ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.9

Analysing the Impact of Sybil Attacks on the Performance of MANETS

B.Damodhara Rao[1], M.Ramesh[2]
PG Scholar[1], HOD & Assistant Professor[2]
Department of Computer Science and Engineering
Thandra Paparaya Institute of Science and Technology, Bobbli, Andhra Pradesh, India

Abstract:
In Mobile-Ad-hoc network (MANET) security is a challenging issue due to its open nature, infrastructure, less property and mobility of nodes. Due to this, Sybil attack is one of the most severe attacks in the vast domain of the ad-hoc network under the control traffic attack. Sybil attack is a spoofing attack, where a malicious node illegitimately creates multiple fake identities (called the Sybil nodes) to impersonate as normal nodes. The research paper that I took as my benchmark is observed that most of the existing protocols fail to defend against Sybil attack. Therefore, Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, this approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS). The RSSI is used to form the cluster and to elect the cluster head. The CA's responsibility is given to the CH. Whenever huge variations occur in RSSI on neighbor's entry and exit behavior, the Certification Authority comes into play. The CA checks the certification of a node. If it is not valid, its certificate is revoked otherwise it is free to communicate in the network.

Keywords: RSS, MANET, GPS, Sybil attack, Identity-based attacks, intrusion detection, Digital Certificate, Components.

1. INTRODUCTION

1.1 Background of Cellular networks

There are currently two variations of mobile wireless networks infrastructure and infrastructure less network (Ad-hoc networks).The infrastructure ***networks,*** also known as **Cellular network**, have fixed and wired gateways. They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station).

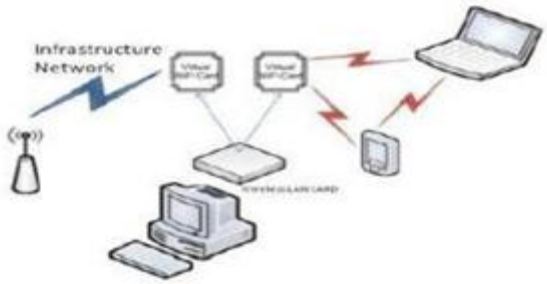

Figure .1. Infrastructure networks

A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs). Infrastructure network is as shown in Figure 1 [1]. The other type of network, as shown in the Figure 2 is infrastructure less network (Ad-hoc network), is also known as Mobile Ad Network (MANET) [6]. These networks have no fixed routers and it is a self-configuring network consisting of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are out of their transmission ranges in the Ad-hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration.

Figure.2. Mobile Ad Hoc Network (MANET)

The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks. An ad-hoc network [6] uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to enter and leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops are generally needed to reach other nodes. Every node in an ad-hoc network must be willing to forward packets for other nodes. Thus every node acts both as a host and as a router. The topology of ad-hoc networks varies with time as nodes move,

join, or leave the network [8]. This topological instability requires a routing protocol to run on each node to create and maintain routes among the nodes.

1.2 CHARACTERISTICS OF MANET:

1.2.1. Distributed Operation

There is no background network for the central control of the network operations; the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

1.2.2. Multi hop Routing

When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

1.2.3. Autonomous Terminal

In MANET, each mobile node is an independent node, which could function as both a host and a router.

1.2.4. Dynamic Topology

Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

1.2.5. Light-weight Terminals

In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

1.2.6. Shared Physical Medium

The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

1.3 APPLICATIONS OF MANETS

Self reconfiguring, easy deployment, decentralized and infrastructure independent nature of MANET makes befit for communication.

1.3.1. Military battlefield

Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.

1.3.2. Collaborative Work

For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

1.3.3. Local level

Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at an e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

1.3.4. Personal Area Network and Bluetooth: A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

1.3.5. Commercial Sector

Ad hoc can be used in emergency /rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

1.4. ADVANTAGES OF MANET

- They provide access to information and services regardless of geographic position.
- Independence from central network administration. Self-configuring network, nodes are also act as routers. Less expensive as compared to wired network.
- Scalable—accommodates the addition of more nodes. Improved Flexiblibility.
- Robust due to decentralize administration. The network can be set up at any place and time.

1.5. DISADVANTAGES OF MANET

1.5.1. Lack of Centralized Management

MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult

1.5.2. No Predefined Boundary

In MANET we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network.

1.5.3. Cooperativeness

Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation.

1.5.4. Limited Power Supply

The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems.

1.5.5. Adversary inside the Network

The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behaviour of the node is malicious. Thus this attack is more dangerous than the external attack.

1.6. OVERVIEW OF MANETS:

Mobile ad hoc networks (MANETs) is an infrastructure-less, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks.

1.6.2. CHALLENGES OF MANETS:

- **Limited bandwidth:**

Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference

conditions, etc., is often much less than a radio's maximum transmission rate.

- **Dynamic**

Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

- **Routing Overhead**:

In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

- **Hidden terminal problem**

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

- **Packet losses due to transmission errors**

Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.

- **Mobility-induced route changes**

The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

- **Battery constraints**

Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

- **Security threats:**

The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

1.7. Attacks in MANET

Attacks on mobile ad hoc networks can be classified into following two categories:

1.7.1. Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard.

1.7.2. Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These Attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more servers and difficult to detect when compared to external attacks.

II.SYBIL ATTACKS IN MANETS

2.1. Sybil Attack

Fully self-organized mobile ad hoc networks (MANETs) represent complex distributed systems that may also be part of a huge complex system, such as a complex system-of-systems used for crisis management operations. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions. 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.

2.2. EXISTING SYSTEM

A Sybil attacker can cause damage to the ad hoc networks in several ways. For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. In reputation and trust-based misbehaviour detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic. Therefore, Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, this approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS) in this project; we will present our scheme that detects Sybil identities. In particular, our scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First, we demonstrate the entry and exit behaviour of legitimate nodes and Sybil nodes using simulation and tested experimentation. Second, we define a threshold that distinguish between the legitimate and Sybil identities based on nodes' entry and exit behavior. Third, we tune our detection threshold by incorporating the RSS data fluctuation taken from our test bed experimentation. Fourth, we evaluate our scheme using extensive simulations, and the results show that it produces about 90% true positives (detecting a Sybil node as Sybil) and about 10% false positives (detecting a normal node

as a Sybil node) in mobile environments. The scheme can be applied to both scenarios of Sybil attacks, i.e., whether the new identities are created one after the other or simultaneously make no difference to the detection process. Our detection scheme can work as a standalone scheme, but could equally be deployed as an add-on to existing schemes, for example it could be incorporated into a reputation-based system, i.e., the detected Sybil identities from the MAC layer will be plugged into the reputation-based system on network layer. Our proposed scheme does not use localization technique for Sybil attack detection and hence does not need any directional antennae or any GPS equipment. Unlike, our proposed scheme does not use centralized trusted third party. In our scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner.

III. DETECTION OF SYBIL ATTACKS:

A. Attack Model:

There are two flavors of Sybil attacks. In the first one, an attacker creates new identity while discarding its previously created one; hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any bad history of malicious activities. This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack, an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack. The motivations of this attack is to cause disruption in the network or try to gain more resources, information, access, etc. than that of a single node deserves in a network. The difference between the two is only the notion of simultaneity; however, their applications and consequences are different in our scheme, we will consider both types of Sybil attacks. The strategy of our detection mechanism is to detect every new identity created by a Sybil attacker; it does not matter if the intention of the attacker is to use that identity for whitewashing or simultaneous Sybil attacks. Hence, in this paper, we will refer to the new Sybil identity and whitewash identity (WID) interchangeably we assume that the attacker joins the network with its single identity, and that malicious nodes do not collude with one another. We also assume that nodes do not increase or decrease their transmit power. The attackers can get identities by two ways. First, they can fabricate identities (for example, creating an arbitrary identifier). Second, they can use stolen identities, i.e., spoof the identities of legitimate nodes (masquerading) in the network. We assume the first case where nodes can create arbitrary identifiers because in MANETs, there are no restrictions on identity creation

B. SIGNAL STRENGTH BASED ANALYSIS

The distinction between a new legitimate node and a new Sybil identity can be made based on their neighborhood joining behavior. For example, new legitimate nodes become neighbors as soon as they enter inside the radio range of other nodes; hence their first RSS at the receiver node will be low enough. In contrast a Sybil attacker, which is already a neighbor, will cause its new identity to appear abruptly in the neighborhood. When the Sybil attacker creates new identity, the signal strength of that identity will be high enough to be distinguished from the newly joined neighbor. In order to analyze the difference between a legitimate newcomer and Sybil identity entrance behavior, we setup some experiments in the following. Before we start, it is important to explain how each node collects and maintains the RSS values of the neighboring nodes**.** Each node maintains a list of neighbors in the form **<Address, Rss-List <time, rss>>**, and records the RSS values of any directly received or overheard frames of 802.11 protocol, i.e., RTS, CTS, DATA, and ACK messages. In other words, each node will capture and store the signal strength of the transmissions received from its neighboring nodes. This can be performed when a node either takes part in the communication directly with other nodes acting as a source or a destination or when a node does not take part in the direct communication. In the latter case it will capture the signal strength values of other communicating parties through overhearing the control frames. Each Rss- List in front of the corresponding address contains Rn RSS values of recently received frames along with their time of reception, Tn. Where n is the number of elements in the Rss- List that can be increased or decreased depending upon the memory requirements of a node. In our simulation, we used n to be five elements; however, for real-world scenarios, it should be greater than that because of the time varying nature of RSS

C. DETECTION

We will setup our detection threshold based on the maximum speed of the network; assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first RSSs from newcomers, if greater than the threshold imply abnormal entry into the neighborhood. Now the question becomes, which speed should we adopt as the upper bound for our detection threshold from table. We used 10 m/s as an upper bound speed because we believe that in most of the ad hoc network applications including vehicular ad hoc networks in urban or congested areas, nodes usually may not move faster than 10 m/s (36 km/h) that is why we chose it to be a good upper limit for our scheme. So any new identity creation in the white zone will be detected as a whitewashing or Sybil identity, because normal nodes cannot produce their first appearance in this area. From the above discussion, we can deduce that smaller speed-based thresholds will work better than larger ones because they will produce high true positives. Please note that we adopt a 10 m/s threshold in our simulation based evaluation in this section, and for this speed the simulation produced sound results. We believe that detection will be improved by using a lower speed threshold than 10 m/s. For example, if in a network the maximum speed of nodes is 2 m/s then the detection threshold based on this speed would produce narrower gray zone, hence detection accuracy will be improved. In order to detect new identities spawned by a whitewasher or Sybil attacker, Algorithm 1 checks every received RSS by passing it to the add New Rss function, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been interacted with before, i.e., it is a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an UB−THRESHOLD (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e., whitewasher). If it is greater than or equal to the threshold, indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood; the address is added to the malicious node list. Otherwise, the address is added to the RSS table and a link list is created for that address in order to store the recently received RSS along with its time of reception in it. Finally, the size of the link list is checked, if it is greater than the LIST−SIZE, the oldest RSS is removed from the list.

Algorithm 1

addNewRss (Address, rss, time−recv)

BEGIN SUB:
IF: Address is not in the Table
THEN:
IF: rss >= UB−THRESHOLD
THEN: Add−to−Malicious−list(Address)
Bcast−Detection−Update(Address)
ELSE: Add−to−Table(Address)
END−IF
Create−Record(Address)
Push−back(rss,time−recv)
IF: list−Size > LIST−SIZE
THEN: Pop−front()
END SUB:

Algorithm 2
IF: RSS−TIMEOUT
THEN: rssTableCheck( )
rssTableCheck( )
BEGIN SUB:
FOR: for each Address in the Table
DO:
Pop−element()
IF: (Current−Time—getTime()) >TIME−THRESHOLD
//Indicating that we did not hear from this Address since the TIME-THRESHOLD
THEN:
IF: getRss() > UB−THRESHOLD
THEN: Add−to−Malicious−List(Address)
//Indicates previous ID of aWhitewasher
ELSE: Print "Normal out ofRange"
END FOR:
END SUB:

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. Now to check the reason of disappearance of nodes, the strength of the last RSS is checked against the UB−THRESHOLD, if it is greater, indicates that it is the previous identity of a whitewasher; otherwise it is concluded as a normal out of range scenario. The complexity, in terms of operations, of Algorithm 1 is O (1) and Algorithm 2 is O(n).

3.1. FAILURES IN THE EXITING SYSTEM

- It is failed to detect the stolen identities of Sybil attackers.
- In this the RSSI parameter to detect Sybil node because of its light weight but it has to failed to detect the fast moving Sybil attack.
- It is fail to detect when the Sybil attacker changes continuously ip address and Mac address.

3.2. PROPOSED SYSTEM

In this project we are proposed to find all Sybil attackers based on the Transmission Times. The key roles in my proposed system are to decrease the false positive rate and Increase the Throughput of the network.

3.2.1 Methodology

Sybil attackers are two ways to attack stolen identities and fabricate identities. Here we are building to algorithms to detect and prevent Sybil attackes. Algorithm1 is take the every ip address transmission time for certain fixed time period and form list<ipaddress, Transmission_time_micro_sec> and to the list<table> The list<table> count reachs five then those list of table transferred to proposed_sybil_attacker_detection function then it returns the sybill attacker list. To block those ipaddress in the Sybil attacker list in the network.
The list<table> maintain the queue so, the height of the queue is five. Whenever new element delete the old element in the list<table>.

Algorithm1
//To identifies the List of five tables from network nodes.
Step1: Collect the all the transmissions times for connected nodes. And maintain table
List <ipaddress,Transmission_time_micro_sec>.
Step2: Collect the table for every 5 seconds. And maintain those are in list<Table>
Step3: Collect the last five tables in the tables list.
Step4: Process the last five tables into proposed_sybil_attacker_detection. And Take the list<sybil ipaddres> from proposed_sybil_attacker_detection function.
Step5: To block the all the ipaddress contains in list<sybilipaddess>.

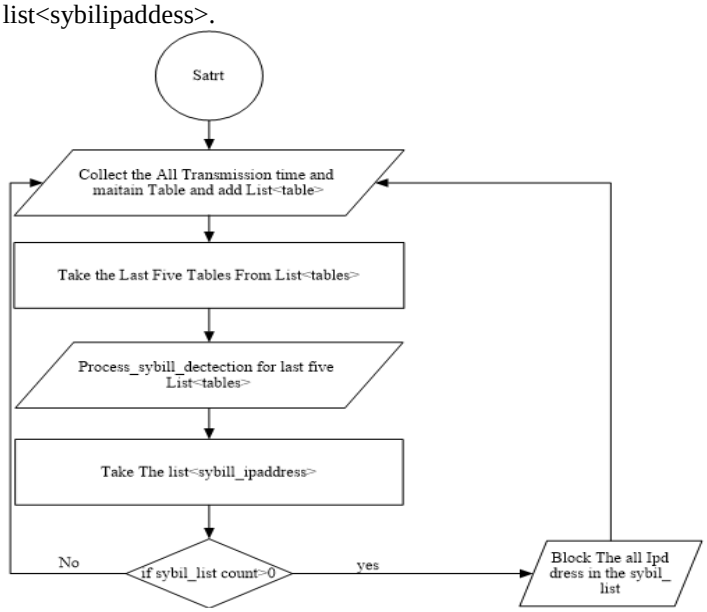

Figure.3. Flowchart for forming the list of list of tables.

Take the list<table> having length is five from alogithm1. identify the unique ip address of the every transmission time for five tables and form
list<ipaddress,list<transmission_time>>.
To calculate the pair of difference in the every table for every ipaddress and form final<ipaddress,list<times>>.
Compare the every list<times> in the final list if the list<times> is repeated more than once then those ipaddress add to the sybillist<ipaddress>.
Finally sybillist<ipaddress > are returned these ip address are Sybil attackers.

Algorithm2
//To Detect the Sybil_ipaddress from list<tables> given by alogorithm 1
//Return the Sybil_ipaddress_list.

Step1: Take five list<table> from algorithm 1
Step2: Filter the transmissions times from list<table> for each and every unique ipaddress and maintain the list<ipaddress,list<transmission_time>>.
Step3: Take each ipaddrss and list<transmission_time> from list<ipaddress,list<transmission_time>.
Step4: Calculate the every pair of values in the list and find the difference of that and maintain the list and the those list into to Final_list<ipaddress, list<transmission_time>>.
Step5: Repeate the step3 and step4 until all ipaddrss are added to the Final_list.
Step6: Find the duplicate list<transmission_times> in the final_list and identify those ipaddress and add to the Sybil_attacker_list<ipaddress>.
Step7: Return Sybil_attacker_list.

Table 1.

Ip Address	Transmission Time (Micro-secs)
169.254.172.64	0.7840
169.254.144.79	0.4780
169.254.167.38	0.2809
169.254.120.56	0.3578

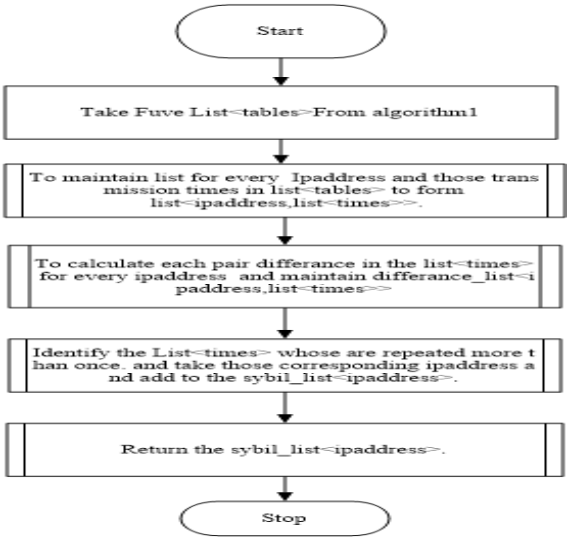

Figure.4. Flowchart of detecting Sybil attackers.

Experimental results of these algorithm is in the below tables.

Table.2.

Ip Address	Transmission Time (Micro-secs)
169.254.130.76	0.4616
169.254.156.62	0.5783

Table.3.

Ip Address	Transmission Time (Micro-secs)
169.254.172.64	0.8320
169.254.144.79	0.5460
169.254.167.38	0.3289
169.254.120.56	0.4058
169.254.130.76	0.4746
169.254.156.62	0.6463

Table.4.

Ip Address	Transmission Time (Micro-secs)
169.254.172.64	0.8680
169.254.144.79	0.5580
169.254.167.38	0.3509
169.254.120.56	0.4418
169.254.130.76	0.5206
169.254.156.62	0.6583

Table.5.

Ip Address	Transmission Time (Micro-secs)
169.254.172.64	0.8970
169.254.144.79	0.6110
169.254.167.38	0.4139
169.254.120.56	0.4708
169.254.130.76	0.5486
169.254.156.62	0.7113

Table.6.

Ip Address	Transmission Time (Micro-secs)
169.254.172.64	0.9159
169.254.144.79	0.6340
169.254.167.38	0.4269
169.254.120.56	0.4897
169.254.130.76	0.5666
169.254.156.62	0.7343

Difference Tables of Ip Address

Table.7.

IP address(169.254.144.79)	Difference
|0.7840-0.8320|	0.048
|0.8320-0.8680|	0.036
|0.8680-0.8970|	0.029
|0.8970-0.9159|	0.0189

Table.8.

IP address(169.254.172.64)	Difference
|0.4780-0.5460|	0.068
|0.5460-0.5580|	0.012
|0.5580-0.6110|	0.053
|0.6110-0.6340|	0.023

Table.9.

IP address(169.254.167.38)	Difference
|0.2809-0.3289|	0.048
|0.3289-0.3509|	0.022
|0.3509-0.4139|	0.063
|0.4139-0.4269|	0.013

Table.10.

IP address(169.254.120.56)	Difference
|0.3578-0.4058|	0.048
|0.4058-0.4418|	0.036
|0.4418-0.4708|	0.029
|0.4708-0.4897|	0.0189

Table.11.

IP address(169.254.130.76)	Difference
|0.4616-0.4746|	0.013
|0.4746-0.5206|	0.046
|0.5206-0.5486|	0.028
|0.5486-0.5666|	0.018

Table.12.

IP address(169.254.156.62)	Difference
|0. 5783-0.6463|	0.068
|0.6463-0.6583|	0.012
|0.6583-0.7113|	0.053
|0.7113-0.7343|	0.023

Final Sybil attackers

Table.13. Sybil attackers

IP address
169.254.144.79
169.254.167.56
169.254.172.64
169.254.156.62

IV.TEST BED DESIGN AND IMPLEMENTATION

Designing an efficient network plays an important role in this world and then it even essential part to check the performance of the designed network. This test bed entire on real time application. This test bed purely designed on c#.

4.1 TESTBED PLATFORM

This testbed used for design and implementation of our thesis work. This is real time creation of network with group of computers. This test bed works on windows platform.

4.2 TESTBED WORKING

Working of this testbed is first creating the network in ad hoc mode with connection of group of computers. It is analyzing the results in network, if it has identified any attackers then prevents that attacker with those attacker detection algorithms.

4.3 TESTBED ARCHITECTURE

4.3.1. Network Architecture for Connection

1. Bring 10/more laptops that should be exits in Ad- hoc network support IEEE802.11 a/b/g/n
2. Those Laptops contains operating system windows7/ windows8. At least one computer having Windows7 os, why because only windows 7 is shown for all Ad hoc networks.
3. Take windows7 laptop that is for your network admin (It is just for creation of network, "manets" has no infrastructure).Then Go to network and sharing center->create new network->manually create network->create adhoc-adhoc network->Type "ssid" and no password then click ok…
4. See the wifi-network on the taskbar, It shows the your "ssid" with try symbol and "waiting" label.
5. **(***windows7)**Then turn on wifi, all windows7 laptops you contains and connect the "ssid"
6. **(***windows8/8.1)** it for quite different, you must create manual network with network "ssid" with no password. And deselect "connect automatically" and click ok. Then open command prompt "run as Admin" and type command "**netsh wlan connect ssidname**"
7. Then connection was established..then check ping msg to all ip address,
8. **(***Note)**Here, The network "ping ip address" result is only for on-link (direct) connections only.. For Indirect connections you must set the routing information then it is works…**In "manets" proactive and reactive routing is there u must set any one of the following then it works.**
9. Now connection was established (total network formed), then you must provide routing protocols to the network for all indirect connections.

4.3.2 Routing protocol Needs

1. In this two issues is there 1)Direct link 2)indirect
2. Direct link no need to use routing protocols
3. Indirect link needs to the routing protocols
4. Direct link node are gives reply is success message using network **ping**
5. .Indirect link nodes are gives reply is **NOT Reachable** message using network **Ping**
6. (***Note) we have to introduce the any one of the routing protocols to communicate Indirect link nodes.

4.3.3 Finding the Network ip address

1. Open command prompt and type command "**arp –a**" and see the network information for active links of Dynamic filter.
2. Using c# to find those ip address..
3. Only direct link ip address are found here..
4. Once you have to find that ip address next we have to maintain direct link ip address at every node.
5. Direct link nodes are directly communicated no need to routing protocols as you know already

4.4 TEST BED KEY ROLES IN SYBIL ATTACKER

4.4.1 Key Points for Sybil Attacker

- Sybil attackers are two ways to attack
  1) Fabricate identities 2) Stolen identities
- Sybil attacker are create more number of identities on single physical device to gain more resources, memory..etc,
- This attackers are degrades the network performance.
- (Fabricate identities) it creates more no of identities on single physical device.
- (Stolen identities) it is stolen the other identities means stolen the ip address and mac address for the other nodes.

4.4.2 Creation of Sybil Attacker

1) Fabricate identities

Chose some ip address and mac address (dynamically /normally) generated in to the system.

First we have taken one laptop; it is connected to the ad hoc network (it is in ad hoc connection document)

Once connection was established, and then add ip address and mac address to the network in two ways. (it is done many ways but I am using two ways)

1) (Manual) open network and sharing center, click the your adhoc network, then goto ipv4, then click advanced, the add your list of ip address.

2) (C#) take the registry keys for your network, Add ip address to network.

To start communication continuously (to gain resources) using all ip address.

2) Stolen identities

To find the ip address and mac address of the other identities in the network.

Using network ping command to see, otherwise arp –a command line to see the ip address and mac address, these are only show the neighbours .
Using c# to provide all ip address and mac address of the each node in the network.
Once we choose the ip address and mac address, then add to the ip address and mac address to the network like fabricate identities process. Then start communication continuously in the network.

V. RESULTS AND ANALYSIS

Scenario 1
Nodes: 1
Attackers: 0

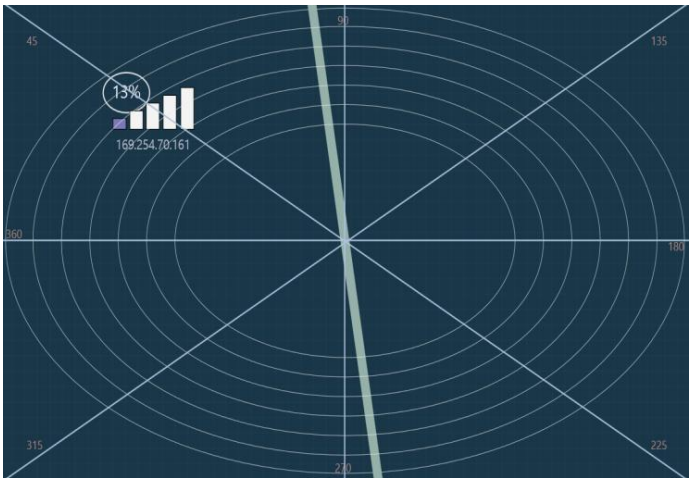

Figure.5. Testbed GUI with No Sybil Attacker

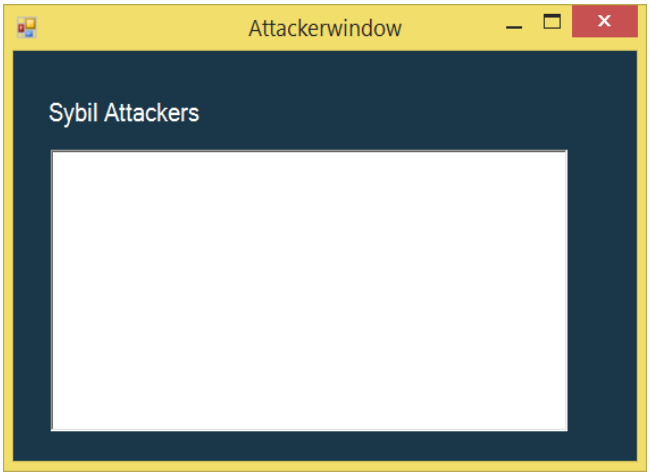

Figure.6. Testbed Attacker Window with No Sybil Attacker

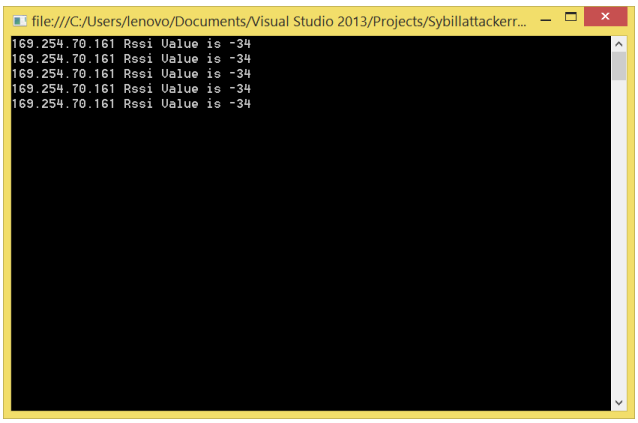

Figure.7. Existing Testbed with No Sybil Attacker

Scenario 2
Nodes: 2
Attackers: 4
Attacker node: 1 &2

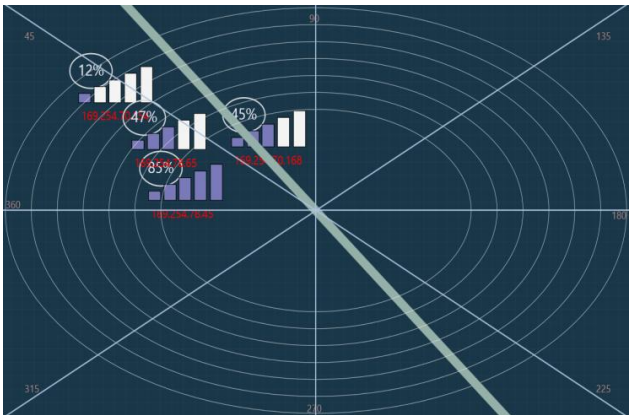

Figure.8. Testbed GUI with four Sybil Attacker

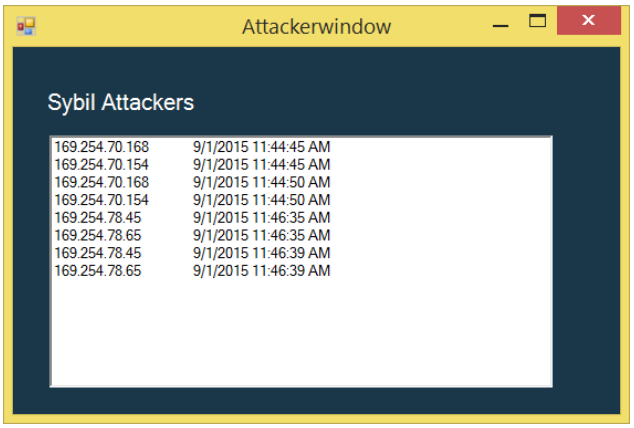

Figure.9. Testbed Attacker Window with four Sybil Attacker

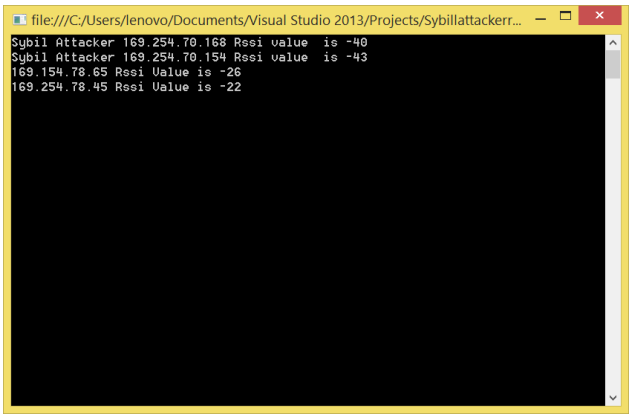

Figure.10. Existing Testbed with two Sybil Attacker

VI. CONCLUSION AND FUTURE WORK

We proposed a transmission time based detection mechanism to safeguard to the network against Sybil attacks schemed worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. We determined through various experiments that a detection threshold exists for the distiction of legitimate new nodes and new malicious identities. We confirmed this districting of legitimate new nodes and new malicious identities. We confirmed distracting through simulations and through the use of a real world test bed of Laptops. We also showed the detection accuracy. Our

future work includes tracking issues related to variable transmit powers and masquerading attacks in the network

VII. REFERENCES

[1].Chlamtac M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," Ad Hoc Netw., vol. 1, no. 1, pp. 13–64, 2003.

[2].J. R. Douceur, "The Sybil attack," presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.

[3]. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defences," presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268.

[4].B. Parno and A Perrig, "Challenges in securing vehicular networks," in Proc. 4th Workshop HotNets, 2005, pp. 1–6.

[5].K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes," in Security in Distributed and Networking Systems (Computer and Network Security). Singapore: World Scientific, 2007.

[6].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.

[7].Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2418–2434, Jun. 2010

[8].M.S.Bouassida, G.Guette ,M.Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," Int. J. Netw. Security, vol. 8, pp. 322–333, May 2009.

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

[10].A.Tangpong, G. Kesidis, H. Hung-Yuan, and A. Hurson, "Robust Sybil detection for MANETs," in Proc. 18th ICCCN 2009, pp. 1–6.

[11].T. Suen and A. Yasinsac, "Ad hoc network security: Peer identification and authentication using signal properties," presented at the Proc. 6thAnnual IEEE SMC Information Assurance Workshop (IAW), New York, Jun. 2005, pp. 432–433

VIII. AUTHOUR'S BIOGRAPHIES

B.DamodharaRao was born on 30th April 1994 Vizianagaram in Andhra pradesh. He received his B.Tech degree in Computer Science and Engineering from IIIT-RGUKT Kadapa in 2015 and currently pursuing M.Tech degree with specialization Computer Science and Engineering in TPIST, JNTU-Kakinada. This work is a part of his M. Tech project. His area of interests including C and C#.Net, Data- Structures , Operating Systems, Software Engineering and web technologies.

M.Ramesh was born Visakhapatnam in Adhra pradesh in India in 15 Aug 1991. He received his B.Tech degree in Information Technology from KPRIT JNTU-Hyderabad in 2013. .He was received the M.Tech Computer Science and Technology with Specialization Artificial Intelligence and Robotics in Andhra University College of Engineering, Andhra university Visakhapatnam in 2015. Now He is working as H.O.D and Assistant Professor in the department of Computer Science and Engineering in Thandra Paparaya Institute of Science Technologies (TPIST) Bobbili, Vizianagaram, and Andhra Pradesh from June 2016 onwards. His area of interests including C, C++ and JAVA, Web technologies, Data Mining, and Artificial Intelligence.