ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Defending Sybil Attack in MANET by Modified Secure AODV

Dr.T.Pandikumar[1], Yibrah Legesse[2]
Associate Professor[1], M.Tech Student[2]
Department of Computer & IT
College of Engineering, Defence University, Debre Zeyit, Ethiopia

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. In order to provide better security against the issues, the existing static & dynamic routing protocols like AODV, DSR, OLSR needs to be updated. This research work proposes an efficient technique to detect & prevent Sybil attack without the need for special hardware. Deployment of Sybil attack, Implementation of Sybil Node detection & development of SAODV to prevent Sybil nodes are the techniques be used. The performance of proposed technique i.e., SAODV is evaluated by reviewing different papers and their respected techniques in which they have used to defend the Sybil attack. By comparing the advantages and disadvantages of the techniques and by using Neighbor node id based Sybil attack deployment, it is proposed the technique in which its performance will superior as packet delivery ratio and throughput increases. This research paper analyzed that the modified Secure AODV is suitable to detect & prevent Sybil attack.

Keywords: AODV, MANET, SAODV, Sybil attack

1. INTRODUCTION

1.1 Background of wireless 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).

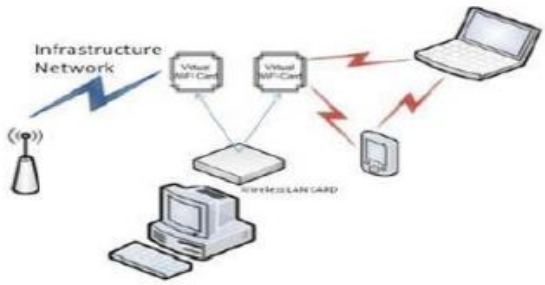


Figure .1. Infrastructure networks

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.

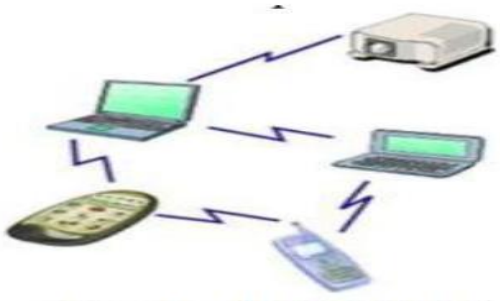


Figure.2. Mobile Ad Hoc Network (MANET)

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 Statement of the Problem

In Mobile Ad-hoc networks (MANETs), mobility of the nodes poses a problem for providing security services. The ad-hoc network is more vulnerable to attacks, since it uses wireless communication link between the mobile nodes. Therefore, security of mobile ad-hoc networks is one of the major issues; hence research is being done on many routing attacks on mobile ad-hoc networks [7]. The Sybil attack is particularly harmful attack in networks. In the Sybil attack, a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities. In the worst case, an attacker may generate an arbitrary number of additional node identities, using only one physical device. 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.

1.3 Objectives of the research paper

The objective of this work is to provide higher security against these attacks with minimum overhead and acceptable delay. And to propose efficient techniques to detect and prevent Sybil attack in Mobile Ad-hoc Network (MANET) by securing AODV protocol. It is also desirable to evaluate the performance of modified routing protocol on the basis of different performance metrics by reviewing different papers and their respected techniques in which they have used to defend the Sybil attack. Another objective is to propose a technique by comparing the advantages and disadvantages of the different author's techniques, by using Neighbor node id based Sybil attack deployment and by comparing the results of modified protocol and existing protocol under these attacks.

1.4 Significance of the research works

To have secure communication it is necessary to eliminate the Sybil nodes from the network [1]. The significance of the research work is to fulfill the following security goals:

- Authentication: It means that each and every node, participating in communication must be genuine and legitimate node.
- Availability: All services should be available all the time to all the nodes for the proper functioning and security of the network.
- Integrity: It gives the assurance that the data received by the receiver will be same as the data send by the sender.
- Confidentiality: It means that some data is only accessible by the authorized users.
- Non-repudiation: It means sender and receiver cannot deny that they didn't send or receive the data.

1.5 Literature Reviews

The literatures I referred for this seminar are as follows:

In the paper [1], author proposed neighbor discover distance algorithm used to detect the Sybil attacks. In MANET each and every nodes consists of a neighbor's data address. The neighbor's data address transfer to destination without any packet loss. Near duplication detection algorithm is more security and efficient data transmission on their network. Proposed NDD algorithm is verification and authentication method. NDD algorithm based to find detection and prevention Sybil attack and secure and avoid the attacking system on the network. This paper [1] is my benchmark paper during preparing my seminar. The benefits of this technique are to reduce packet delay, detect the attacker, and data delivery quickly from source to destination. The disadvantage is doesn't avoid the attacking system on the network.

In the paper [2], proposed a technique to detect and prevent Sybil attack that firstly sender node broadcast a request packet which in return wants a reply message which contain logical (IP) address and physical address (MAC).sender nodes maintain a table for that and checks if a node with same physical address reply with different logical address then the node with different logical identity is declared as a Sybil node and the sender node chooses another path for sending packets to destination. In the paper [3], the authors proposed an RSS-based detection mechanism to safeguard the network against Sybil attacks. The scheme worked on the MAC layer using the 802.11 protocol without the need for any extra hardware. The authors demonstrated through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities. Using this technique is it can detect both join - and - leave and simultaneous Sybil attackers with a high degree of accuracy. But in this technique the author didn't mention to solve tackling issues related to variable transmit powers. In the paper [4], *the* authors showed that a legitimate node in the network along with the Local Server (LS) can detect the Sybil attacker using Associatively Based Routing (ABR)**.** This paper mainly deals with the defense mechanism proposed using the Direct Validation technique [9], where a node directly validates another node with the help of a secure and unique PKI based SESSION KEY (SESS_KEY), generated by a central authority called the Local Server (LS) which confirms the identity of one node with the other nodes in the network. This technique is able to prevent the Sybil attack because authenticated messages are kept and others are ignored. But the disadvantages of using this technique are it is time consuming, very complex, and requires large memory. In the paper [5], the authors proposed an identity verification and resource based algorithmic approach for the detection and elimination of Sybil nodes. The Sybil node is detected with involvement of base server by verification the identity and resources node through the trustworthiness of secure Id of all node. The drawback of this technique is inefficient for most systems.

1I. ROUTING PROTOCOLS AND ATTACKS

2.1 Ad-hoc Routing Protocols

A number of routing protocols have been suggested for ad-hoc networks. These protocols can be classified into two main categories:

- Table driven routing protocols(Proactive routing protocols)
- Source initiated on demand routing protocols

2.1.1 Table Driven Routing Protocols

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. Figure 3 illustrates classification of ad-hoc routing protocols.

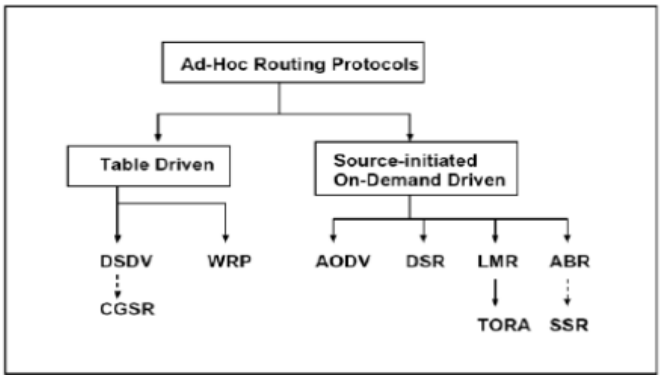


Figure. 3. Categorization of ad hoc routing protocols

2.1.2 Source Initiated On Demand Routing

A different approach from table-driven routing is source-initiated on demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired.

2.2 Overview of Ad Hoc On Demand Distance Vector Routing (AODV)

The Ad Hoc On Demand Distance Vector (AODV) routing protocol builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. AODV classify as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges.

2.3 Attacks in MANET

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

2.3.1 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.

2.3.2 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 severe and difficult to detect when compared to external attacks.

2.3.3. Sybil Attack

Sybil attack is a type of active attack in which malicious node carries fake identities of existing or non-existing legitimate node to control a part of network. A Sybil attack may apply due to poor authentication on network layer .it is an attack which creates repudiation of large fake identities a single physical node to gain disproportional large influence this attack aims to degrade network services or availability of resources when co-operation is required. The Sybil attack occurs in network when it runs without central authority. Sybil attack is an approach in which a malicious node illegitimately fakes multiple identities by compromised node or clamming same from external source. In figure 3.1[12], node M1 assumes identities of M2, M3, M4, and M5. So, to node B, M1 is equivalent to those nodes.

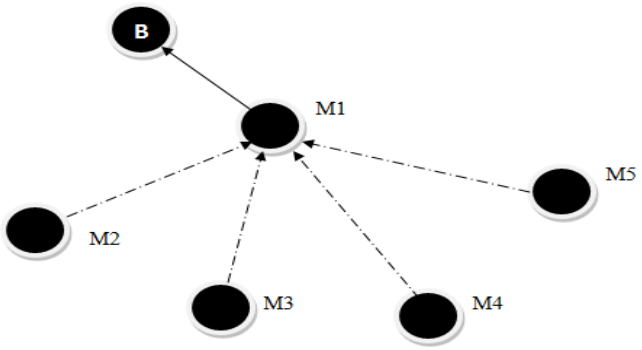


Figure 3.1: Sybil Attack

Sybil attack is also capable of disturbing routing mechanism in MANET multipath routing and secure routing may affected by this attack. In multipath routing fake identities may be the part of one or various routes in different position. To compromise communication and degrade network performance.

2.4 Types of Sybil attack

2.4.1 Direct and Indirect Communication

In direct attack, the legitimate nodes communicate directly with Sybil nodes whereas in indirect attack, the communication is done through malicious node.

2.4.2 Fabricated and Stolen Identities

It creates a new identity for itself based on the identities of the legitimate nodes, that is, if legitimate nodes have an ID with length 32-bit integer, it randomly creates ID of 32-bit integer. These nodes have fabricated identities. In stolen identities, attacker identifies legitimate identities and then uses it. The attack may go unidentified if the node whose identity has been stolen is destroyed. Identity replication is when the same identities are used many times in the same places.

2.4.3 Simultaneous and Non-Simultaneous Attack

In simultaneous, all the Sybil identities participate in the network at the same time. Since only one identity appears at a

time, practically cycling through identities will make it appear simultaneous.

III. DETECTION AND PREVENTION OF SYBIL ATTACK

3.1 Proposed Technique

This research work proposes an efficient technique to detect and prevent Sybil attack without the need for special hardware or strict location or synchronization requirements. The proposed technique makes use of variance in routing information between neighbors to detect Sybil attack. The detection technique uses an approach based on identity verification formally known as ID verification. The Sybil affected routes are distinguished from legitimate routes by analyzing ID value of all neighbors. Basic idea of the technique is to discover alternative routes to the destination. These alternative routes will be dissimilar in length. The idea behind this approach is illustrated below.

3.2 Deployment of Sybil Attack in MANET

The objective of this phase is to create malicious environment of Sybil node to observe the impact of Sybil attack in MANET. Here, a Sybil node is deploy at time of network deployment. Afterwards, it starts participating into network activity and attempt to collect IDs of neighbor nodes. Sybil attack may be deploying into two ways either through fresh identity or through existing identity. work uses the existing node identity to create multiple ID replicas. In this ways, Sybil node collect neighbor node IDs in routing table. When source broadcast RREQ packet to discover route from source to detonation, it uses fake IDs to misguide source about shortest route towards destination. Thus source register Sybil node into routing table and start communication through malicious node.

3.3. Implementation of Sybil Node Detection

This phase comprises the detection technique of malicious node using intrusion detection system. AODV protocol has been modified and monitoring methods are deploying to listen and validate fake node id. As per traditional process source will broadcast the RREQ packet to discover shortest route towards destination and register Sybil node into routing table. But in case of detection, it will rebroadcast packet to multiple routes and attempt to collect information of all neighbor nodes. Because Sybil node always uses multiple id for communication, it will have multiple id for same neighbor. Source will compare the id details with stored path and if it found different it consider it as malicious node. In simple words, detection system collect neighbor node information hop count and compare this result with existing routing table. if it found any entry in existing table missing from recently collected neighbor node information, it consider that node as malicious node and forward this detail to SAODV.

3.4 Development of SAODV to prevent Sybil nodes

This phase is to detect and prevent Sybil attacks in AODV routing protocol which has been done in the proposed technique based on identity verification approach. The basic idea behind the proposed technique is to integrate Intrusion detection scheme and SAODV algorithm to detect and prevent Sybil attack. Here, detection approach detect malicious node by cross examine identity verification and forward malicious node ID to SAODV. This process deletes malicious node entry from source routing table and blacklists the malicious node at source node. Next time, when source attempt to forward packet towards destination, it verify node information from blacklist and bypass the malicious route.

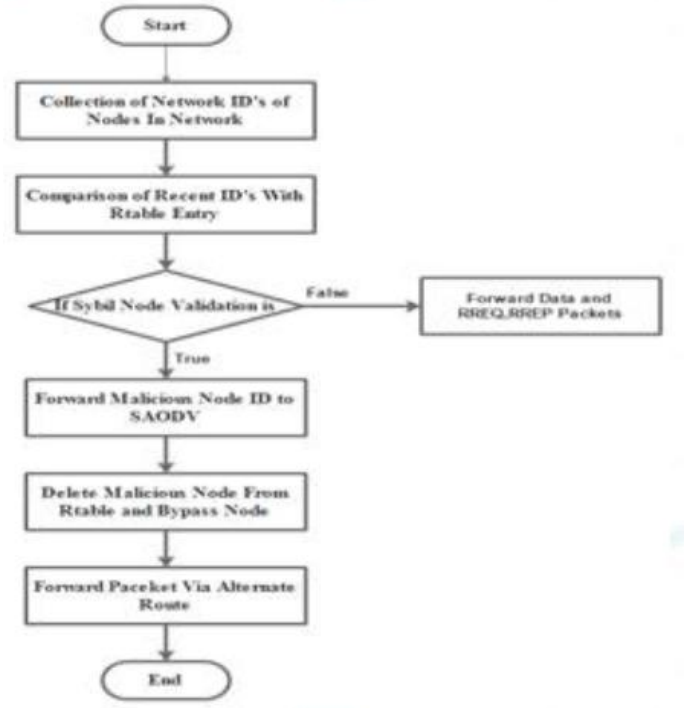


Figure 4. Flow Chart of Proposed Algorithm

3.5 Implementation Steps

The work starts with studying the theoretical and practical concept of the AODV routing protocol.

1. AODV routing protocol is then implemented in ns2 on different scenarios have 100 nodes, 300 nodes and 500 nodes in network.

2. Performance evaluation of AODV protocol under different scenarios is done on basis of Throughput, Packet Delivery Ratio and Packet Drop Ratio.

3. Theoretical aspects of security issues and their impacts on ado network are studied.

4. Simulation of network AODV routing protocol with Sybil Attack is done to analyze the impact of malicious node on performance metrics.

5. Analyze the impact Sybil Attack on various performance metrics for AODV.

6. Implement the proposed detection technique in AODV for detection of Sybil Attack.

7. Analyze the performance metrics for modified AODV using detection technique to detect Sybil attack.

8. Implement the proposed Secure-AODV technique in AODV for prevention of Sybil Attack

9. Analyze the performance metrics for modified SAODV using to prevent Sybil attack.

10. Compare the performance parameters for AODV under Sybil Attack, IDS AODV and SAODV for 100 nodes, 300 nodes and 500 nodes Scenario

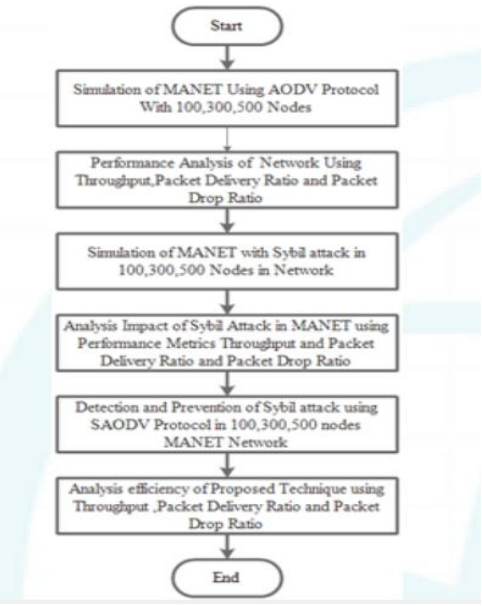


Figure. 5. Flow Chart of Implementation

IV. RESULT OBSERVATION

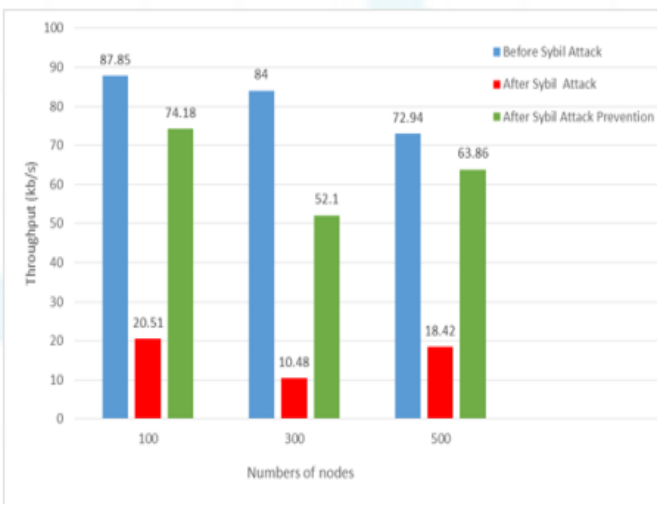
The simulation of the work completed in three scenarios. The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node. Initially all nodes in each scenario are normal and no malicious node is present in the scenario. The standard AODV routing algorithm is used at routing protocol on network layer. The scenarios are differentiated as per normal scenario, scenario with Sybil nodes and scenario with proposed technique. Impact of performance variation is observed in 100 nodes, 300 nodes and 500 nodes.

Scenario 1: It describes the normal situation of mobile ad-hoc networks with normal AODV routing protocols.

Scenario 2: It described impact of Sybil Attack and impact of Sybil attack on performance of ad-hoc networks.

Scenario 3: it implements the proposed technique to detect and prevent Sybil attack in mobile ad-hoc networks.

Figure 6. Demonstrates the evaluated performance of normal AODV, AODV with Sybil attack and modified AODV with improved performance. The network performance metric is throughput and packet delivery ratio.



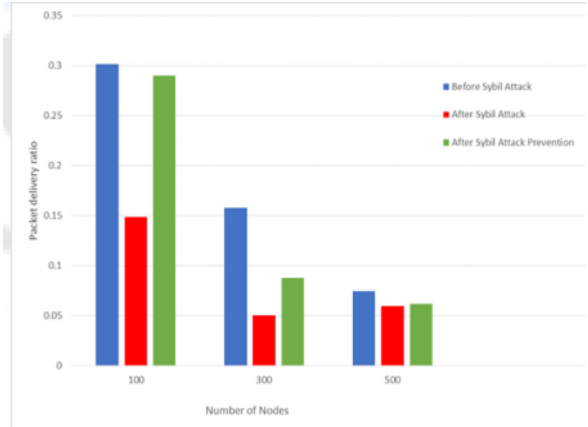


Figure.6. Comparison of Throughput in 100, 300, 500 Node Network with Different Scenario

Throughput = Total received packets / Total simulation time
…Equation (1)

Packet Delivery Ratio = (packets received/packets sent)
...Equation (2)

4.1 Result Description

Result show in graph describe that before Sybil attack throughput and packet delivery ratio is high and after Sybil attack, it decrease and after prevention values are restored with some difference due to routing path change and routing packet delivery .In 300, 500 nodes network throughput in 500 nodes network have high throughput after prevention of Sybil attack because of new routing path and low routing overhead.

V. CONCLUSION AND FUTURE WORK

5.1 Conclusion

This work proposed SAODV based technique to detect and prevent Sybil attack. To evaluate the performance of proposed techniques, Neighbor node id based Sybil attack deployment has been used. The performance of this approach improves nodes. This means scalable to large population of nodes. The work was started by studying theoretically concept of the AODV and the proposed technique, according to the proposed techniques shows broadcast is minimized, reduces memory requirements, and needless duplications as well as loop-free route are maintained by use of destination sequence number, and it is nose store only the routes that are needed. Therefore, it is found that the modified Secure AODV has superior performance than AODV. Modified Secure AODV is suitable to detect and prevent Sybil attack. It improves the PDR under attack conditions, with acceptable decrease in throughput due to routing path change and new route.

5.2. Future Research work

Further work needs to be done to understand the effect of Trust and reputation in MANET. Existing algorithms tends to detect attacks in MANET but more work required to enhance security in MANET, hence more intrusion detection algorithm should be proposed. Also In the future work, I propose to work on detecting the presence of the Sybil attacker in the other phases of routing protocols like DSR or DSDV.

VI. REFERENCES

[1]. R. Bhuvaneswari, N. Balamalathy, S. Premalatha "An Improved Performance, Discovery and Interruption of Sybil Attack in MANET", Middle-East Journal of Scientific Research ISSN: 1990-9233 Vol. 23 No. 7, Page No. 1346-1352, Year 2015

[2]. Anamika Pareek, Mayank Sharma, "Detection and Prevention of Sybil Attack in MANET using MAC Address" International Journal of Computer Applications (0975 – 8887) Volume 122 – No.21, July 2015.

[3]. N.V.V. SATYA NARAYANA, D. SRINIVAS, "Detecting Techniques to Mitigate Sybil Attack in MANETs" International Journal of Scientific Engineering

[4]. Sowmya P, V. Anitha, "Defence Mechanism for SYBIL Attacks in MANETS using ABR Protocol" International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue-15 June-2014.

[5]. Sangeeta Bhatti, Prof Meenakshi Sharma, "A Novel Algorithmic Approach for Detection of Sybil Attack in MANET" International Journal of Advanced Research in Computer Science and Software Engineering 5(5), May- 2015, pp. 1680-1685 and Technology Research, ISSN 2319-8885 Vol.03, Issue.49 December-2014, Pages:9937-9945.

[6]. Nidhi Joshi, Prof. Manoj Challa," Secure Authentication Protocol to Detect Sybil Attacks in MANETs", International Journal of Computer Science & Engineering Technology (IJCSET) Vol 5 No. 06 June 2014.

[7]. RoopaliGarg, HimikaSharma, "Lightweight Sybil Attack Detection Technique in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 5, May 2014.

[8]. Amol Vasudeva, Manu Sood, "Sybil Attack on Lowest Id Clustering Algorithm in the Mobile Ad Hoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.

[9]. N. KOHILA, R. GOWTHAMI, "Routing Protocols in Mobile Ad-Hoc Network", International Journal of Computer Science and Mobile Computing, ISSN 2320–088X IJCSMC, Vol. 4, Issue. 1, January 2015, pg.159 – 167

[10]. Ms. Amita Pandey, "Introduction to Mobile Ad Hoc Network", International Journal of Scientific and Research Publications, Volume 5, Issue 5, ISSN 2250-3153, May 2015

[11]. Roopali Garg, Himika Sharma, "Lightweight Sybil Attack Detection Technique in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 5, May 2014.

[12]. Amol Vasudeva, Manu Sood, "Sybil Attack on Lowest id Clustering Algorithm in the Mobile Ad Hoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.

[13]. J. Newsome, E. Shi, D. Song and A. Perrig. "The Sybil Attack in Sensor Network: Analysis & Defenses." IPSN‟04, April 26–27, 2004, Berkeley, California, USA