International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

Sybil Attack Detection in Mobile Ad-hoc Networks using AODV protocol

Dhanashri Saindane[1]

[1]PG Student, Dept. of EC Engineering, GTU-Graduate School of Engineering and Technology, Ahmedabad, Gujarat, India

---

Abstract - *Mobile ad hoc networks are a technology that enables fast, easy, and inexpensive network deployment, but unfortunately these benefits also make an attacker's job easier by making it easier to deploy a malicious node in the environment. Mobile ad Hoc networks are prone to various attacks because of the broadcast nature of the wireless medium and the lack of a central authority. In this proposed work, we created a real network scenario that offers a more accurate solution to the attack. We performed a topology analysis based on the routing protocol and found that the AODV protocol performed better than other routing protocols. Since wireless network security is a major concern, the Sybil attack affects the performance. In a Sybil attack, an adversary illegitimately claims to have multiple imaginary identities called Sybil nodes. This attack is capable of compromising various operations on these networks, such as data aggregation, coordination mechanisms based on , fair resource allocation schemes, detection of bad behavior and routing mechanisms. In our research, we implemented the attack in a real-time network scenario and compared the results with the normal AODV protocol, the AODV protocol with the Sybil attack and the AODV protocol after mitigation technique.*

Key Words: **Mobile Ad hoc network, AODV, Routing, Sybil Attack, Mitigation.**

1. INTRODUCTION

Wireless communication between mobile users has become more vital than ever. This leap is attributed to the most recent technological advances in notebook computers and wireless transmission instrumentality equivalent to wireless modems, wireless LAN's and lots of more. Currently there are technologies with cheaper price and better data rate than before which is why mobile computing continues to grow larger and sophisticated. There are presently two variations of mobile wireless networks infrastructure and infrastructure less network (Ad-hoc networks).The infrastructure networks, in addition said as Cellular network, have constant and wired gateways. They need constant base stations that are involving completely different base stations via wires. The transmission kind of a base station constitutes a cell.

All the mobile nodes lying at intervals the vary connects to and communicates with the closest base station.The other type of network, is infrastructure less network,is additionally referred to as Mobile Ad Network (MANET).These networks don't have any mounted base stations and are self-configuring networks of mobile hosts equipped with wireless devices. Because of the character of wireless and antenna transmission, the transmission from the mobile host is received by all hosts within its transmission range.

1.1 Mobile Ad hoc Network

Mobile Ad Hoc Network (MANET) is one of the most important key technologies in various fields of communication and research. MANET is composed of several types of mobile nodes, which can be dynamically organized according to needs without centralization. MANET can freely move and exchange data through multi-channel communication channels. The MANET topology is dynamic, as shown in Figure 1. Then, the different protocols are classified according to indicators such as packet loss rate, routing protocol overhead,end-to-end packet delay, network performance, and scalability.

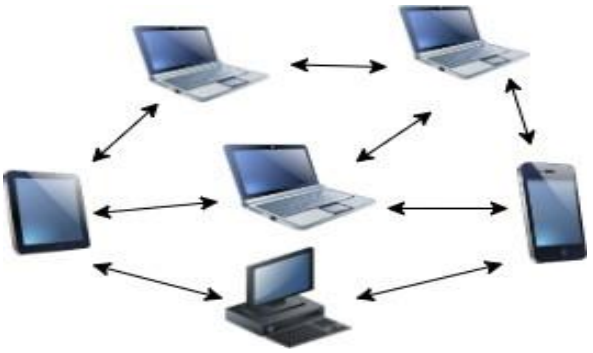

Fig 1 : Mobile Ad hoc network

1.2 Ad hoc On-Demand Distance Vector(AODV) Routing Protocol

AODV protocol discovers the routes primarily based totally on on-demand routing approach. Whenever, a source node needs a path for forwarding data packets,and then only a route is established. The packet consists of the sequence numbers of the destination node so as to identifythe most recent path. AODV differs from the other on-demand routing protocols, because the data packets in AODV use the destination sequence numbers in order to identify an up-to- date path for reaching the destination.

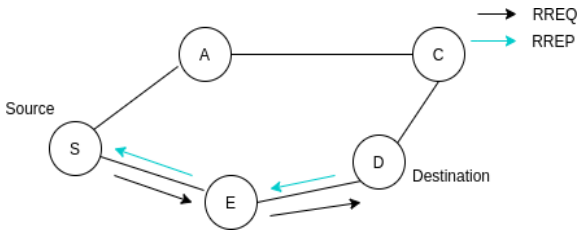

Fig 2 : AODV routing mechanism

2. RELATED WORK

[2]Authors conclude that MANETs play a very important role through a vital range of applications. But it becomes very risky without involvement of security policy. The complete phenomena observe that Sybil attack may give a big impact to degrade network performance and compromise information. [1]Sybil attack is a type of attack in which a malicious host transmits false information about existing or non-existing legitimate hosts to control parts of the network. Due to poor authentication at the network layer, Sybil attacks can be used. This is an attack that rejects large false IDs on a single physical node to produce a disproportionate impact. This type of attack is designed to disrupt network services or resource availability when collaboration is required. Sybil attacks occurred on the Internet without central authorization. [3]The successful launch of the Sybil attack also provides opportunities for various other attacks, such as sleep deprivation torture, black hole attacks, fast attacks, thin attacks, Byzantine attacks, and gray hole attacks.

3. PROBLEM STATEMENT

Sybil attack is carried out when a malicious node declares a couple of fabricated or stolen identification in the network. The node constitutes a couple of false identification and impacts the network operation, overall performance and fault tolerance of the network. Malicious nodes use IP spoofing approach to put into effect Sybil attack. Sybil attack is effective in both distributed and Peer to peer network, it effective on redundancy mechanisms of distributed data storage systems and effective against routing algorithms, data aggregation, voting, fair resource allocation and misbehavior detection, reputation system, torrent network, content delivery network. The attack introduce form inside or outside of network outside attack can be prevented by authentication but inside attack is not. It is important to detect Sybil attack. Sybil attacks are dangerous for security and trust of networks in peer to peer and distributed networks.

4. SYBIL ATTACK

Sybil Attack is an attack where the attacker pretends to be so many people at the same time. This is one of the most important issues when connecting to a P2P network. Manage the network and manage the entire network through the growth of husband and wife. From forged ID cards. At first glance, these unique identifiers seem to be ordinary users, but in the background, an object is called an unknown attacker, and he controls all these fake objects at the same time. The Sybil attack arises in a network when it runs without central authority. Sybil attack is likewise able to disturbing routing mechanism in MANET multi path routing and stable routing may also suffering from this attack.In multi path routing fake identities can be the a part of one or numerous routes in one of a kind position.To compromise communication and degrade network performance.

Types of Sybil Attack

Influence of Sybil Attack can be direct or indirect.

Direct Sybil attack : In this the honest nodes are affected directly by the Sybil node.

Indirect Sybil attack : In this the legitimate nodes are attacked by a node that communicates specifically with the Sybil nodes.This center node is compromised as it is under the malicious impact of Sybil nodes. Below Fig.2 node, M1 assumes compromised nodes identified as M2, M3, M4, and M5. Node A is a Normal node, M1 is equivalent tothose nodes.

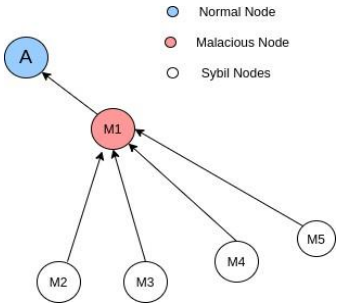

Fig 3 : Sybil attack

5. PROPOSED SOLUTION

Below fig 4 shows the flow of the proposed solution.

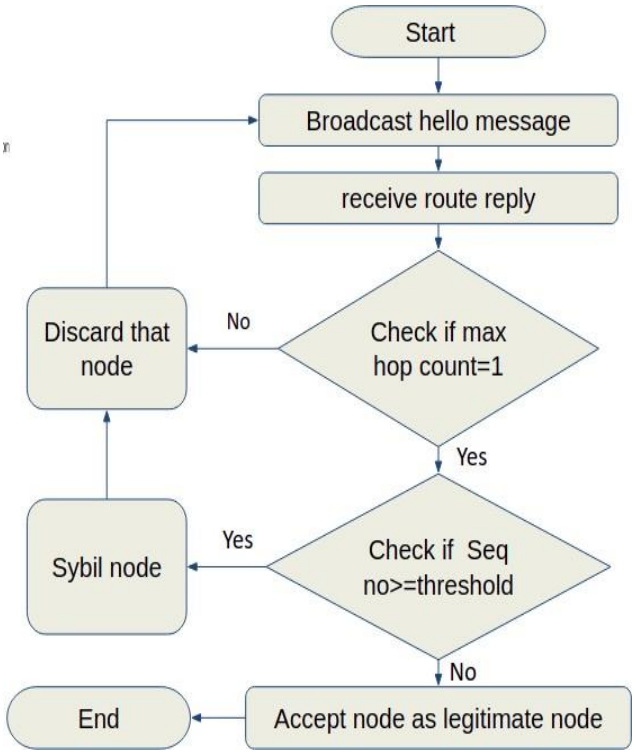

Fig 4 : Flow chart

Initially when a source node sends a RREQ in the network, the Sybil node (attacker node) reverts a fake RREP in response to the RREQ with highest sequence number. If only one RREP is received then there is no attack and the network is ok. If more than one RREP is received then it will compare those RREP and will select the packet having the highest sequence number and more current time. Then it will black list the fake RREP and will add it to the routing table list. Then it will remove the node from the network and all the nodes will update the blacklist. This process will be followed every time when the route discovery process is taking place in the network.

6. SIMULATION DETAILS

The simulation tool used for implementation is NS 2.35.The configuration of scenarios is based on the number of nodes deployed and the position of the source and destination nodes. 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 the network layer. Impact of performance variation is observed in 10,20,40,60,80 and 100 nodes.This work is differentiated in three scenarios asfollows:

Scenario 1: In this scenario the normal situation of AODV protocol in mobile ad hoc networks is observed.
Scenario 2: In this scenario the performance of AODV protocol is observed when Sybil Attack introduces in the mobile ad hoc networks
Scenario 3: In this scenario the performance of the AODV protocol after mitigation of Sybil attack is observed.Simulation parameters used for this implementation process are mentioned in the below Table1

Table 1 : Simulation Parameters

Simulation Parameter	Value
Simulator	NS-2.35
Routing Protocol	AODV
Network Area	800 x 800
Network Model	Random Mobility
No. of Nodes for Simulation	10,20,40,60,80,100
Traffic Agent	UDP
Traffic Application	CBR
No. of connections	Multiple
Speed	10 m/s
Simulation time	600 sec

7. RESULTS

As the proposed approach is meant to ensure mitigation of the Sybil attack, the performance analysis is done by calculating the Throughput,Packet Delivery Ratio,Packet Dropping Ratio and Delay of the network with normal AODV and AODV with Sybil attack implemented and AODVafter mitigation technique.

A. Throughput

It is the ratio of total number of packets sent by the source to the total number of packets received by the destination node.Figure 4 shows throughput results:

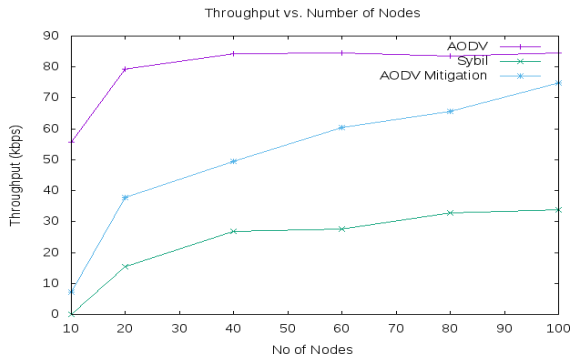

Fig 5 : Throughput

B. Packet Delivery Ratio

It is calculated by the number of bytes received by the destination node. Figure 5 shows Packet Delivery Ratio results:

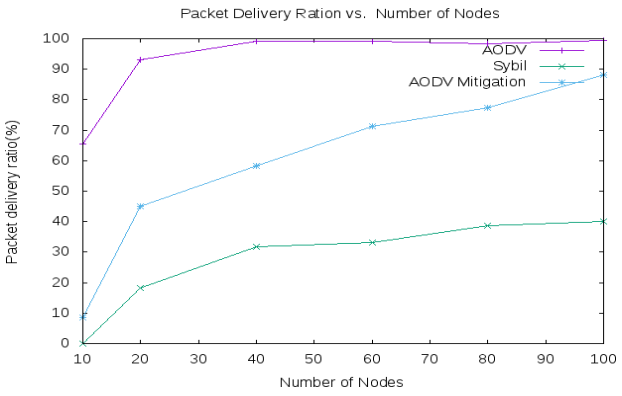

Fig 6 : Packet delivery ratio

C. Packet Dropping Ratio

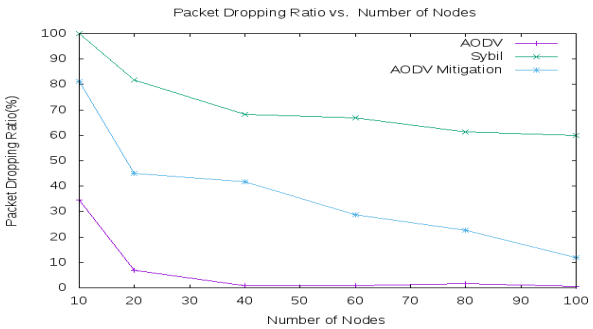

Fig 7 : Packet dropping ratio

It is the ratio of total number of lost packets to the total number of sent packets by source node.Figure 6 shows Packet Delivery Ratio results:

D. Delay

It is calculated by the time required to reach the packet from source to destination node.Figure 5 shows Packet Delivery Ratio results:

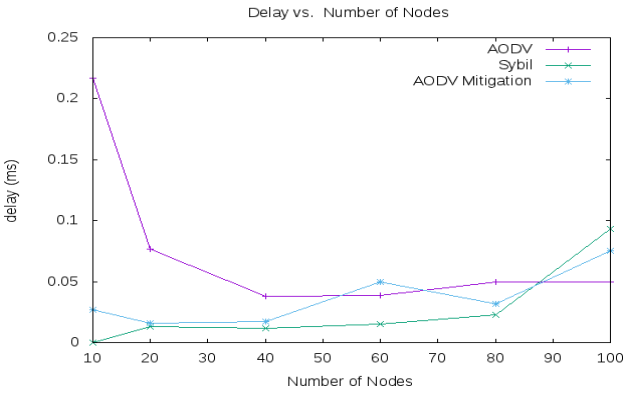

Fig 8 : Delay

7. CONCLUSION

In our research we have successfully mitigated Sybil attack for random mobility scenario and observed the results. The conclusion made from results shows that when Sybil attack introduces in the network its performance becomes degrading but after applying mitigation technique the performance of the network shows improvement in the results to some extent. Further work can be done for more improvement in delay parameter.

REFERENCES

[1] Pandikumar, T. and Yibrah Legesse. ”Defending Sybil Attack in MANET by Modified Secure AODV.” International Journal of Engineering Science 12725 (2017).

[2] Gupta, Ankit, Deepak Sukheja, and Amrita Tiwari. ”Impact of Sybil Attack and Security Threat in Mobile Adhoc Network.” International Journal of Computer Applications 124.9 (2015).

[3] Vasudeva, Amol, and Manu Sood. ”Survey on sybil attack defense mechanisms in wireless ad hoc networks.” Journal of Network and Computer Applications 120 (2018): 78-118.

[4] Aluvala, Srinivas, K. Raja Sekhar, and Deepika Vodnala. "An empirical study of routing attacks in mobile ad-hoc networks." Procedia Computer Science 92 (2016): 554-561.

[5] Mohd Amir Siddiqui, Roshan Jahan, Ijtaba Saleem Khan. "Design and Implementation of Routing Protocol for Detection of Sybil Attack in MANET." International Journal of Advance Research in Science and Engineering 2015.

[6] Vaijayanthi, K., et al. "DETECTING AND RESOLVING THE SYBIL ATTACK IN MANET USING RSS ALGORITHM." (2014): 233-24.

[7] Dhamodharan, Udaya Suriya Raj Kumar, and Rajamani Vayanaperumal."Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing methods." The Scientific World Journal 2015 (2015).

[8] Pareek, Anamika, and Mayank Sharma. "Detection and prevention of sybil attack in MANET using MAC address." International Journal of Computer Applications 122.21 (2015): 20-23.

[9] Dorri, Ali, Seyed Reza Kamel, and Esmaeil Kheirkhah. "Security challenges in mobile ad hoc networks: A survey." arXiv preprintarXiv:1503.03233 (2015).

[10] Rao, G. Shankara, et al. "Performance Analysis of MANET Routing Protocols-DSDV, DSR, AODV, AOMDV Using Ns-2." Global Journal of Computer Science and Technology (2015).

BIOGRAPHY

Dhanashri Saindane
Student of GTU-Graduate School Engineering and Technology, Ahmedanad, Gujarat.
Department of Master of Engineering in Electronics and Communication(Mobile Communicationand Network Technology)