ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# DETECTING SYBIL ATTACK BASED ON RSS IN MOBILE AD HOC NETWORKS

**Mr.Sivakumar.B*, Assistant Prof. Gracy Theresa.W**
* PG Scholar Dept of CSE, Adhiyamaan college of engineering, Hosur, Krishnagiri(dist..)
Assistant Professor Dept of CSE, Adhiyamaan college of engineering, Hosur, Krishnagiri(dist..)

## ABSTRACT

Mobile Ad hoc Networks (MANETs) is an autonomous collection of mobile nodes that form a temporary network without any existing network infrastructure or central access point. Since MANETs require a unique, distinct, and persistent identity per node in order for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. Sybil attacker can illegally claim multiple identities on single node and violate one-to-one mapping. There are various approaches to detect Sybil identities on network one of the promising solution is RSS (Received Signal Strength) based detection of Sybil attack this scheme detect Sybil identities without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system.

**KEYWORDS**: Mobile Ad hoc Networks (MANETs), Sybil Attack, Received Signal Strength, Security.

## INTRODUCTION

MANETs is a self organized collection of mobile nodes that form a dynamic topology without any fixed infrastructure. Communication on MANET based on unique identity of each mobile nodes that forms the one to one mapping between an identity and an entity and that is usually assumed either implicitly or explicitly by many protocol mechanisms; hence two identities implies two distinct nodes. But the malicious nodes can illegitimately claim multiple identities and violate this one-to-one mapping of identity and entity philosophy [1].

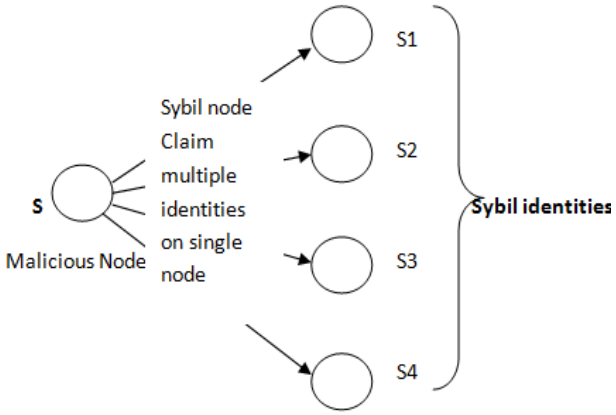


***Figure 1 A Sybil attacker with multiple identities***

Figure 1 represents a malicious node S along 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 will have illusion that it has communicated with five different nodes. But in actual, there exists only one physical node with multiple different IDs.

Masquerading attack is active attack in which user of the system illegally spoof the identity of another legitimate user [2]. Masquerade attacks can occur in several different ways. In general terms, a masquerader may get access to a legitimate user's account either by stealing a victim's credentials, or through a break in and installation of key logger. In either case, the user's identity is illegitimately acquired. In MANETs communication based on unique id this type of attacks are giving serious threat to network here by utilizing the Received Signal Strength of nodes to identify the Malicious nodes.

## RELATED WORK

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

Trusted Certification: It is considered to be one of a good preventive solution for Sybil attacks [3] in which a centralized authority is employed for establishing a Sybil-free domain of identities. Each entity in the network is bound to a single identity certificate [6]. However, trusted certification suffers from costly initial setup, lack of scalability and a single point of attack or failure.

Resource Testing: In this approach [5], various tasks are distributed to all identities of the network in order to test the resources of each node and to determine

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

whether each independent node has sufficient resources to accomplish these tasks. These tests are carried out to check the computational ability, storage ability and network bandwidth of a node. A Sybil attack will not possess a sufficient amount of resources to perform the additional tests imposed on each Sybil identity. The drawback of this approach is that an attacker can get enough hardware resources, such as storage, memory, and network cards to accomplish these tasks.

Piro et al. [8] proposed to detect Sybil identities by observing node dynamics. Nodes are keeping track of identities which are often seen together (Sybil identities) as opposed to the honest distinct nodes that move freely in different directions. However, the scheme will produce high false positives where node density is high, such as a conference hall or nodes moves in a same direction, such as a group of soldier moving toward a target.

Abbas, M. Merabti et al. [11] Reputation based schemes to detect Whitewashing attack. A selfish node can easily escape the consequences of whatever misbehaviour it has performed by simply changing identity to clear all its bad history, known as whitewashing

B. N. Levine et al. [4] Use the recurring Cost and Fees approach this technique is a variation of the normal resource testing, and can limit the number of Sybil nodes an attacker, with constrained resources, can introduce in a period of time. Charging a recurring fee for each participating identity is more effective as a disincentive against Sybil attacks.

Yingying Chen et al. [9] Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and further utilize the identity information to launch identity-based attacks. In this by using the physical properties associated with wireless transmissions to detect identity-based attacks. In particular, utilize the received signal strength (RSS) measured across a set of landmarks (i.e., reference points with known locations) to perform detection of identity-based attacks.

Capkun et al. [7] Mobility of nodes in a wireless network can be used to detect and identify nodes that are part of a Sybil attack. this rely on the fact that while individual nodes are free to move independently, all identities of a single Sybil attacker are bound to a single physical node and must move together. The individual nodes that wish to detect Sybil attackers monitor all transmissions they receive over many time intervals. These intervals are chosen long enough to capture behavior from all the Sybil identities of an attacker, including data transmissions, HELLO and keep alive messages, and routing requests and replies. The node keeps track of the different identities heard during the interval. By made many observations, the node analyze the data to find identities that appear together often and that appear apart rarely. These identities are Comprise as Sybil attack.

Mohamed Salah Bouassida et al. [10] Sybil detection approach, based on received signal strength variations, allowing a node to verify the authenticity of other communicating nodes, according to their localizations. This technique allows detecting malicious and Sybil nodes within VANET by using received signal strength variations, localization verification and nodes distinguishability degree evaluation. Geometrical analysis, that an attacker should not increase its sending power. Then, by successively measuring the received signal strength variations, can obtain an estimation of relative nodes localization.

## PROPOSED WORK

It is used to detect Sybil nodes. It does not require any extra hardware or antennae to implement it. So it is referred as Lightweight Sybil attack Detection. [12].

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 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.

Enquiry Based on Signal Strength: In this step, each node collects the information about the RSS value of neighbouring 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 neighbour nodes in the form of

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

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.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

We logically partition the radio range of node A into two zones: a gray zone and a white zone as shown in figure 2.
Node A will make a decision based on the RSS values of the nodes. If the first RSS value captured is greater than the threshold, i.e., a node is in the white zone, A will deem that identity as a new identity from a Sybil attacker, since no node can penetrate into white zone within the specified speed. If the first RSS value received is less than the threshold, i.e., a node is in the gray zone, it will be considered as a normal new entrant and will be added to the neighbor list.

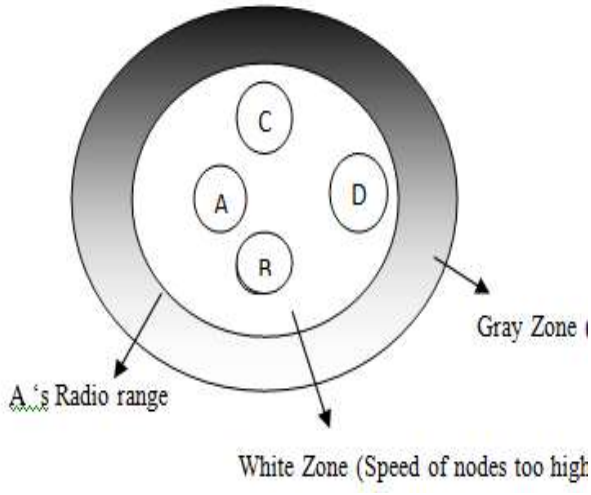


***Figure 2 Categorization of Radio Range***

***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 | |

Explanation of figure 2, 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. It is important to control the size of Table I, otherwise it would grow indefinitely. In order to control its size, the unused records need to be deleted. These unused records are due to certain reasons. First, when a malicious node changes its identity, its previous identity record stays in the RSS table. Second, nodes join and leave the network at any time; hence nodes that depart from the network, leave behind a record of their RSS histories. In order to control the size, a global timer, called RSS−TIMEOUT shown in Algorithm 2, is maintained to flush the unnecessary records. When this timer expires, the rssTableCheck function is called, which checks the time of the last received RSS against the TIME−THRESHOLD for every address of the RSS table. If the time obtained is greater than this threshold, indicates that it is enough time past since it is not heard from this node.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

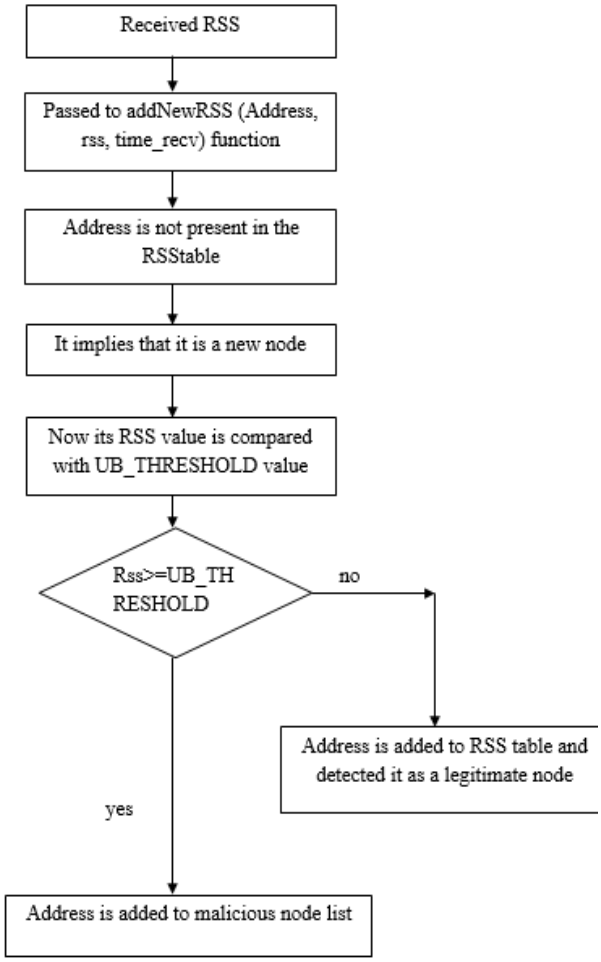


***Figure 3 Flowchart of Light weight Sybil attack detection algorithm***

## 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. We use two metrics in order to determine the detection accuracy of our scheme in different environments, i.e., true positive rate (TPR) and the false positive rate (FPR). True positive means a malicious node is correctly detected and false positive means a legitimate node is incorrectly detected as a malicious node.

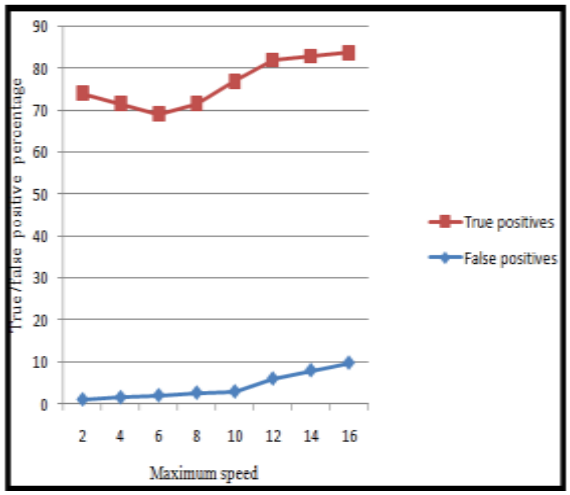


***Figure 4 True and False positives with various speeds***

Figure 3 shows that by using the RSS based scheme to detect Sybil identities with good accuracy and improved true positive rate is achieved.

## CONCLUSION AND FUTURE WORK

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 discussed about various techniques to detect Sybil nodes in the network. Also use Received Signal Strength of nodes to detecting the Sybil node with good accuracy even in the presence of mobility. In future taking issues of masquerading attack in networks and detecting the attack using the same Received Signal Strength of mobile nodes.

## 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

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

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