Detection on Sybil Attack in MANET

Jyoti Parmar
Department of Computer Engineering
C. U. Shah Engineering and Technology

Abstract- *Mobile Ad Hoc Network (MANET) is a collection of mobile nodes that dynamically form a temporary network without infrastructure. It has many numbers of applications mainly in the areas of Sensor Networks (SN), medical, military and rescue operations. Routing is an important component in mobile ad hoc networks and it has several routing protocols, which are affected from different attacks. Ad hoc On Demand Distance Vector (AODV) is one of the most suitable routing protocols for the MANETs and it is more vulnerable to Black hole attack and Sybil attack by the malicious nodes. A malicious node that incorrectly sends the RREP (route reply) that it has a latest route with minimum hop count to destination and then it drops all the receiving packets. This is called as black hole attack. In the case of multiple malicious nodes that work together with cooperatively, the effect will be more. This type of attack is known as cooperative black hole attack. In this paper, we have surveyed and compare the existing solutions to black hole attacks on AODV protocol and their drawbacks.*

Keywords- MANETs, AODV, Malicious node, Sequence Number

I. INTRODUCTION

MANETs being an emerging technological field is an active area of research and has found usage in a variety of scenarios like emergency operations, disaster relief, military service and taskforces. Providing security to the nodes and their data communication in such scenarios is critical. A mobile adhoc network (MANET) is a self configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network [1,3]. Mobile Adhoc Network (MANET) [1] is a set of mobile devices like laptops, PDAs, smart phones which communicate with other over wireless links without a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network using single hop or multi hop communication. There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentially. Active attacks, including injecting packets to invalid destinations into contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication [11,12]. The characteristics of MANET like dynamic topology, lack of fixed infrastructure, vulnerability of node sand communication channel, lack of traffic concentration points, limited power, computational capacity, memory, and bandwidth make the task of achieving a secure and reliable communication more difficult. Attacks like sleep deprivation, jamming transmission channel with garbage packets, Black hole, Grey hole, Warm hole and Dos. The selfish nodes may not participate in routing and forwarding packets leading to loss of packets. This paper is a survey of different Intrusion Detection System proposed for MANETs based on the irarchitecture

II. ROUTING PROTOCOLS IN MANETs

Routing is the process of information exchange from one host to the other host in a network [4]. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, Traffic, Security, etc. In Ad-hoc network each host node acts as specialized router itself [3].

Different Strategies:

Routing protocol for ad-hoc network can be categorized in three strategies.

1) Pro-active routing protocol
2) Re-active routing protocol
3) Hybrid protocol

A. Proactive (table driven) Routing Protocol

The pro active routing is also known as table- driven routing protocol. In this routing protocol, mobile nodes periodically broadcast the irrouting information to the neighbor's nodes. Each node needs to maintain the irrouting table of not only adjacent nodes and reachable nodes but also

the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familier types of the proactive routing protocol are:- Destination sequenced distance vector (DSDV) routing protocol [5] and Optimized link state routing (OLSR) protocol [6].

B. Reactive (on demand) Routing Protocol

The reactive routing protocol is equipped with another application named on-demand routing protocol. In compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Here we briefly describe two prevalent on-demand routing protocols which are:-Adhoc On-Demand Distance Vector (AODV) [7] and Dynamic source routing (DSR) [8] protocol.

C. Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are:- Zone Routing Protocol (ZRP) [9], and Temporally-Ordered Routing Algorithm (TORA) [10].

III. ADHOC ON DEMAND ROUTING PROTOCOL

AODV combines some properties of both DSR and DSDV. It uses route discovery process to cope with routes on demand basis. It uses routing tables for maintaining route information. It is reactive protocol. It doesn't need to maintain routes to nodes that are not communicating. AODV handles route discovery process with Route Request (RREQ) messages. RREQ message is broadcasted to neighbor nodes. The message floods through the network until the desired destination or a node knowing fresh route is reached. Sequence numbers are used to guarantee loop freedom. RREQ message cause by passed node to allocate route table entries for reverse route.

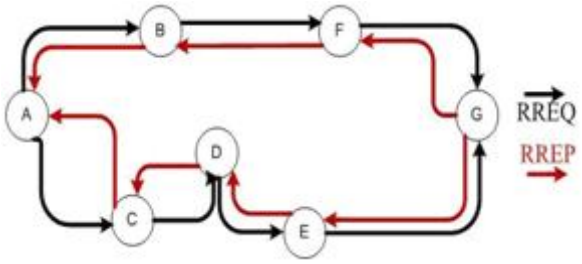

Fig 1. AODV routing protocol with RREQ and RREP messages

The destination node unicasts a Route Reply (RREP) back to the source node. Node transmitting a RREP message creates routing table entries for forward route. Fig 1. Shows, AODV routing protocol with RREQ and RREP message [14].

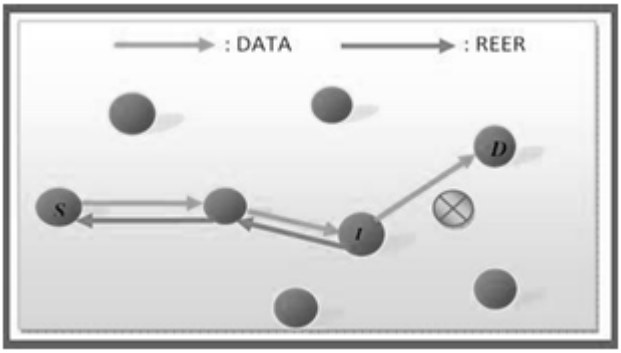

Fig 2. AODV routing protocol with RERR message.

For route maintenance nodes periodically send HELLO messages to neighbor nodes. If a node fails to receive three consecutive HELLO messages from a neighbor, it concludes that link to that specific node is down. A node that detects a broken link sends a Route Error (RERR) message to any upstream node. When a node receives a RERR message it will indicate a new source discovery process. Fig 2. Shows AODV routing protocol with RERR message [14].

IV. ATTACKS ON MANETs

I will now categorize and describe possible attacks on MANETs. Most descriptions are intentionally abstract as I do not want to analyze specific protocols but list general attacks on all kinds of MANETs and protocols.

1) Passive Attacks
2) Active Attacks

A. 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 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, there by making it impossible for eavesdroppers to obtain any useful information from the data over heard [16,17]. There are some attacks which is particular to the passive attack brief details are given below:

1) Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile adhoc networks. It aims t oobtain some confidential information that should be kept secret during the communication[17]. The information may contain the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

2) Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to anticipate important information such as a source, destination and source-destination pair.

B. Acive 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 severe and difficult to detect when compared to external attacks [16]. There are some attacks which is particular to the passive attack brief details are given below:

1) Worm hole Attack

In a worm hole attack, an attacker receives packets at one point in the network,‖ tunnels‖ them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a worm hole[18]. For example, when a worm hole attack is used against a non-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the worm hole [17].

2) Black hole Attack

In black hole attack [19] [20], a malicious node uses its routing protocol in order to advertise it self for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [21].

3) Byzantine Attack

A compromised with set of intermediate, or intermediate nodes that working alone within network carry out attacks such as creating routing loops, forwarding packets through non-optimal paths or selectively dropping packets which results in disruption or degradation of routing services within the network [18].

4) Gray hole Attack

This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise it self as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability [18].

5) Jamming Attack

Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet,or by preventing the reception of legitimate packets [17].

Now we are focusing on detecting the Black hole Attack when routing the information from sender to receiver. So here we describe the entire details of Black hole Attack in below.

6) Sybil Attack

In this attack , a malicious attacker assumes multiple identities while a normal participant is allowed only one identity . This attack is facilitated when obtaining a new identity is inexpensive as is often the case in a Mobile Ad-hoc Network.

V. ROBUST SYBIL ATTACK DETECTION

This is another technique used to detect the sybil nodes. To implement this technique, some methods are required for the correct observation of traffic . These methods are discussed below [7,8,9]:

1. Robust Sybil attack uses the authentication mechanism for the traffic observation . In this, each packet is signed by the sender's private key and also signed by the nodes which are traversed by it to reach the destination and in the end receiver authenticate it by its public key. So, it gives the proof that at what time and location sender sends the packet and in which direction the packet is send by the sender, so that it will reach to the destination.
2. To check the similarity of the path, it uses the novel location based Sybil attack detection mechanism. The nodes whose path is exactly similar to each other are detected as Sybil nodes.

$$Sim(L_1, L_2) = \left(\frac{\sum_{i=1}^{k} T_{cmn_i}}{max(T_{obs_1}, T_{obs_2})} \right) * \left(\prod_{i=1}^{k} \frac{T_{ovl_i}}{T_{cmn_i}} \right)$$

Here, L1,L2 are

Tobc = Period that each node isobserved

Tcmn = Period in which there are observations of both nodes in the observation table (commonly observed)

Tovl = Period that both nodes are commonly observed and co-occurred in the same region ,

K = The number of times in which they are commonly observed.

The first part of equation is used to calculate that till what time both nodes are observed commonly and second part of equation is used to determine the overlap region of the nodes.

VI. PROPOSED ALGORITHM

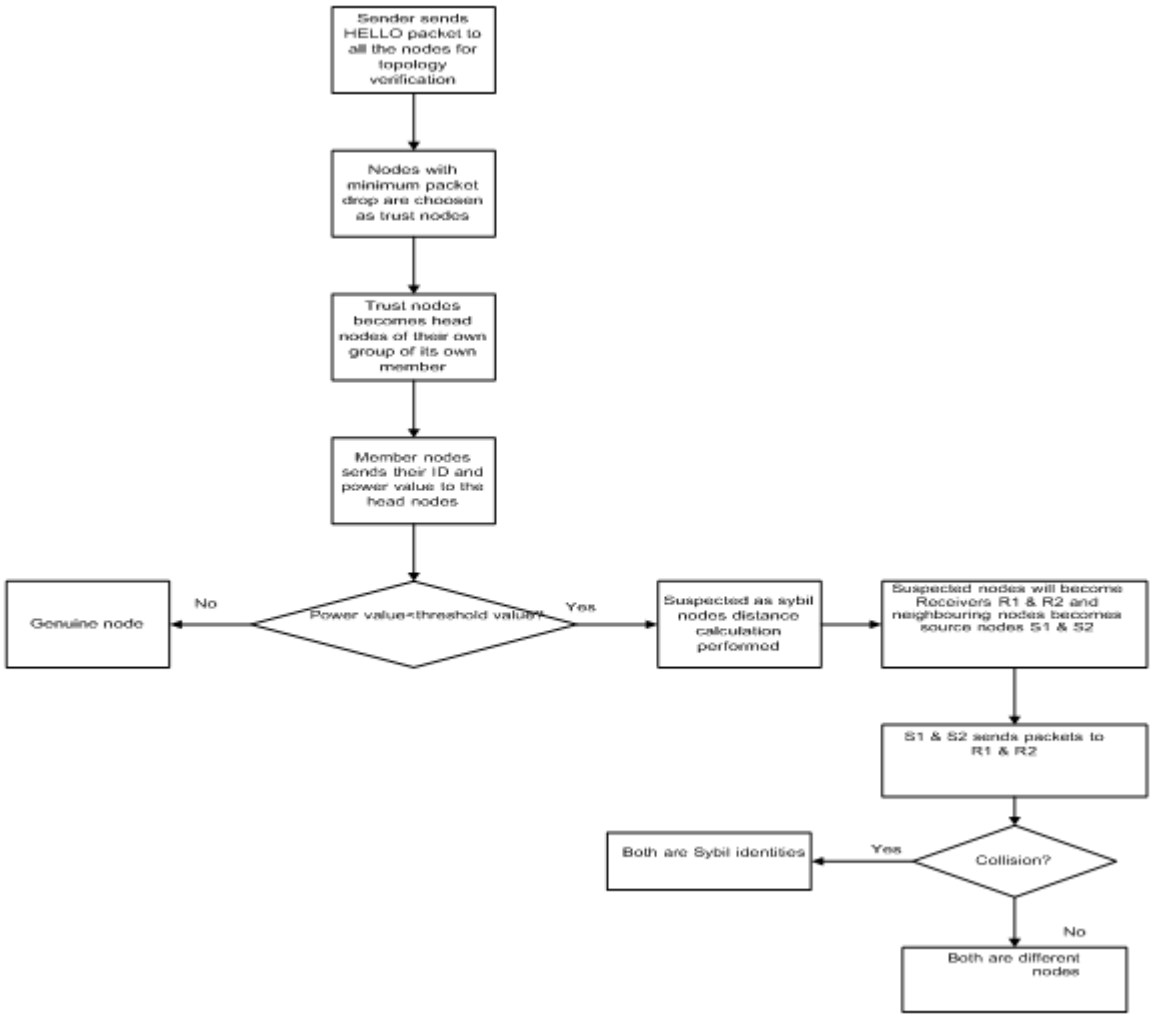

Fig .3 Flow Chart

Proposed Method

The sender sends HELLO packets to all the other nodes for topology verification. The nodes with minimum packet drop are chosen as the trust nodes. The trust nodes now become the head nodes with a group of its own member nodes. The member nodes send their ID and power value to the head nodes. The head node checks for nodes with power value below the threshold value. If the power value is lesser than the threshold value, those nodes are detected as Sybil nodes & distance calculation is performed according to following steps.

- These abnormal (Sybil) nodes are selected as receivers r1, r2.
- Two nodes closer to Sybil nodes are selected as senders s1, s2.
- Packets are sent to s1 and s2 to both receivers.
- sinceboth the identities are present at the same node ,there is collision of packets that leads to the packet drops.

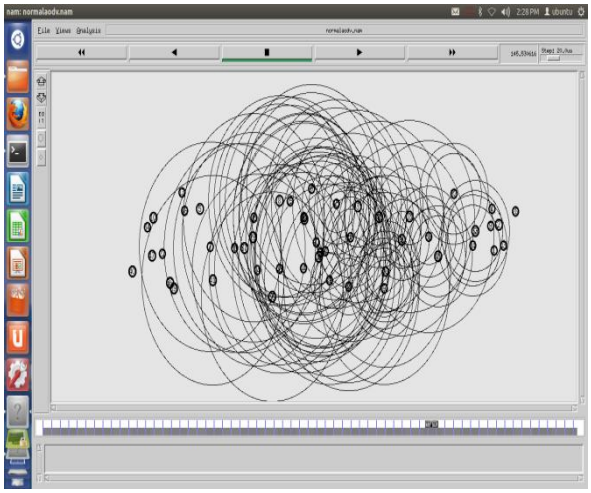

Fig.4 Original AODV Routing Protocol

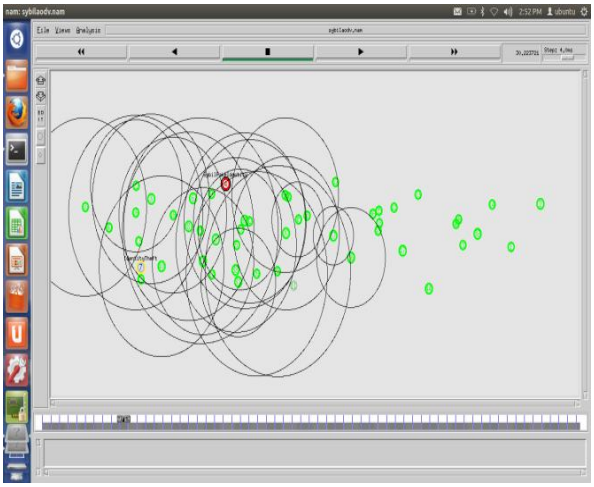

Fig.5 AODV Routing Protocol with Sybil Attack

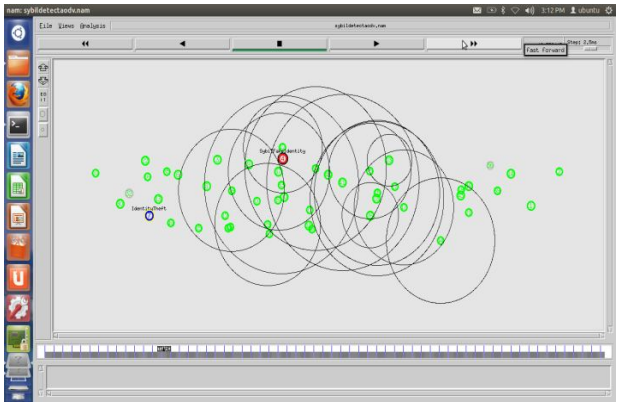

Fig.6 AODV Routing Protocol Sybil Attack Detected

VII. RESULT SUMMARY

	Without attack	With attack	Attack detected
No. of Sent TRF_MSG	556	556	556
No.of Received TRF_MSG	450	284	284
No.of Dropped TRF_MSG	102	96	87
No.of forwarded TRF_MSG	903	900	990
Delivery Rate (%)	80.94	51.08	50.35
Packet Delivery fraction (Received/Sent	0.8094	0.5108	0.5035
Avg. End to End delay(second)	147.613	147.701	149.139
Avg. Throughput (kbps)	20.21	10.22	11.90

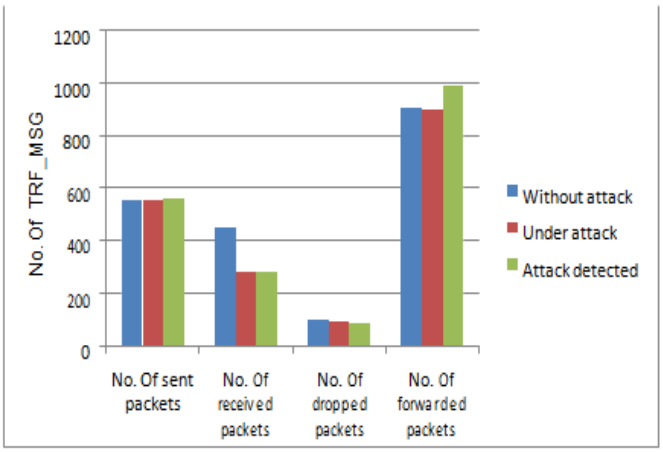

Fig.7 Data packets

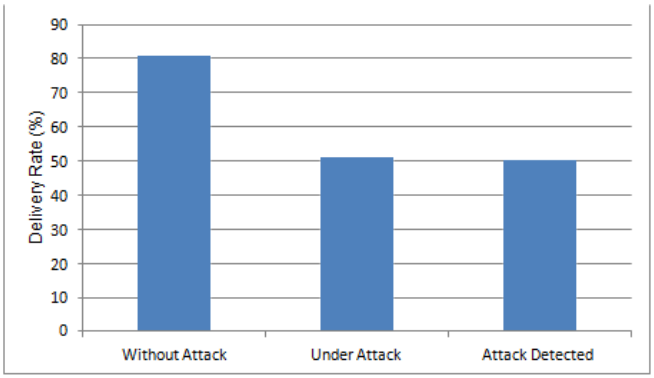

Fig.8 Delivery Rate

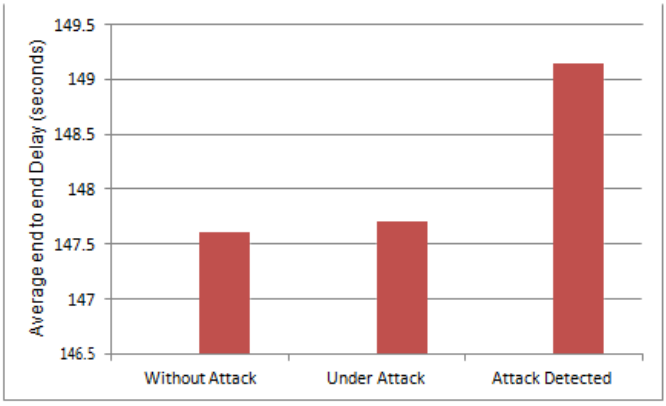

Fig 10.Average Throuput

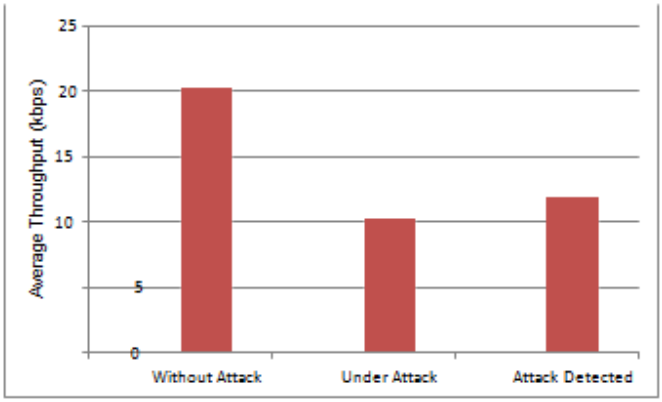

Fig 10.Average Throuput

IX. COMPARISON

COMPARISON OF SYBIL ATTACK DETECTION TECHNIQUES: LIGHTWEIGHT AND ROBUST

Algorithm	Parameters	Directional Antennae	Cost	Results*	Summary
Lightweight Sybil Attack Detection Technique	Speed, RSS	Not required	Cheap	90% true positive,10% false Negatie	The nodes entering in the network with RSS greater than the threshold value are
Robust Sybil Attack Detection Technique	Time, Location	Required	Costly	80% true positive,20% false Negatie	The nodes having exactly the same path or pattern are detected as Sybil nodes

X. CONCLUSION

There is rapid grow and change in the field of MANETs. While there are still many challenges that need to be met, it is likely that such networks will observe widespread and extensive use within the next few years. One of these challenges is security. Security of mobile ad hoc networks has recently gained momentum in the research community. Security solutions for MANET have to cope with a challenging environment including limited energy and computational resources.

With the above proposed work, the attacks which cause the damaged to the network are being easily detected.

XI. FUTURE WORK

In this method 50 mobile nodes are used. In which there is one malicious node. For future work we can change the below parameters and get the results for our proposed methodology and analyze it for security purpose. Like,

Change the MANET area.
Change the number of total participating nodes.
Change the number of malicious identities. Change the simulation time.

REFERENCES

[1] www.wickipedia.com

[2] John R. Douceur, The Sybil Attack, Microsoft Research

[3] Roopali Garg and Himika Sharma, Prevention Techniques for Sybil Attack, INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

[4] Anil Manohar Dogra, Rajvir singh, ZONE BASED ANALYSIS OF ZRP UNDER VARYING MOBILITY AND RANSMISSION RANGE IN MANETs, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 2 February, 2014 Page No. 4007-4016

[5] Ankush Tehale, Amit Sadafule, Swapnil Shirsat, Rahul Jadhav, Satish Umbarje, Sandip Shingade, Parental Control algorithm for Sybil detection in distributed P2P networks, International Journal of Scientific and Research Publications, Volume 2, Issue 5, May 2012

[6] Chris Piro Clay Shields Brian Neil Levine, Detecting the Sybil Attack in Mobile Ad hoc Networks

[7] Wenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering, Security Issues in Mobile Ad Hoc Networks- A Survey, University of Maryland, Baltimore County

[8] MANET: Vulnerabilities, Challenges, Attacks, Application [Priyanka Goyal, Research Scholar, Dept. of CSE, Technological Institute of Textile and Science, Bhiwani, Haryana, India Vinti Parmar, Dept. of CSE, Technological Institute of Textile and Science, Bhiwani, Haryana, India Rahul Rishi, Dept. of CSE, Technological Institute of Textile and Science, Bhiwani, Haryana, India

[9] Alice Cheng, Center for Applied Mathematics Cornell University, Ithaca, NY 14853 and School of Operations Research and Industrial Engineering, Cornell University, Ithaca, NY 14853 , Sybilproof Reputation Mechanisms.

[10] Chuang Lin, Yuanzhuo Wang, Yang Wang, Haiyi Zhu, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, P.R. China, Stochastic Game Nets and applications in Network Security

[11] Lesniewski-Lass, C. (Apr. 2008) "A Sybil-proof one-hop DHT," in Proc.ACM SocialNets, Glasgow, Scotland.

[12] Sieka, B. (2006) "Using Radio Device Fingerprinting for the Detection of Impersonation and Sybil Attacks in Wireless Networks," in Proceedings of ESAS.

[13] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, Carnegie Mellon University, The Sybil Attack in Sensor Networks: Analysis & Defenses

[14] RoopaliGarg and Himika Sharma "Comparison between Sybil Attack Detection Techniques: Lightweight and Robust", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014

[15] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester" An Overview of Mobile Ad Hoc Networks: Applications and Challenges"

[16] Himadri Nath Saha, Dr. Debika Bhattacharyya, Dr. P. K.Banerjee, "Semi- Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack", International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 338 Volume 1, Issue 4, December 2010

[17] S.Sharmila1, Research Scholar, Anna university, Tamil Nadu, India, G Umamaheswari, Assistant Professor, Department of ECE, PSG College of Technology, Tamil Nadu, India, Detection of Sybil Attack in Mobile Wireless Sensor Networks, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2, Issue-2, 256 – 262

[18] Murat Demirbas, Department of Computer Science and Engineering Department State University of New York at Buffalo, Youngwhan Song, Department of Computer

Science and Engineering Department State University of New York at Buffalo, An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks

[19] Aarti Department of Computer Science & Engineering , MRIU Faridabad, India. Dr. S. S. Tyagi, Department of computer science & Engineering, MRIU, Faridabad, India, "Study of MANET: Characteristics, Challenges, Application and Security Attacks" , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X

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

[21] Buttyan, L. and J. Hubaux (2003) "Report on a Working Session on Security in Wireless Ad Hoc Network," ACM Mobile Computing and Communications Review, 7(1), pp. 74 – 94.