7th International Conference on Recent Innovations in Science, Engineering and Management
The Institutions of Engineers, Delhi State Center (India) RISEM - 16
16th September 2016, www.conferenceworld.in ISBN : 978-93-86171-07-8

ANALYSIS OF LIGHTWEIGHT SYBIL ATTACK DETECTION TECHNIQUE IN MANET

Vrushali Kelatkar[1], Prof. Pravin Dere[2]

[1]*P.G Student: Electronics and telecommunication, Alamuri Ratnmala Institute of Engineering and Technology, Mumbai, India*

[2]*Assistant Prof: Electronics and telecommunication, Terna Engineering College, Nerul, Navi Mumbai, India*

ABSTRACT

A set of mobile nodes which can communicate directly with other nodes within its transmission range and use multihop routing for nodes outside its transmission range is called Mobile Ad hoc Network (MANET). The infrastructure less nature (bandwidth, memory and battery power) of MANET makes it susceptible to various attacks. 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 discrete and persistent identity per node in order for their security protocols to be workable, Sybil attacks create a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a synchronized attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of responsibility in the network It is strongly desirable to detect Sybil attacks and eliminate them from the network. This paper proposes a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any additional hardware, such as directional antennae or a geographical positioning system.

Keyword: *MANETs, Sybil attack, RSS, Legitimate*

I. INTRODUCTION

A Mobile Ad hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. A Sybil attacker can cause damage to the ad hoc networks in several ways (6) such as 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.

Usually Sybil attacks are reduced, using cryptographic-based authentication or trusted certification (7). 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. However, this approach requires extra hardware, such as directional antennae or a geographical positioning system (GPS).

II. PROPOSED SYSTEM

In this work, lightweight sybil attack technique is used to detect the malicious sybil nodes. In this technique there is no extra requirement of hardware or antenna therefore it is called as lightweight technique. This technique is used in wireless ad hoc network, so in this work, authenticate global instructor is used to protect the network from Sybil attack.

To remove the sybil attack we introduce a lightweight authority known as global instructor which will authenticate all the communication occurring between any source and destination. So for all communication the GI or global instructor will act as a an intermediate relay node. If any sybil node tries to get data from any authenticate node then the communication pattern does not involved the GI. So the data is drop by the router, there by defecating sybil attack.

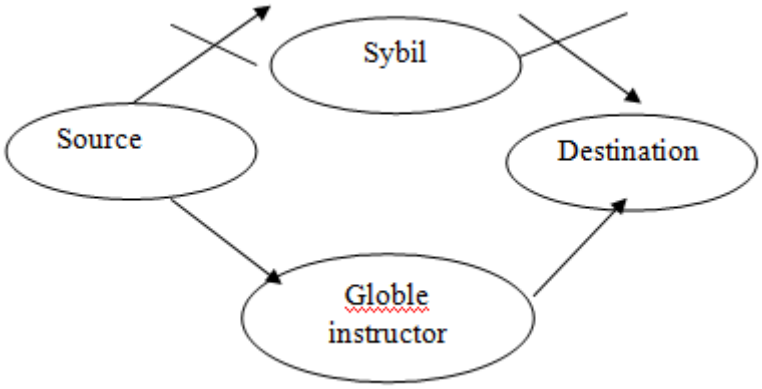

Fig 1: Remove Sybil attack through authenticate GI.

2.1 Algoritham

1. Form the network: The wireless networking model can be created using Tool Command Language (TCL) script with fixed number of nodes. Nodes are configured with the components of channel, networking interface, radio propagation model, Medium Access Control (MAC) protocol, adhoc routing protocol, interface queue, link layer, topography object, and antenna type.

2. Introduce Sybil attack: here is always a threat to open-access distributed systems like peer-to-peer systems from Sybil attacks, where a ill-willed user creates many fake identities known as Sybil nodes. Unless a reliable

central authority is organized to bond identities to real persons, safeguarding against Sybil attacks is a serious problem.

3. Perform sybil attack detection: If a single malicious node is able to convince its neighbors by presenting multiple identities, it will have control over the substantial portion of the network and can adversely affect the functioning of this network.

4. Remove nodes which have sybil attack: in this paper, Authenticate global instructor is used to protect the network from Sybil attack.

5. Result analysis: In this we analyze and identify the attack through parameter. In all the graphs, on X axis we have simulation time, and on Y axis we have the parameter. Delay, Jitter and Energy should be low for the green line, and high for the red line, Throughput, PDR should be low for red and high for green.

2.2 Network Simulator:

Network simulator is a package of tools that simulates behavior of networks such as creating network topologies, log events that happen under any load, analyze the events and understand the network.

2.2.1 Platform required to run network simulator

- Unix and Unix like systems
- Linux (Use Fedora or Ubuntu versions)
- Free BSD
- SunOS/Solaris
- Windows 95/98/NT/2000/XP

Category	Network Simulator Name
Commercial	OPNET, QualNet
Open Source	NS2, NS3, OMNET++, SSFNet, J-Sim

Table1: Network Simulators

2.2.1 Network Simulator – 2 (Ns2)

The one of the most widely used network simulators and object-oriented discrete-event network simulator is NS-2 that was originally developed at Lawrence Berkeley Laboratory at the University of California. Basically it was designed for network research community to simulate routing algorithms, TCP/IP protocols and multicast. It is written in C++ and uses OTcl as a command and configuration interface.

Features of NS2:

1. It is a discrete event simulator for networking research.

2. It provides substantial support to simulate bunch of protocols like TCP, FTP, UDP, HTTP and DSR.

3. It simulates wired and wireless network.

4. It is primarily Unix based.

5. Uses TCL as its scripting language.

6. Otcl: Object oriented support

7. Tclcl: C++ and otcl linkage

III. PERFORMANCE EVOLUTION

Parameters used for performance measurement are following:

1.Delay : A specific packet is transmitting from source to destination and calculates the difference between send times and received times.

Fig 2 shows the delay graph it indicate simulation time on X-axis and parameter delay on Y-axis.

Table 1 shows the delay is more in attack i.e. sdelay as compared to without attack i.e. Rem_sdelay.

Packet delay = packet receive time – packet send time.

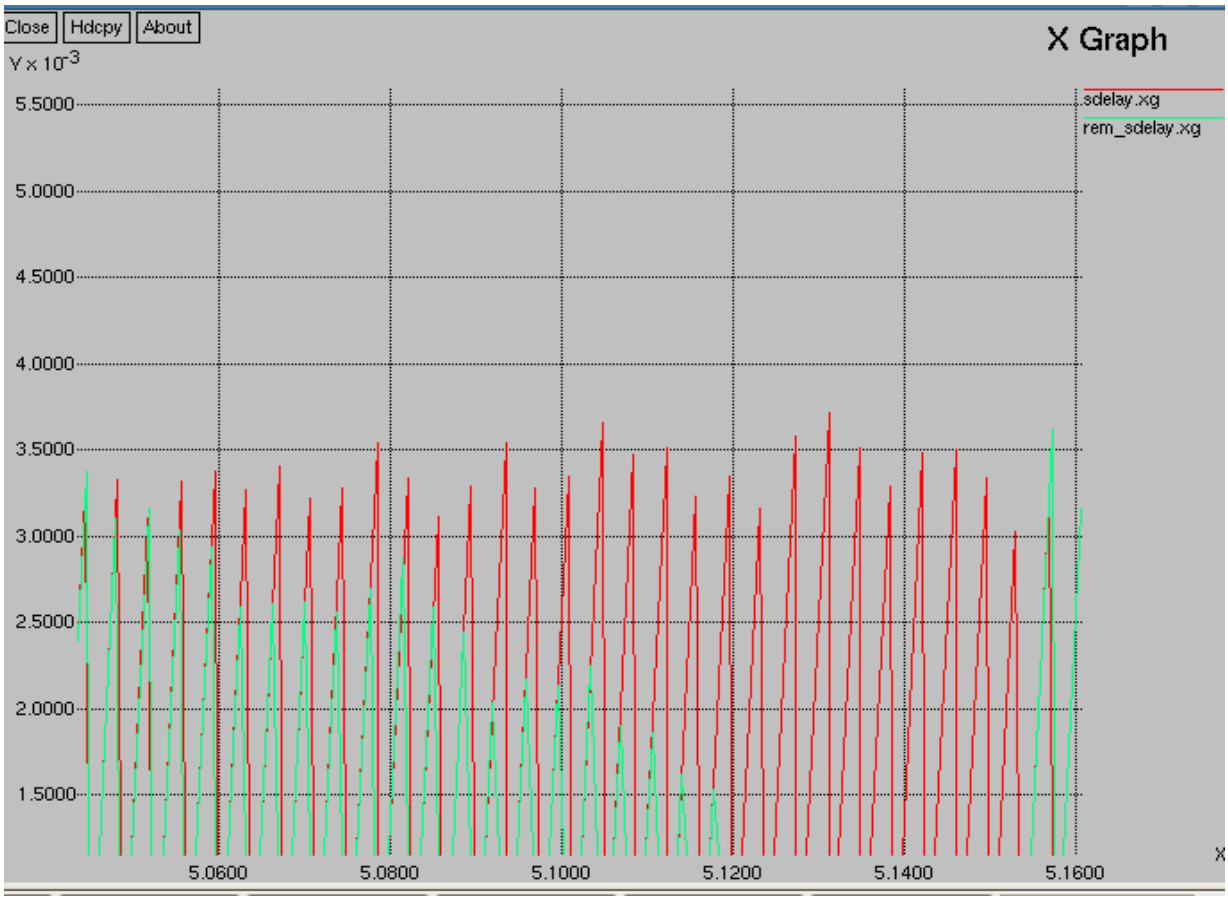

Fig 2: Delay

Sdelay		Rem_sdelay	
Parameter	Simulation time	Parameter	Simulation time
5.060000	0.000000	5.060000	0.000000
5.063273	0.003273	5.063750	0.000000
5.070725	0.003225	5.082500	0.000000
5.082087	0.003337	5.082500	0.000000
5.100853	0.003353	5.101250	0.000000
5.112263	0.003513	5.112500	0.000000
5.123161	0.003161	5.123750	0.000000
5.142235	0.003485	5.142500	0.000000

Table 2: delay analysis

2. PDR : Packet Delivery ratio is the ratio of actual packet delivered to total packets sent. Fig 3 shows delay graph it shows simulation time on X-axis and performance parameter i.e. packet delivery ratio (PDR) on Y-axis. PDR is high in without attack that is rem_spdr as compared to with attack as shown in table 3.

PDR = no. of packets receive at destination node/no. of packets at source node.

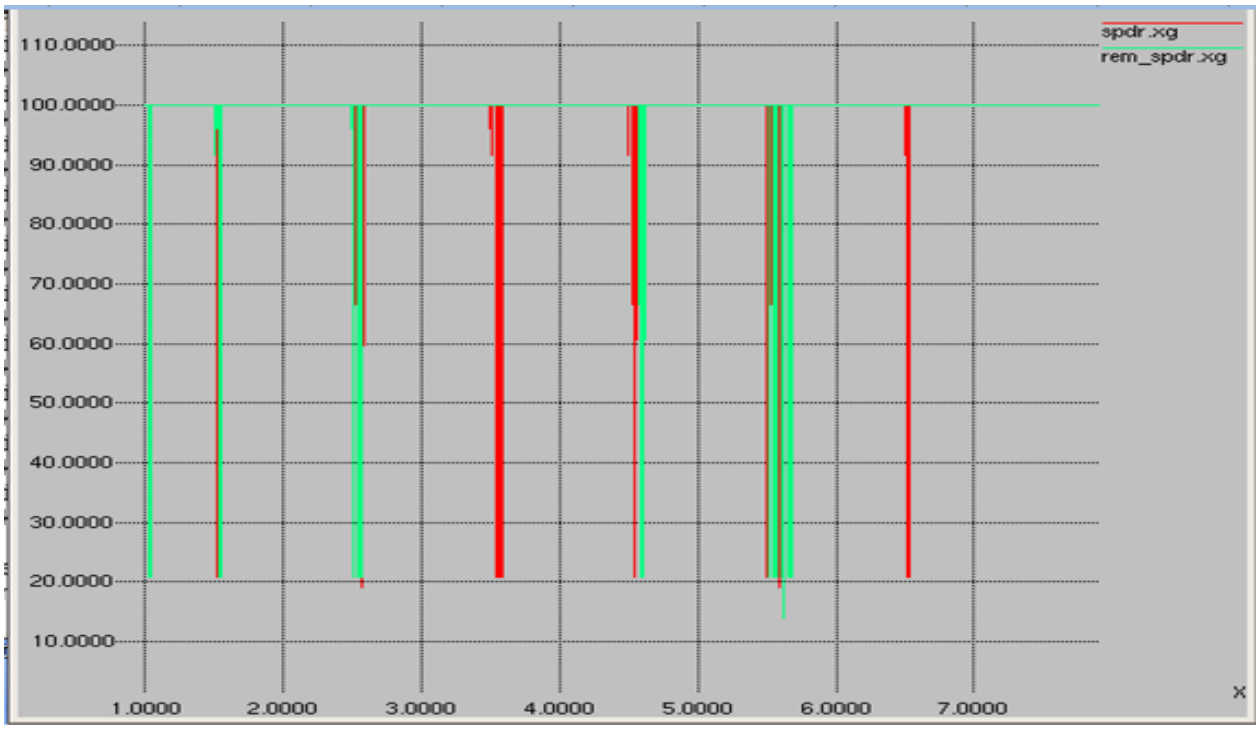

Fig 3: PDR

Spdr		Rem_spdr	
Parameter	Simulation time	Parameter	Simulation time
1.000000	100.000000	1.000000	100.000000
2.504193	91.666607	2.502500	100.000000
2.526912	66.666667	2.526250	100.000000
2.546535	20.8695	2.546789	100.000000
2.575487	19.130435	2.574504	100.000000
3.503142	91.666667	3.503750	100.000000
4.503122	91.666667	4.503201	91.000000
6.502681	91.666667	5.501488	100.000000
6.511367	20.869565	6.511306	100.000000

Table 3: PDR analysis

3.Jitter : Jitter is any deviation in signal or displacement in signal pulse in high frequency digital signal.

as shows from fig 4, jitter graph it indicates simulation time on x- axis and performance parameter that is jitter on y-axis table 3 shows jitter is low in without attack as compared to with attack.

Jitter = Delay – mean delay.

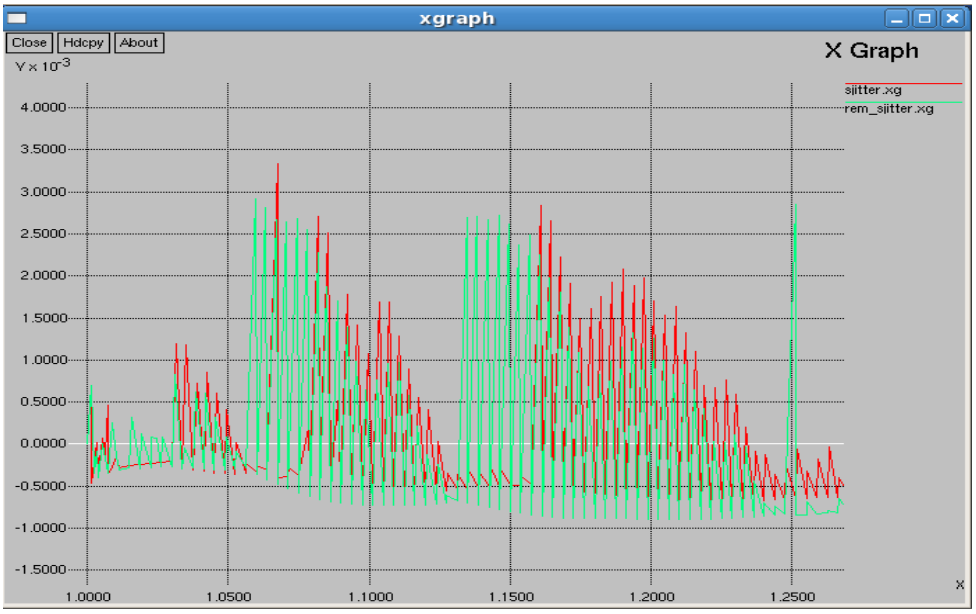

Fig 4: jitter

Sjitter		Rem_sjitter	
Parameter	Simulation time	Parameter	Simulation time
1.067444	0.003340	1.067500	-0.000482
1.078507	0.000200	1.078750	-0.000626
1.082500	-0.00407	1.082500	-0.000661
1.085476	0.002515	1.085072	0.001873
1.092265	0.001776	1.092125	0.001394
1.101250	-0.000508	1.101250	-0.000722
1.107243	0.001655	1.108750	-0.000727

Table 4: jitter analysis

4.Thoughtput : throughput is no bits received per unit time. as shows from fig 5, throughput graph it indicates simulation time on x- axis and performance parameter that is throughput on y-axis table no. 4 shows throughput is low in without attack as compared to with attack because unwanted packets are not received at destination and only required authenticated packets are received

Throughput = no. of bits received/time

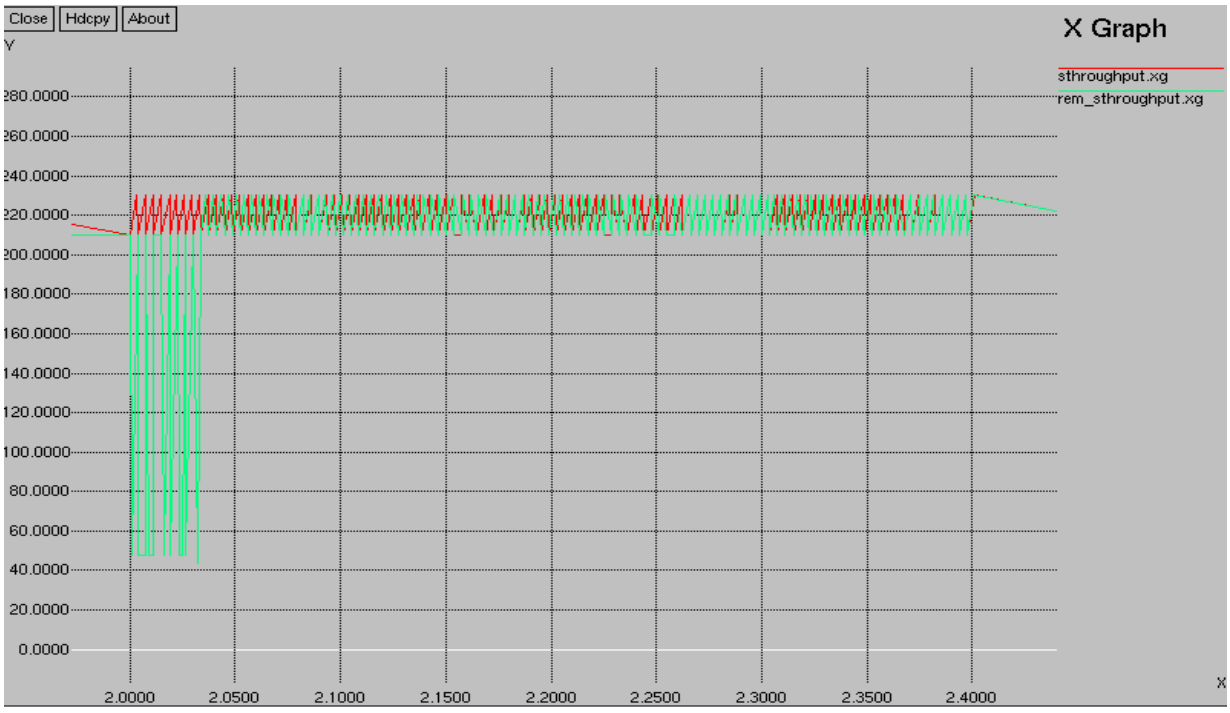

Fig 4: Throughput

S_thrghput		Rem_sthroughput	
Simulation time	Parameter	Simulation time	Parameter
2.007	210	2.007	48
2.02	210	2.02	210
2.04	230	2.04	210
2.041	230	2.041	210
2.05	230	2.05	210

Table 5: Throughput analysis

IV. CONCLUSION

It is observed that various factors affect the detection accuracy, such as network connections, packet transmission rates, node density, and node speed. Based on the above theory we conclude that our scheme works better even in mobile environments and can detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy. It is a developed and improved lightweight sybil attack detection technique. In this we used three parameter i.e. delay, PDR, Jitter and throughput. In this work throughput of the network is increased and number of sybil nodes are decreased .It implies that through RSS lightweight sybil attack detection technique network becomes more secure.

REFRENCES

[1] Sivakumar B, Gracy Theresa W "SURVEY ON SYBIL ATTACK DETECTION TECHNIQUES IN MOBILE AD HOC NETWORKS" International Journal of Science Technology & Management Volume No.04, Special Issue No.01, February 2015 ISSN (Print) 2394-1529, (Online) 2394-1537

[2] Sangeeta Bhatti, Prof Meenakshi Sharma." A Review of Sybil Attack in Mobile Ad-hoc Network" International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE) Volume 1, Special Issue , ICCICT 2015. Impact Factor: 1.036, Science Central Value: 26.54

[3] P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan, "Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network" International Journal of Communication and Computer Technologies Volume 02 – No.02 Issue: 02 March 2014 ISSN NUMBER: 2278-9723

[4] S.Abbas, M.Merabti, and D.Llewellyn-Jones "Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks" School of Computing and Mathematical Sciences Liverpool John Moores University Byrom St. Liverpool, L3 3AF, UK

[5] A. Amalorpava Preethi, and R. Boopathiraj" Detection of Sybil Attack using Received Signal Strength and Masquerade Attack using Mutual Guarding" International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 11 No. 2 Nov. 2014, pp. 520-526 © 2014 Innovative Space of Scientific Research Journals http://www.ijisr.issr-journals.org

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

[7] R. Kanni Selvam , Mr.C.Karthikeyan M.E "Identifing The Sybil Node By Using Lightweight Scheme In Mobile Ad hoc Network" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 5, May 2014

[8] Himika Sharma, Roopali Garg "Enhanced lightweight Sybil attack detection technique" 978-1-4799-4236-7/14/$31.00 2014 © IEEE

[9] Roopali Garg, Himika Sharma "Proposed Lightweight Sybil Attack Detection Technique in MANET" International Journal of Advanced Research in Electrical, Electronics and nstrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 5, May 2014

[10] K. Kayalvizhi1, N. Senthilkumar, G. Arulkumaran "Detecting Sybil Attack by Using Received Signal Strength in Mantes" International journals of Innovative research in science and engineering (IJIRSE) (Online) 2347-3207.

[11] RoopaliGarg, Himika Sharma "Comparison between Sybil Attack Detection Techniques: Lightweight and Robust" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 2, February 2014 Copyright to IJAREEIE www.ijareeie.com 7142

[12] Rakesh G.V , Shanta Rangaswamy , Vinay Hegde , Shoba G "A Survey of Techniques to Defend Against Sybil Attacks in Social Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014

[13] A. Amalorpava Preethi and R. Boopathiraj "Detection of Sybil Attack using Received Signal Strength and Masquerade Attack using Mutual Guarding" International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 11 No. 2 Nov. 2014, pp. 520-526

[14] K.Vaijayanthi, M.Baskar, M.Sc., M.Phil. "DETECTING AND RESOLVING THE SYBIL ATTACK IN MANET USING RSS ALGORITHM" IJCSMC, Vol. 3, Issue. 11, November 2014, pg.233 – 24.

[15] Chris Piro Clay Shields Brian Neil Levine D "Detecting the Sybil Attack in Mobile Ad hoc Networks"