Secure Authentication Protocol to Detect Sybil Attacks in MANETs

Nidhi Joshi[1]
M.Tech IV Semester
Department of Computer Science & Engineering
CMR Institute of Technology
Bangalore, India
nidhijoshi_64@rediffmail.com

Prof. Manoj Challa[2]
Associate Professor
Department of Computer Science & Engineering
CMR Institute of Technology
Bangalore, India
manojcmrit@gmail.com

Abstract

Mobile ad-hoc networks (MANETs) are well known to be susceptible to various attacks, due to features such as lack of centralized control, dynamic topology, limited physical security and energy constrained operations. In this paper, we focus on preventing Sybil attack and Intruder nodes (malicious node). We are presenting a novel and secure authentication of nodes as soon as they comes in to the network (checks the identity of a new node) and then checking the RSS value of node continuously and accurately detecting the sybil identity in the network.

Keywords: MANETs, Sybil attack, Authentication mechanism, MAC.

I. INTRODUCTION

A mobile-ad-hoc network (MANET) is a collection of nodes forming a provisional or permanent network without relying on any centralized architecture or control. Nodes can enter and join or leave the network at any time, as well as can roam across the network freely. As MANETs do not rely on any centralized architecture, such as access points or base stations, all the necessary network functionalities are performed by the nodes forming the network. Each node acts as a host as well as a router, relaying data to extend the range by establishing connectivity between the source and destination nodes that do not fall within direct range of each other. Such networks are mainly intended for use in disaster relief scenarios, rescue and search operations, campus networks, robot networks and vehicular networks. Communication & data transfer in MANETs are usually based on Unique Identifier (Uid), which represents the node entity. Figure1 is an example of MANETs containing various mobile phones, smart phones and Laptops.

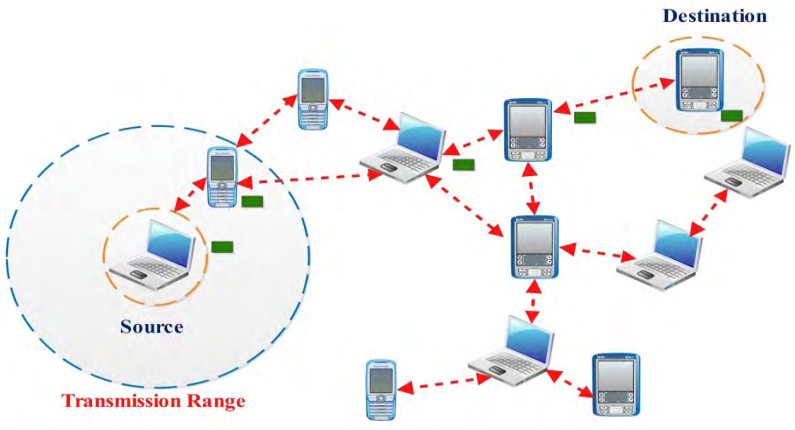

Figure 1: MANETs Example

In the above Figure, each devices represents a node . Nodes connect to all other nodes nearby. When one node wishes to send data to another, the data is passed across, or routed, through several other nodes until its destination is reached. Nodes are able to be dropped and reconnected to the network as needed since their connections may be unstable. This works well for the devices as most devices in MANETs are typically low-

power with a small transmission range but are still capable of routing information over large distances by bouncing off other device in a MANET.

MANET also vulnerable to many security attacks. Due to lack of centralized identity management and the requirement of unique, distinct and persistent identity per node for their security protocol to be viable, Sybil attack [1] poses a serious impact to such a network. A Sybil attack is in which a malicious node in the network, illegitimately claims to have multiple identities on a single physical device. If an entity on a network does not have physical knowledge of the other entities, it will perceive them purely as informational abstractions called identities. Sybil attack [2] occurs when the one-to-one correspondence between an entity and its identity is violated. They affect a number of environments and application domains in a variety of ways. For instance, the reputation system of a Peer-to-Peer network may be compromised as the attacker is able to favorable alter reputation scores by the use of the newly created rogue identities. In the worst case scenario, an attacker can create an infinite number of forged identities with just one physical device.

A Sybil attack [3] creates a serious impact on the normal operation of the network. So, it's required that as soon as the Sybil identity identified in the network, it should be eliminated from the network. The traditional approach of preventing Sybil attack is to use Trusted Certification [4] or Cryptographic-based-Authentication.

However, this approach is not suitable because it requires costly initial setup and overhead involved in maintaining & distributing Cryptographic Keys. On the other hand, Received Signal Strength (RSS) [5] is considered as a Lightweight solution for MANETs. However, this approach does not require any extra hardware such as antennas or Geographical Positioning System (GPS). In this, node share & manage identities of Sybil and Non-sybil identities in a distributed manner. Although, it is a Lightweight scheme, but cannot accurately identifying Sybil identity in the network. As people will be encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms if we want to see this exciting technology become widely used in a next few years.

II. RELATED WORK

Sybil attack which was first introduced by Douceur [2] in the context of peer-to-peer network. Douceur showed that there is no practical solution for this attack. Deploying Trusted Certification is the only scheme that can completely eliminate the Sybil attack. However, it suffers from costly initial setup, lack of scalability and a single point of attack or failure. Also, it's based on the assumption that each entity has single identity which is very difficult to achieve on the large network.

Resource Testing: This technique was proposed by Douceur [2].In this approach; various tasks are distributed to all the identities of the network to test the resources of each node and to determine whether each node has enough resources to accomplish these tasks [6]. This test checks the computational ability, storage ability and network bandwidth of a node. Sybil attacks will not posses enough resources to perform additional tests imposed on each Sybil identity. This approach has two main drawbacks; first, in many applications very few Sybil identities are required to launch an effective Sybil attack. Second, an attacker can acquire enough hardware resources, such as storage, memory, and network cards to accomplish these tasks

Recurring Costs & Fees: In this approach, identities are regularly re-validated using resource tests. Each participating identity is further periodically charged with a fee. For example, Margolin et al. [7] proposed the use of a recurring fee per participating identity to deter Sybil attackers and they suggest that such a recurring fee is more of a deterrent than a one-time fee. They also established that recurring fees can incur a cost to the Sybil attacker that increases linearly with the total number of participating identities, whereas a one-time fee incurs only a constant cost. The recurring fee may not be a monetary based payment mechanism, but it can be a nonmonetary payment mechanism such as CAPTCHAs [8], charges SMS messages or cooperation in the network [9]. However, fee management is generally too costly to implement and manage in MANETs.

Trusted Devices: It is a one-to-one mapping of a hardware device and a network entity. In other words, one hardware device, such as a network card, is bound to one network entity. However, there is no way of preventing an entity from obtaining multiple hardware devices, such as an attacker can install two network cards. Capkun *et al.* [10] exploited mobility to enhance security in MANETs. Piro *et al* [11] proposed to detect Sybil identities by observing node dynamics. BARTER [12] is a behavior-based access and admission control system for MANETs in which nodes initially exchange their behavior profiles and calculate individual local definitions of normal network behavior.

Received Signal Strength based Detection: Signal strength based [5] position verification seems most promising among the three because it is Lightweight solution and even can be used without the use of GPS. However, these schemes sometimes require additional hardware, such as directional antennae, or extra overhead incurred due to periodic localization of nodes [13]. Here, nodes share and manage identities of Sybil and Non-sybil nodes in distributed manner.

III. PROPOSED SCHEME

A. Attack Taxonomy

A Sybil node can forge different identities to trick the network with multiple fake nodes. Sybil attack is classified into two types. First, in which attacker node creates new identity while discarding its previous identity from the network. Such type of attack is called Whitewashing Sybil attack. In this, attacker might present a large number of identities over a period of time, while only acting as a smaller number of identities at a given time. The attacker can do this by having one identity seem to leave the network and have other identity to join in its place. Due to this is also known as Join & Leave Sybil attack. The main purpose of this attack is to delete the bad history of malicious node & promoting lack of accountability in the network. Second, in which an attacker participates with all its identity at once for an attack is called Simultaneous Sybil attack .The main purpose of this attack is to create confusion in the network or try to gain more resource, information, access etc than that of a single node deserves in a network.

A Sybil node can get the identity in one of two ways. First, it can fabricate the identity (or get some arbitrary identity) .In some cases the attacker node create an arbitrary identities in the network. For example, if the node is identified by 16 bit integer, the attacker simply assigns each Sybil node with a random 16 bit integer. Second, it can steal an identity from legitimate node. Attacker assigns the identity of legitimate node to Sybil identities.

B. Received Signal Strength Based Analysis

To compare the behaviour of new legitimate node with new Sybil identity, this is usually based on the Received Signal Strength. In the Figure 2, the Node 'A' is called a Master Attack Detection Node, which is a static node. If any new node 'B' enters in to the neighbours of 'A' node the first RSS value received at node 'A' will be lower. However, the node 'B' gradually enters over time in the network. This is the normal entrance of node in the network. That node is termed as Legitimate node. In contrast to Sybil attacker, where new identity launched by an attacker, which causes an abrupt changes in the RSS value at the receiver.

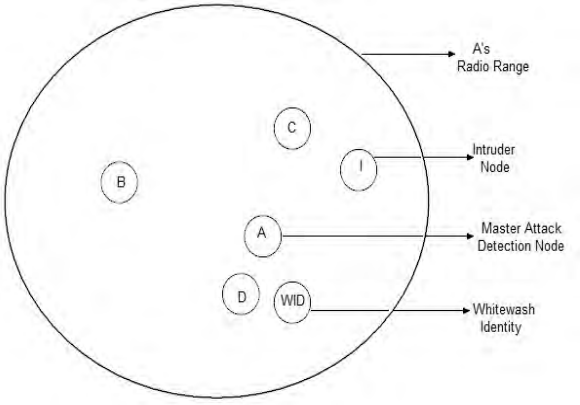

Figure 2: Entrance & Exit of a node

In the Figure 2, shows the entrance & exit of a node in the network, which is based on the neighborhood joining behavior. Due to natural behaviour of node joining & leaving the network, suppose if any node 'B' entering in to the radio range of 'A' node, which is the main attack detection node, the RSS value will be increasing continuously.

If we plot the graph between RSS and Time, if 'A' node plots B's RSS reading, B moves towards A, and then goes ultimately out of range. In graphical form the RSS of B will produce more or less a complete elliptical curve as shown in Figure 3.

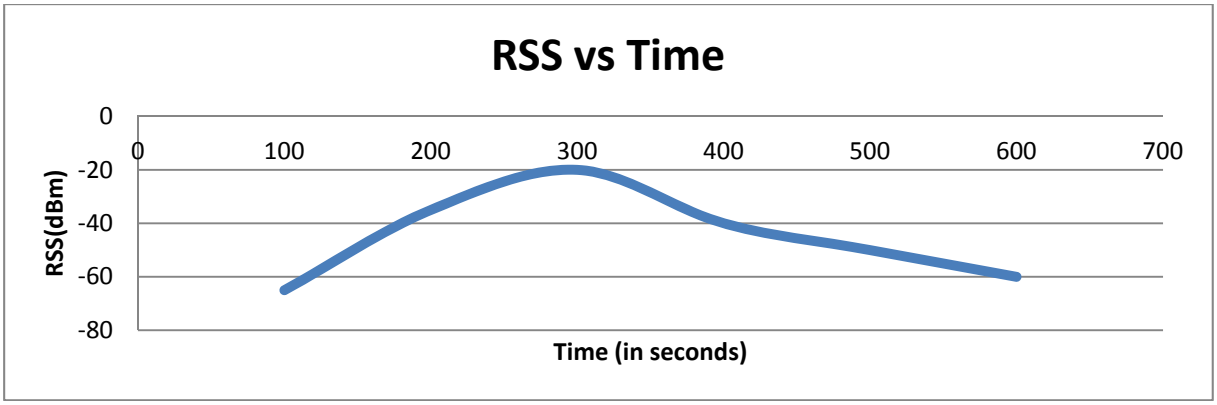

Figure 3: RSS Value versus Time

The smallest readable RSS value could be used as a detection threshold. Each node collects & maintains the RSS value of neighbouring nodes. Each node maintain a list of neighbours in the form of < Address, RSS-list, <X, Y>> as shown in Table I.

Node ID	RSS-List
1	R1 T1 X1,Y1 → Rn Tn Xn,Yn
2	
3	
N	

Table I: RSS-List of node

Each RSS list in front of the address contains RSS value of directly received frame, time of reception along with the coordinate value (i.e. X, Y),which provide the actual location of Sybil identity . Each RSS list of a node contains 'n' node value. For the threshold detection; we logically partition the radio range of node A in to two zones: a Gray Zone & White Zone. This logically partition is based on the speed based detection threshold. We will setup our detection threshold based on the maximum speed of the network. Assuming that no nodes cannot move faster than the maximum speed (36 km/h). This threshold would make distinction, because if any new received RSS is greater than equal to Threshold detection, it's a Sybil identity; otherwise it's a Normal or legitimate identity. For the detection of a node, we adopt the lower speed threshold (2 m/s or 4 m/s).

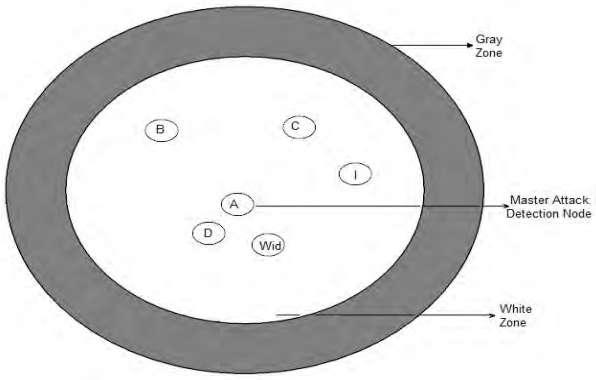

Figure 4: Logically Partition: Gray & White Zone

In the figure 4, the partition is done on the speed based detection threshold. If a higher speed threshold would produce a thin gray space, where to detect Sybil identity is difficult because the first presence of any node will pretends as normal entry in to the radio range of the node. Hence, lower bound detection threshold would

produce a thick gray zone, where first the node identity is checked by using a Secure Message Authentication Code (MAC) and then checks the signal strength behaviour of a node (RSS value). If any abnormal entry or whitewashed identity is detected, then it's immediately updating the entire neighbouring node in the network. Otherwise, it's a legitimate node entry. As well as after crossing the gray zone, node RSS value is constantly updating in the RSS-List. If any abnormal entry found, it's immediately updated with message. Here, if a Sybil attacker creates an identity in the white zone then the Sybil identity first RSS value is checked, if it's greater than lower bound threshold detection, then it's an abnormal entry. Hence, an identity change attack is found in the network.

In this approach, as soon as the node comes in to the network, its identity & RSS value checked with the detection threshold. In short, if Sybil identity is far & near it's accurately identified. If not detected soon, otherwise causes a lot of disturbance in the network.

C. Authentication of a Node

A Message Authentication Code (MAC) is a short piece of data which is mainly used to authenticate a message. As well as, it's used to provide integrity & authenticity assurance over the message. Sometimes MAC algorithm is called as a keyed hash function because it accepts secret key as input and an arbitrary-length message to be authenticated, and MAC as an output. The MAC provides both the authenticity & data integrity, by allowing verifiers to detect any changes to the message content.

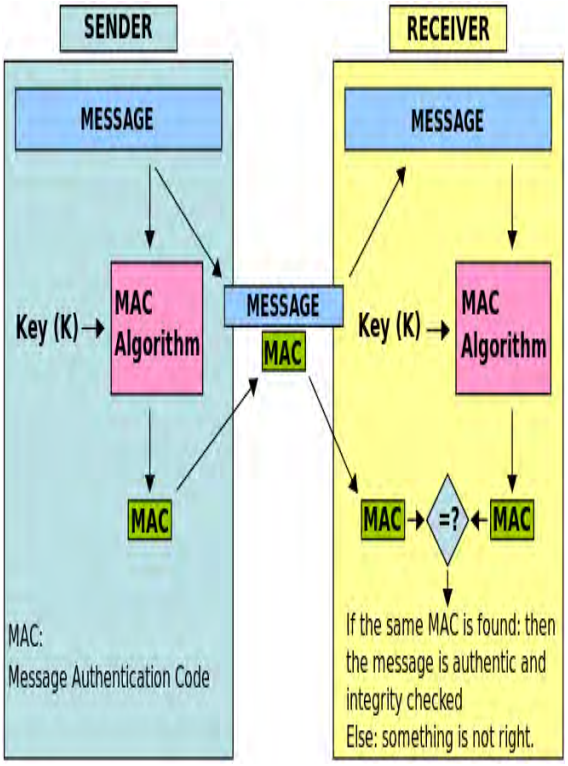

Figure 5: MAC Creation

In this Figure 5, the sender of a message, first generate the MAC through the MAC algorithm & Key (K). The original message along with the MAC tag is then transmitted to the receiver. Upon receiving the message, receiver in turn runs the original message portion of the transmission through the same MAC algorithm using the same key, producing a second MAC data tag. The receiver then compares both the MAC tag i.e. first MAC tag send by sender & second MAC tag generated by receiver. If both are identical, the receiver can assume that the integrity of the message was not changed, and the message is not altered by intruder in between the transmission

D. Workflow Diagram

For Gray Zone

If any node comes in to the network, it is in Gray Zone. Node is first get Authenticated by using a secure Hash Function. After Authentication, received RSS value is first checked with lower bound detection threshold, if it's lower, it's a Legimate node; otherwise it's a Sybil identity. After this, it's passed to addNewRss function where the address of a node, time of reception, received RSS value & X, Y coordinate value will get store. The X & Y

Coordinate value will help us to determine the exact location of Sybil identities in the network. For a Legitimate node, it's added to RSS-Table. Otherwise the address is added to malicious node list (as shown in Figure 6).

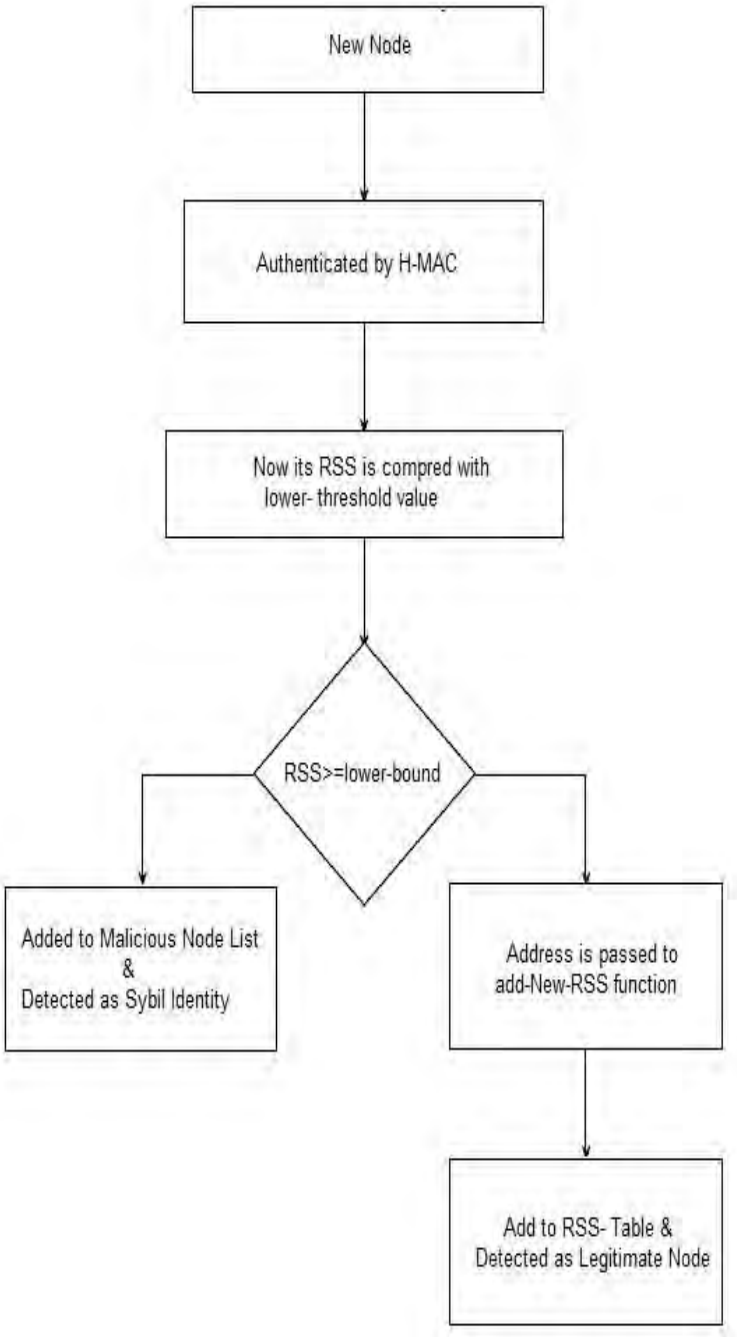

Figure 6: Gray Zone

For White Zone

If any node which launches a Sybil attack or changes an identity, then its checks the received RSS of the node with lower bound detection threshold, if its greater then it's an identity change or Sybil attack in the network(as shown in Figure 7)

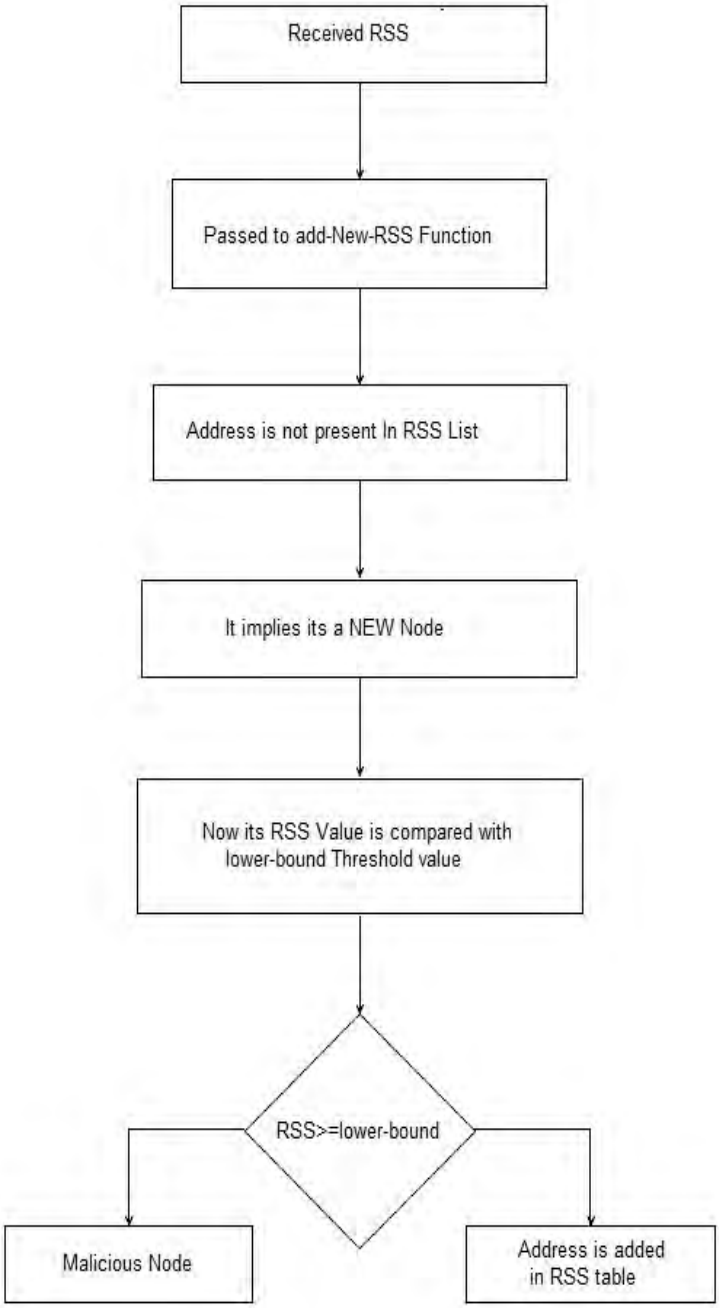

Figure 7: White Zone

IV. IMPLEMENTATION & PERFORMANCE EVALUATION

In order to implement & evaluate our proposed system, we used JAVA platform using the parameters listed in the Table II. The Lower_Bound_Threshold is the averaged RSS value (dBm) of several scenarios, with the speed of 2m/s or 4m/s. The TIME_THRESHOLD is the average time period in which the node listen from another node, otherwise the node is consider as a Whitewashed identity or Sybil identity in the network. The LIST_SIZE is the maximum RSS record retained for an identity, we had consider 5 as an arbitrary number of records per identity and depending upon the memory & buffer it can be increased also.

PARAMETER	LEVEL
Area	800 m*800m
Speed	2 to 4 m/s
No. of Nodes	15 to 30
RSS_TIMEOUT	75s
TIME_THRESHOLD	25s
LB_RSS_THRESHOLD	0.0000000645 W
LIST_SIZE	5
MAC	802.11

Table II: Parameters

The main purpose of conducting is to establish the detection percentage of our proposed scheme in different scenario. In each scenario we take the speed as our main attribute.

Metrics

To determine the detection accuracy, two metrics are used.

True positive Rate (TPR): It means that a malicious node is correctly identified as Whitewash identity in the network.

Mathematically,

TPR = Correctly Detected Whitewash Identity/ Total whitewash identity

False Positive Rate (FPR): It means that a Legitimate or good node is incorrectly identified as a malicious node.

Mathematically,

FPR = Incorrectly detected Legitimate Identity/Total good Identity

Analysis

As shown in Figure 8 (below), describes about the normal entry & exit of a node in to the radio range of other node. The node normally enters in to the radio range of other node, moves normally & then goes out of range.

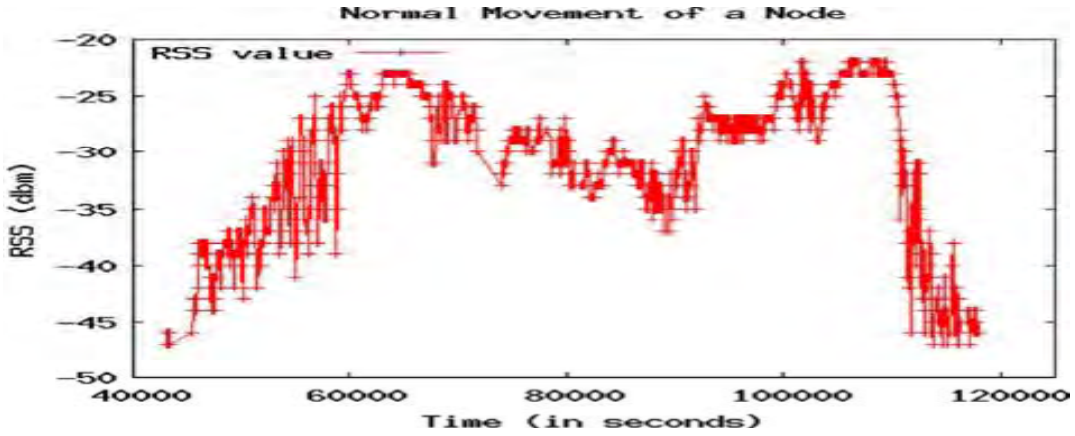

Figure 8: Normal Entrance & Exit of a node

A node enters in to the radio range & after some random movement & pauses changes its identity & with its new identity, then goes out of radio range (launching Sybil attack in the network).

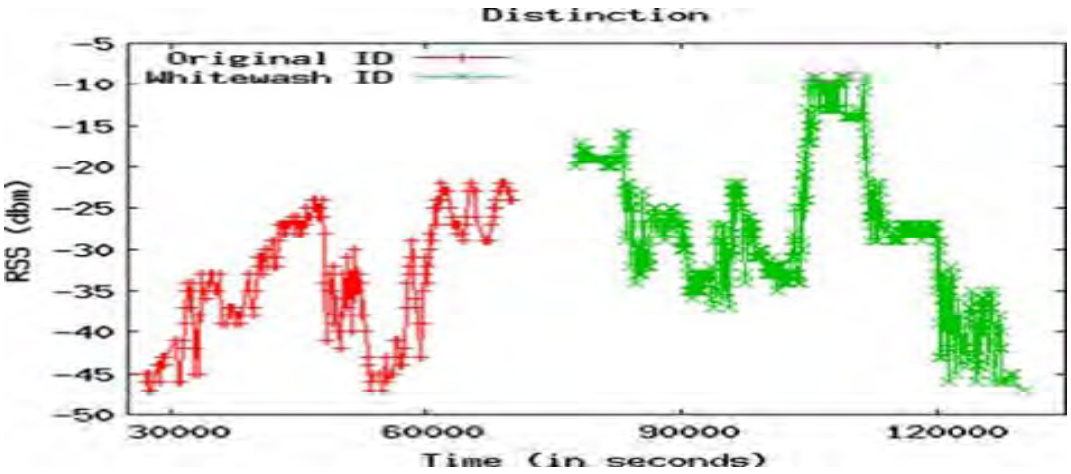

Figure 9: Distinction between Original & Whitewash Identity

V. CONCLUSION & FUTURE ENHANCEMENT

In this paper we proposed the RSS based detection approach along with the authentication of node which will correctly identified the Sybil identity with Higher True Positive. For the authentication of node, Message Authentication Code (MAC) is used. Authentication of node allows only legitimate node to come in to the network. As well as Lower-bound detection threshold is used, and compare with Received Signal Strength (RSS) value, if the comparison is greater than or equal to RSS value, then it's a Sybil identity (Whitewash identity). Otherwise it's a Legitimate node in the network.

Our future works includes the issues related to variable transmits power as well to deal with Rushing Attack with the proposed scheme.

References

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

[2] 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.

[3] Karamjeet Kaur , Sanjay Batish & Arvind Kakaria," Survey of Various Approaches To Countermeasure Sybil Attack" in Proc. Vol.1, Issue 4, IJSCI, 2012, pp. 96-100.

[4] S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks," in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010, pp. 17–24.

[5] 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.

[6] 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.

[7] N. B. Margolin and B. N. Levine, "Quantifying resistance to the Sybil attack," in Financial Cryptography and Data Security. Berlin, Germany:Sprnger, 2008.

[8] V. A. Luis, B. Manuel, and L. John, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.

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

[10] 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.

[11] 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.

[12] V. Frias-Martinez, S. J. Stolfo, and A. D. Keromytis, "BARTER: Behavior profile exchange for behavior-based admission and access control in MANETs," presented at the Proc. 5th Int. Conf. Information Systems Security, Kolkata, India, 2009, pp. 193–207.

[13] A. Parameswaran, M. I. Husain, and S. Upadhyaya, "Is RSSI a reliable parameter in sensor localization algorithms: An experimental study," in Proc. F2DA, 2009.