SADAM: Sybil Attack Detection Approach In Manets Using Testbed

[1] **M.Ramesh** B.Tech,M.Tech.
Asst Professor in Department of CSE.
Thandra Paparaya Institute of Science and Technology,
Bobbili,Vizianagaram,India

[2] **Dr.A.M.Sowjanya** M.Tech,Ph.D
Asst Professor in Department of CS&SE
Andhra University College Of Engineering, AU.
Visakhapatnam, India

Abstract*— MANET is a collection of number of nodes that formulates; either, a temporary or permanent, self-organized wireless network that don't rely on any pivotal central architecture or control. They are designed to use in situations where infrastructure network is either non-existent or its extremely costly to deploy. MANETs require a distinctive, unique and insistent identity for each node for its security protocols to be ef1'ective; Sybil attacks present a grave threat to such networks. We can create large number of logical identities in a Sybil attack on a single physical device by a selfish malicious node which gives a false impression to the network that they are different benign nodes and uses them to launch a harmonized attack against the network or a node. Node cooperation is very important for detection of Sybil attack, but unfortunately nodes may not always behave cooperatively and may collude in hostile environments for disrupting the detection accuracy of such systems. Sybil nodes cannot be accurately detected in the presence of malicious collusion which results in serious impact on detection accuracy of Sybil attacks. This paper proposed a novel scheme in order to detect a Sybil attack resistant to collusion by incorporating a trust based mechanism that would mitigate the benefit (the payof1' gained) from collusion. Experimental results show that our proposed scheme detects Sybil or whitewashers new identities accurately and reduces the benefits of collusion in the presence of mobility. Index Terms-Collusion Attack, Sybil Attack, Recommendation model, Malicious Recommendations. Fully self-controlled mobile ad hoc networks represent a complex system. Due to the broadcast nature of wireless channel, MANET has many security issues. Especially, Sybil Attack is a very serious threat to the MANET as it creates multiple virtual fake identities per entity, there by affecting the routing table. The multiple virtual identities are obtained by spoofing the victim's node or by creating an arbitrary node as there is no restriction to create an arbitrary node in MANET. In the existing system, used RSSI as a parameter to detect the Sybil node because of its lightweight but it has failed to detect the fast moving Sybil nodes. The proposed system works considering the Certification Authority as one parameter and RSSI as the other parameter. 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—Identity-based attacks, Mobility based d-hop cluster, intrusion detection, Certification Authority, Digital Certificate, Sybil attacks, component; formatting; style; styling; insert (key words)

I. INTRODUCTION

A. CELLULAR NETWORKS:

Cellular communications has experienced explosive growth in the past two decades. Today millions of people around the world use cellular phones. Cellular phones allow a person to make or receive a call from almost anywhere. Likewise, a person is allowed to continue the phone conversation while on the move. Cellular communications is supported by an infrastructure called a cellular network, which integrates cellular phones into the public switched telephone network.

Cellular communications has experienced explosive growth in the past two decades. Today millions of people around the world use cellular phones. Cellular phones allow a person to make or receive a call from almost anywhere. Likewise, a person is allowed to continue the phone conversation while on the move. Cellular communications is supported by an infrastructure called a cellular network, which integrates cellular phones into the public switched telephone network.

A cellular network provides cell phones or mobile stations (MSs), to use a more general term, with wireless access to the public switched telephone network (PSTN).[1] The service coverage area of a cellular network is divided into many smaller areas, referred to as cells, each of which is served by a base station (BS). The BS is fixed, and it is connected to the mobile telephone switching office (MTSO), also known as the mobile switching center. An MTSO is in charge of a cluster of BSs and it is, in turn, connected to the PSTN. With the wireless link between the BS and MS, MSs such as cell phones are able to communicate with wireline phones in the PSTN. Both BSs and MSs are equipped with a transceiver.

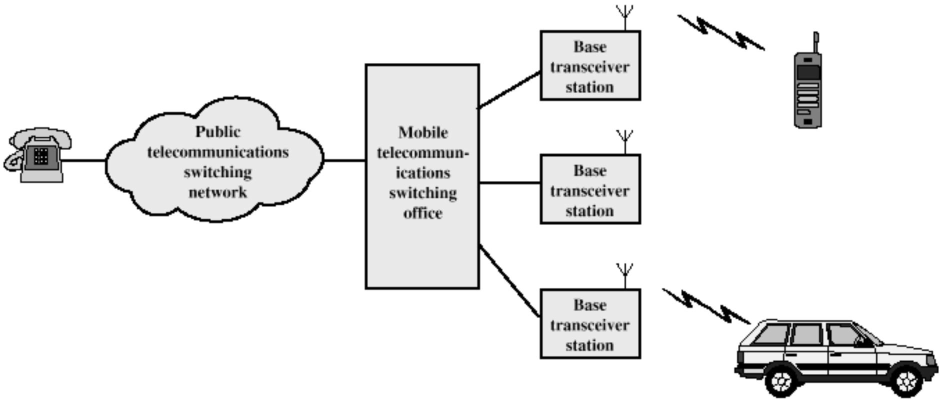
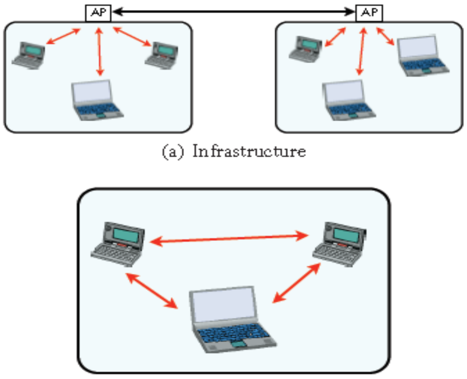

Public telecommunications switching network
Mobile telecommun-ications switching office
Base transceiver station
Base transceiver station
Base transceiver station

FIG (A) TYPICAL CELLULAR NETWORK

B. AD-HOC NETWORKS:

The word ad hoc is from Latin and means “for this (only)”.In the case of computer networks, the ad hoc networks mean wireless network without infrastructure, they can be called spontaneous network. Ad hoc is defined as “Arranged or happening when necessary and not planned in advanced” according to oxfords advanced learners dictionary. Furthermore ad hoc networks are usually such networks that are set up for one time occurrences such as conferences or military operations.[2] This can be paraphrased into the following definition an ad hoc network is a flexible and adaptive network with no fixed infrastructure. Wireless ad hoc networks are collections of wireless nodes, that communicate directly over a common wireless channel. The nodes are equipped with wireless transceiver. They don’t need any additional infrastructure, such as base station or wired access point, etc. Therefore, each node doesn’t only plays the role of an end system, but also acts as a router, that sends packets to desired nodes. One Way to understand ad hoc networks is by comparing them with infrastructure based wireless networks, such as cellular network and WLAN.[3] In the infrastructure based wireless networks a node can only send a packet to a destination node only via access point (in cellular network like GSM, it is called base station). The access point establishes an network area and only the nodes in this area can use access point’s services. There are some unknown events, which cause access point’s malfunction. The nodes lose their network and they are quasi not working. It is the biggest disadvantage of infrastructure based networks.



(a) Infrastructure

(b) Ad-Hoc

FIG (B) DIFFERENCE BETWEEN INFRASTRUCTURED NETWORK AND AD HOC NETWORK

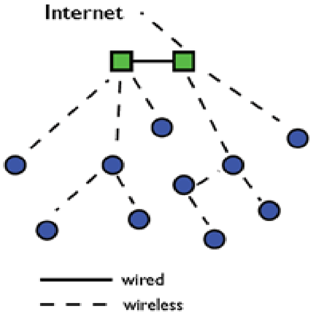


FIG (B.1) COMBINATION OF INFRASTURCTURE AND ADHOC NETWORKS

C. MANETs :

A Mobile Ad-hoc Network (MANET) is a set of wireless mobile nodes forming a dynamic and infrastructure less network. Thus it is also known to be a Self-configuring network formed with wireless connections using a set of wireless mobile nodes. Nodes can communicate with each other without any centralized authority or base stations that could manage the communication in the network. In MANET there is no physical connection between the mobile nodes so they follow the hop-to-hop method to forward the packets and communicate with any other mobile node in the network.[4] In MANETs, every node acts as a router, client and host as well and its topology is dynamic as nodes join the network whenever there is need to transmit the data and leave the network when transmission gets over. [1]Thus the nodes are independent to move freely in the network and organize themselves according to the transmission requirements. For this reason the network topology of MANET is not static as it tends to change rapidly. For a communication of any two nodes, the destination node must lies within the radio range of the source node that wants to initiate the communication.

FIG (C) MOBILE AD HOC NETWORK

II. SYBIL ATTACKS IN MANETS

A) 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. [3][11]A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network.[4][9] In this research, we propose a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations and real-world test bed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility[10].

B) 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 misbehavior 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,[11] a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. [12]In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network[6] 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)[8].

In this pare, i 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 behavior 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 testbed 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.[3][2] 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[9].

C) DETECTION OF SYBIL ATTACKS:

I) 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. [9]The difference between the two is only the notion of simultaneity; however, their applications and consequences are different

II) 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,[11] 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.

III) Detection:

I 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 .In order to detect new identities spawned by a whitewasher or Sybil attacker, Algorithm 1 checks every received RSS by passing it to the addNewRss 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).[11] 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.

The complexity, in terms of operations, of Algorithm 1 is O(1) and Algorithm 2 is O(n).

C) FAILURES IN THE EXITING SYSTEM:

- It is failed to detect the stolen identities of Sybil attackers.
- It is fail to detect when the Sybil attacker changes continuously ip address and Mac address.
- 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.

III. IMPLEMENTATION OF RESEARCH

A) PROPOSED ANALYSIS:

In this paper I proposed to find all Sybil attackers based on the Transmission Times. The key roles in my proposed system is to decrease the False positive rate and Increase the Throughput of the network.

i) Methodology:

Sybil attackers are two ways to attack stolen identities and fabricate identities. Here we are build to algorithms to detect and prevent Sybil attackers.

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 reaches five then those list of table transferred to proposed_sybil_attacker_detection function then it returns the Sybil 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 identify the List of five tables from network nodes.

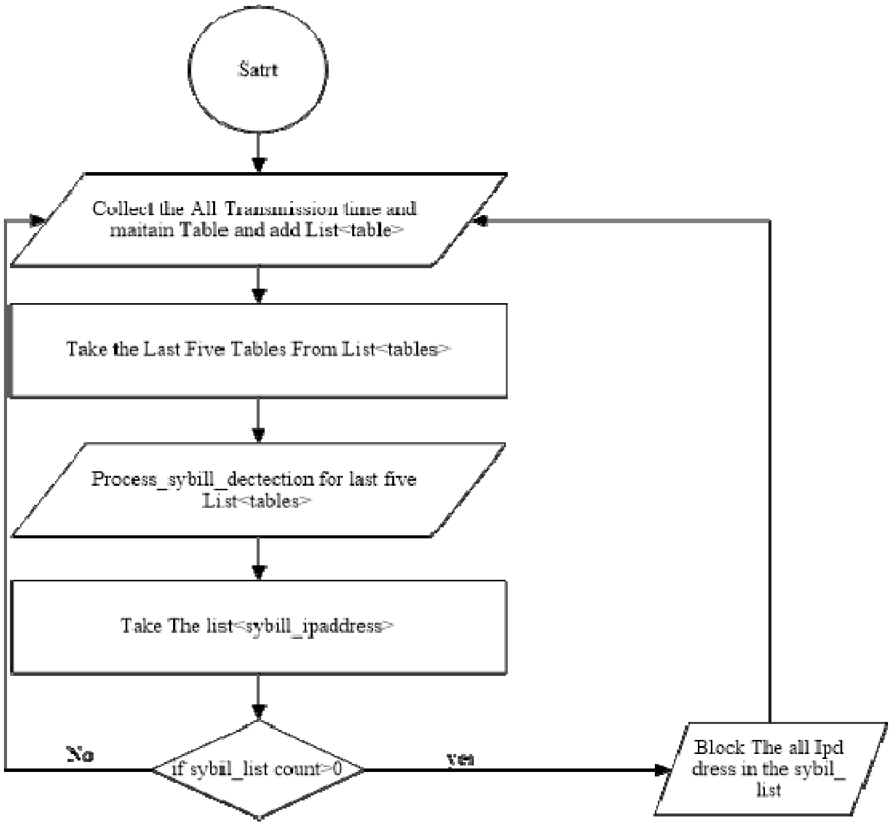
Step1: Collect the all the transmissions times for connected nodes. And maintain table list<ipaddress,Transmission_time_micro_sec>.

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>.


Satrt
Collect the All Transmission time and maitain Table and add List<table>
Take the Last Five Tables From List<tables>
Process_sybill_dectection for last five List<tables>
Take The list<sybill_ipaddress>
if sybil_list count>0
No
yes
Block The all Ipd dress in the sybil_ list

A) FLOWCHART FOR FORMING THE 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>.

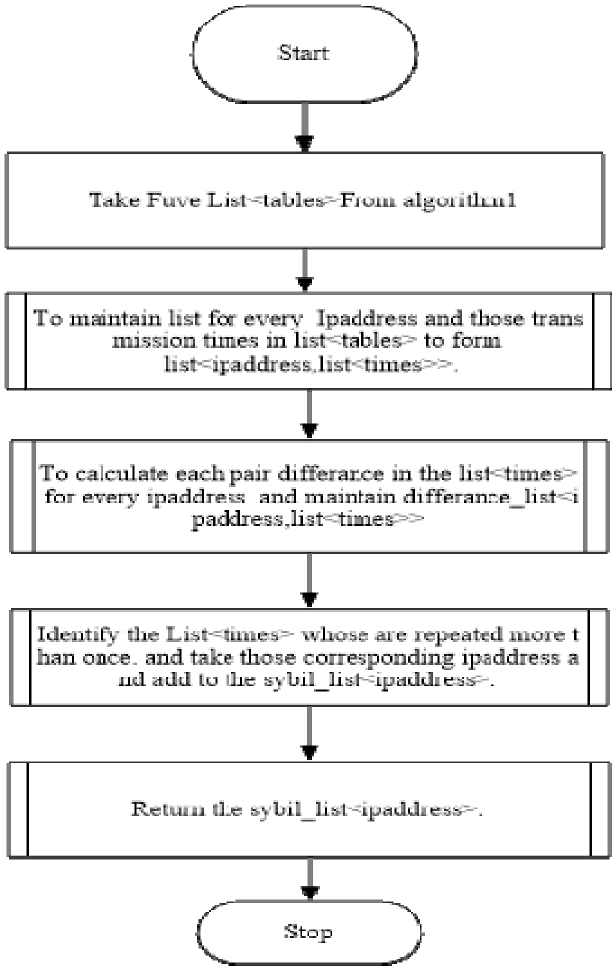
Step4: Calculate the every pair of values in the list and find the difference of that and maintain the list and the those list into to Final_list<ipaddress,list<transmission_time>>.

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.

B) FLOW CHART FOR DETECTING SYBIL ATTACKERS


Start
Take Fuve List<tables>From algorithm1
To maintain list for every Ipaddress and those trans mission times in list<tables> to form list<ipaddress,list<times>>.
To calculate each pair differarce in the list<times> for every ipaddress and maintain differance_list<i paddress,list<times>>
Identify the List<times> whose are repeated more t han once. and take those corresponding ipaddress a nd add to the sybil_list<ipaddress>.
Return the sybil_list<ipaddress>.
Stop

Experimental results of these algorithm is in the below tables.

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

First table

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
169.254.130.76	0.4616
169.254.156.62	0.5783

The above table construct based on flow chart .it is the first table of the detecting Sybil attackers similarly four more tables are designed up to fifth table on the base of first table

Difference Tables

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|	0.018

Ip Address
169.254.144.79
169.254.167.56
169.254.172.64
169.254.156.62

Final Sybil attackers .

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 testbed purely designed on c#.

➔ 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 testbed works on windows platform.

➔ TESTBED WORKING:

Working of this testbed ,is first create the network in ad-hoc mode with connection of group of computers. it is analyze the results in network, if it has identify any attacker then prevent those attacker with those attracter detection algorithms.

➔ TESTBED ARCHITECTURE:

Network Architecture for Connection:

- Bring 10/more laptops that should be exits in Adhoc network support IEEE802.11 a/b/g/n
- Those Laptops contains operating system windows7/windows8 .At least one computer having Windows7 os, why because only windows 7 is shown for all Adhoc networks.
- Take windows7 laptop that is for your network admin(It is just for creation of network , "manets" has no infrastructure).Then Goto network and sharing center->create new network->manually create network->create adhoc-adhoc network->Type "ssid" and nopassword then click ok…
- See the wifi-network on the taskbar ,It shows the your "ssid" with try symbol and "waiting" label.
- **(***windows7)**Then turn on wifi, all windows7 laptops you contains and connect the "ssid"
- **(***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**"
- Then connection was established ..then check ping msg to all ipaddress,
- **(***Note)**Here,The network "ping ipaddress" 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.**
- Now connection was established (total network formed),then you must provide routing protocols to the network for all indirect connections.

Routing protocol Needs

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

Finding the Network ip address

- Open command prompt and type command "**arp –a**" and see the network information for active links of Dynamic filter.
- Using c# to find those ip address ..
- Only direct link ipaddress are found here ..
- Once you have to find those ipaddress next we have to maintain direct link ipaddress at every node.

- Direct link nodes are directly communicated no need to routing protocols as you know already.

➔ **TEST BED KEY ROLES IN SYBIL ATTACKER:**

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 create 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.

V. Results And Analysis

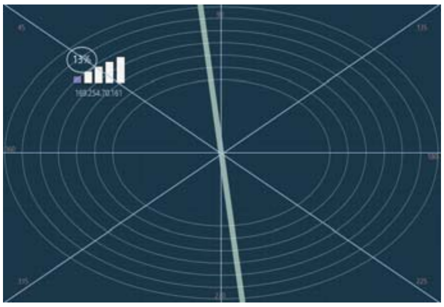
In Results analysis scenario to solve the Sybil attackers by using testbed. The following possible scenarios having nodes and attackers. Here we check all the possibilities of nodes if occur any attackers then we apply the testbed process to remove the attackers. The following scenarios shows the all possibility of attackers with testbeds. The following scenarios consist of three situations i) testbed GUI with Sybil Attackers ii) testbed attacker window Sybil attacker.iii) Existing testbed with sybil attackers.. the following scenarios performs at different no of nodes..

The following scenario having one node and attackers are zero. The first step testbed GUI with no Sybil attackers. In second step displays the testbed window with no Sybil attackers. In third step display the existing testbed with no Sybil attackers. Similarly all four scenarios displays the above the steps with their available attackers.

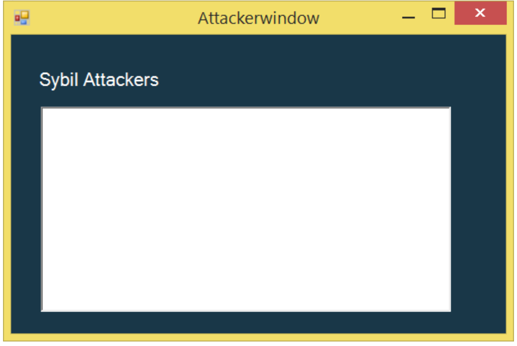
Scenario 1:

Nodes:1

Attackers:0

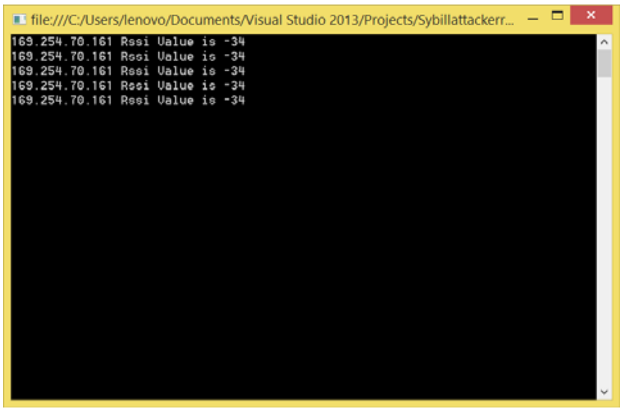


A) TESTBED GUI WITH NO SYBIL ATTACKER



Sybil Attackers

B) TESTBED ATTACKER WINDOW WITH NO SYBIL ATTACKER


file:///C:/Users/lenovo/Documents/Visual Studio 2013/Projects/Sybillattackerr...

```
169.254.70.161 Rssi Value is -34
169.254.70.161 Rssi Value is -34
169.254.70.161 Rssi Value is -34
169.254.70.161 Rssi Value is -34
169.254.70.161 Rssi Value is -34
```

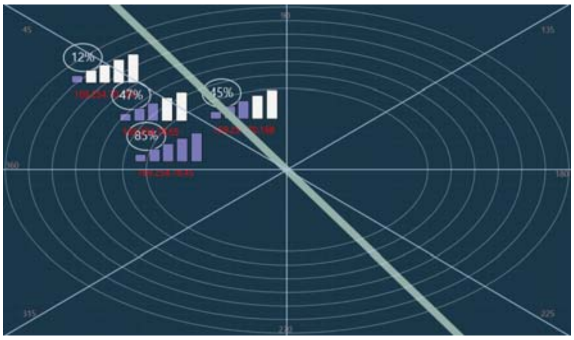
C) EXISTING TESTBED WITH NO SYBIL ATTACKER

Scenario4:

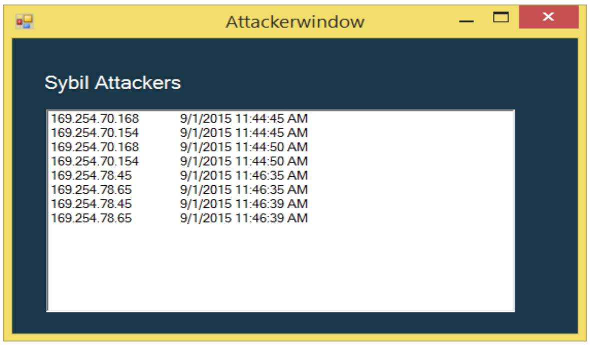
Nodes:2

Attackers:4

Attacker node:1 &2



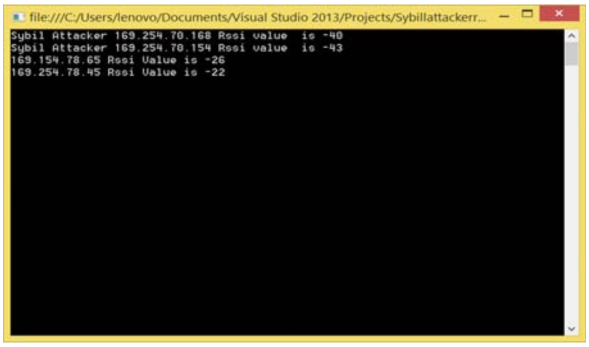
a) TESTBED GUI WITH FOUR SYBIL ATTACKERS WINDOW



Sybil Attackers

```
169.254.70.168     9/1/2015 11:44:45 AM
169.254.70.154     9/1/2015 11:44:45 AM
169.254.70.168     9/1/2015 11:44:50 AM
169.254.70.154     9/1/2015 11:44:50 AM
169.254.78.45      9/1/2015 11:46:35 AM
169.254.78.65      9/1/2015 11:46:35 AM
169.254.78.45      9/1/2015 11:46:39 AM
169.254.78.65      9/1/2015 11:46:39 AM
```

b) ATTACKER WINDOW WITH FOUR SYBIL ATTACKERS


file:///C:/Users/lenovo/Documents/Visual Studio 2013/Projects/Sybillattackerr...

```
Sybil Attacker 169.254.70.168 Rssi value  is -40
Sybil Attacker 169.254.70.154 Rssi value  is -43
169.154.78.65 Rssi Value is -26
169.254.78.45 Rssi Value is -22
```

c)EXISTING TESTBED WITH TWO SYBIL ATTACKERS

In scenario 4 occurs four Sybil attackers ,here testbed GUI with four Sybil attackers so the attackers window consist of four Sybil attackers but the existing testbed with two Sybil attackers only. This approach detect the Sybil attackers using testbed.

VI. Conclusion And Future Work

I proposed an transmission time based detection mechanism to safeguard the network against Sybil attacks. Scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. We demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities. We confirmed this distinction rationale through simulations and through the use of a real-world test bed of Laptops. We also showed the detection accuracy. future work includes tackling issues related to variable transmit powers and masquerading attacks in the network.

Acknowledgment

This paper is made possible through the help and support from everyone, including: My Guide Dr. A.M. Sowjanya professor in Department Computer Science & System Engineering in Andhra university Visakhapatnam.I sincerely thank to TPIST Engineering college . The product of this paper would not be possible without all of them.

References

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

[2] I. 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.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] B. Xiao, B. Yu, and C. Gao, "Detection and localization of Sybil nodes in VANETs," presented at the Proc. 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, 2006, pp.1–8.

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

[12] T. Suen and A. Yasinsac, "Ad hoc network security: Peer identification and authentication using signal properties," presented at the Proc. 6th

Author's Biographies

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 Assistant Professor in the department of Computer Science and Engineering in Thandra Paparaya Institute of Science Technologies (TPIST) Bobbili, Vizianagaram, Andhra Pradesh from June 2016 onwards. His area of interests including C,C++ and JAVA, Web technologies, Data Mining, and Artificial Intelligence.

Dr.A.M.Sowjanya received her M.Tech and Ph.D. Degree in Computer Science and technology from Andhra University. She is presently working as an Assistant Professor in the Department of Computer Science and Systems Engineering, College of Engineering (Autonomous), Andhra University. Her areas of interest include Data Mining, incremental clustering and Big Data.