree from Narasu's Sarathy Institute of Technology Salem in the year of 2012. He is currently doing his M.E in Computer Science and Engineering in Adhiyamaan College of Engineering, Hosur. His area of interest are Ad-hoc Networks, Network Security and Real time Software Development He is an active member of CSI.