Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.5, 2015


# Detection of Sybil Attack for P2P Security in Manets

M.Reshma
M.Tech Scholar, Department of CSE, GITAM University, Hyderabad

V.Sowmya Devi
Assistant Professor, Dept. of CSE, GITAM University,Hyderabad

**Abstract**:
A MANET is an infrastructure-less type networks, which consists of the number of mobile nodes with wireless network interfaces Sybil attack is a serious threat for today's wireless adhoc networks. In this attack a single node pretends several other nodes using various malicious means. Here we considered Topology based routing protocols like DSDV and DSR for the detection of SYBIL attacks in P2P system. Performance metrics such as packet delivery fraction, throughput, and end-to-end delay are evaluated using NS-2.
**Keywords** – Mobile Ad-hoc networks, Sybil attack, NS 2.

## 1. INTRODUCTION

In today's fast and rapidly growing world of technologies, more and more businesses understand the advantages of usage of computer networking. MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires.Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. A mobile ad-hoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Ad-hoc Network usually seek the help of other intermediate nodes to establish communication channels. A Mobile Ad-hoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range[1].

Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute the routing table).A computer network is a system for communication between computers[2].

A vulnerability is a weakness in security system [6]. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

A. **Lack of centralized management**: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network.
B. **Resource availability**: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.
C. **Scalibility**: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.
D. **Cooperativeness:** Routing algorithm for MANETs usually assume that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications

Vulnerabilities of ad-hoc networks from a security point of view, there are several reasons why wireless ad-hoc networks are more vulnerable than their wired counterparts. Sybil attack is a serious threat for today's wireless adhoc networks [5].

## 2. THE SYBIL ATTACK

Malicious nodes in a network may not only impersonate one node, they could assume the identity of several nodes by doing so undermining the redundancy of many routing protocols. This attack is called the Sybil attack. Sybil attack manifests itself by faking multiple identities by pretending to be consisting of multiple nodes in the network. So one single node can assume the role of multiple nodes and can monitor or hamper multiple nodes at a time[3]. A consequence of this is that attackers have a harder time to destroy the integrity of information. If the same packet is sent over several distinct paths a change in the packets incoming from one of these paths can be detected easily. Thus, isolating a possible intruder in the network becomes possible.

However, if a single malicious node is able to represent several other nodes, the effectiveness of these

 

measures is significantly degraded. The attacker may get access to all pieces of the fragmented information or may alter all packets in the same transmission, so that the destination node cannot detect tampering anymore. The Sybil attack is especially aimed at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information [2]. To disturb network topology, adversary often changes the locations with different legitimate node ids. To disturb multi-path routing, the attacker appears with multiple identities in the network, which are taken from the compromised node and appearing in most of the node disjoint paths.

A Sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node. Various effects due to the presence of Sybil attacks are:

- In the presence of Sybil nodes in the network, it may make difficult to identify a misbehaving node.
- Sybil attacks, prevent fair resource allocation among the nodes in the network.
- In certain application, sensors can be used to perform voting for decision making. Due to presence of duplicate identities the outcome of voting process may vary.
- Sybil nodes affect the normal operation of routing protocols by appearing itself at various locations in network [4].

## 3. ALGORITHM

addNewRss (*Address*, *rss*, *time−recv*)
**BEGIN**
STEP1. Check whether the Address is present in the Table
STEP2: If an address is not present then go to step3
STEP3: IF rss value is greater than, equal to the THRESHOLD value going to step4
STEP4:Add the address to the malicious node list
STEP5:Update the broadcast detection (Address)
STEP6:ELSE go to step7
STEP7: Add it to the neighbor Table (Address)
STEP8: End IF loop
STEP9: Create New Record
STEP10:Create Push back algorithm with parameters RSS value and time received
STEP 11: IF list−Size is greater than LIST−SIZE Goto step12
STEP 12: THEN Delete the front value ()
**END**

**Algorithm 2**
STEP 1:IF RSS value is the timeout
STEP2:THEN: go to step3
STEP3: rssTableCheck( )
**BEGIN**
STEP4: FOR loop
STEP5: for each Address in the Table
STEP6:DO Delete the element () go to step7
STEP7:IF Current−Time-- getTime greater than TIME−THRESHOLD go to step 8
//Indicate that we have not heard from this Address since the TIME−THRESHOLD
STEP8: IF getRss() > UB−THRESHOLD go to step9
STEP9: Add node to Malicious−List (Address)
//Indicates previous ID of a Whitewasher
STEP10:ELSE Print A message Normal out of Range”
STEP11: END FOR loop

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.

 

## 4. EXPERIMENT SCREEN SHOTS AND RESULTS:

### 4.1 Command prompt starts ns2 execution

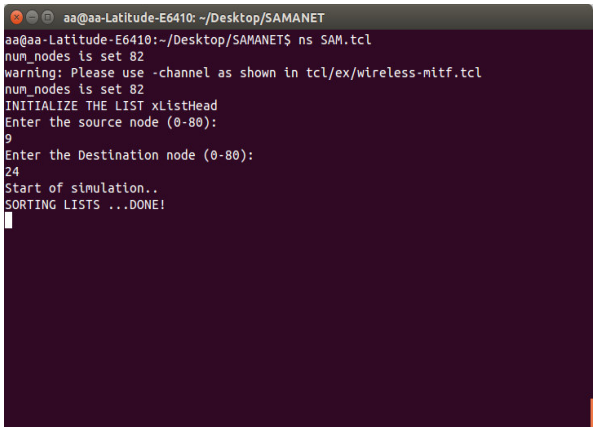


Figure:4.1 inputs for source and destination nodes

### 4.2 Discovering topology

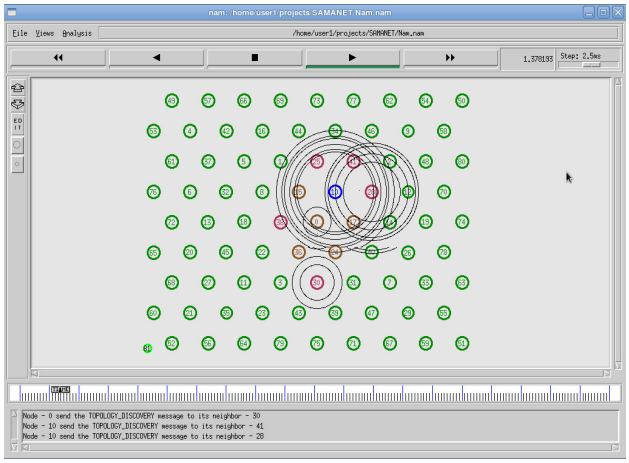

Figure: 4.2 Topology discovery

### 4.3 Discovery of the source and destination nodes and the intruder has been detected as IDS node

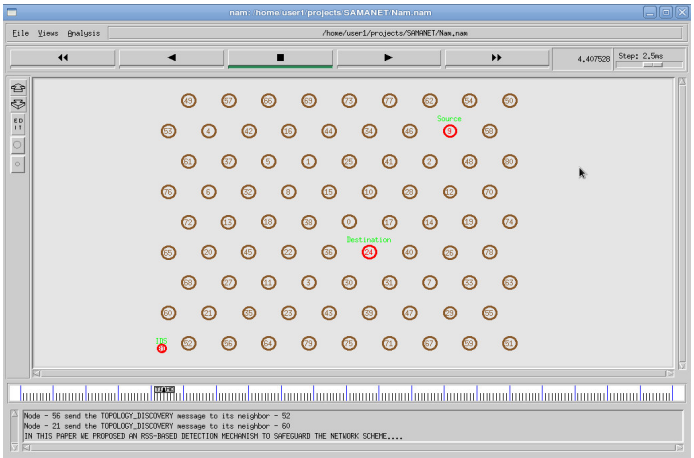


Figure:4.3 Discovery of source and destination nodes

 

### 4.4 Packet loss due to the Sybil attacker on the network

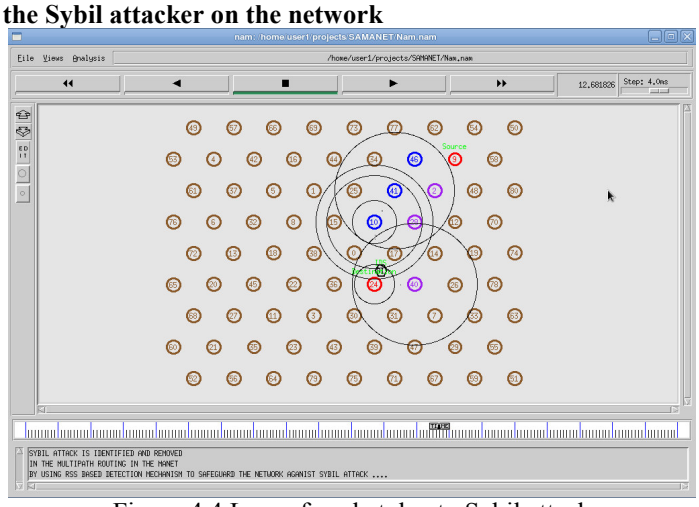


Figure:4.4 Loss of packet due to Sybil attack

### 4.5 Delivery of packets in the trusted path without the Sybil attack

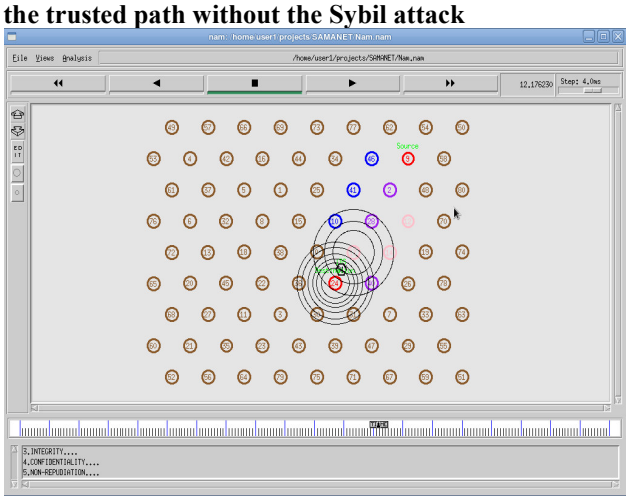


Figure: 4.5 packet delivery after removal of Sybil

The above output screens claims the discovery of topology Figure 4.2 to build a neighbor list using its RSS value and finds the source and destination nodes Figure 4.3. Later the intruder i.e; Sybil attacker was detected which results in packet drop Figure 4.4. After removal the Sybil attacker Figure 4.5 the packet transfers to the destination without any loss in optimal path.

## 5. EXPERIMENTAL RESULTS AND DISCUSSION

**Throughput:** It is one of the dimensional parameters of the network, which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation In this graph Figure 5.1 after the detection of Sybil attack the throughput get increased than before Throughput =N/1000

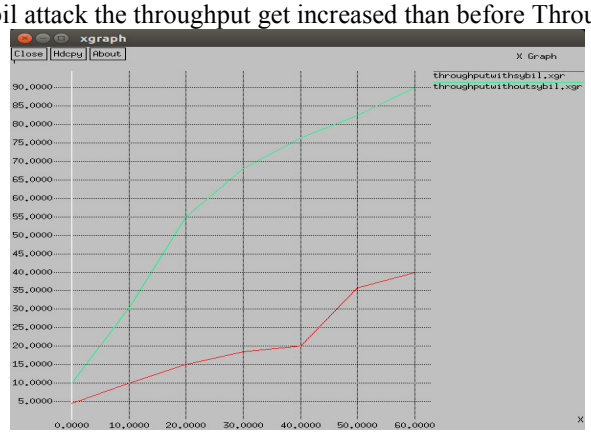


Figure: 5.1 Throughput with and without Sybil attack

 

**Packet delivery ratio:** It is defined as the ratio of data packets received by the destinations to those generated from the sources. The Graphs show the fraction of data packets that are successfully delivered during simulation time versus the number of nodes. In the below graph Figure 5.2 delivery ratio has increased when the packets delivered without Sybil attack when compared to packet delivery with Sybil attacks.

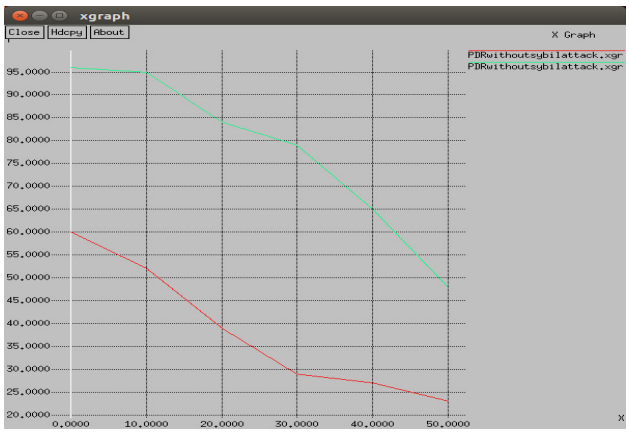


Figure: 5.2 Packet Delivery Fraction with and without Sybil attack

**Packet loss** is the discarding of packets in a network when a router or other network device is overloaded and cannot accept additional packets at a given moment. In the below analysis Figure 5.3 the packet drop becomes high when a Sybil attack is detected. Later after removal of Sybil attack, we found that packet drop has decreased.

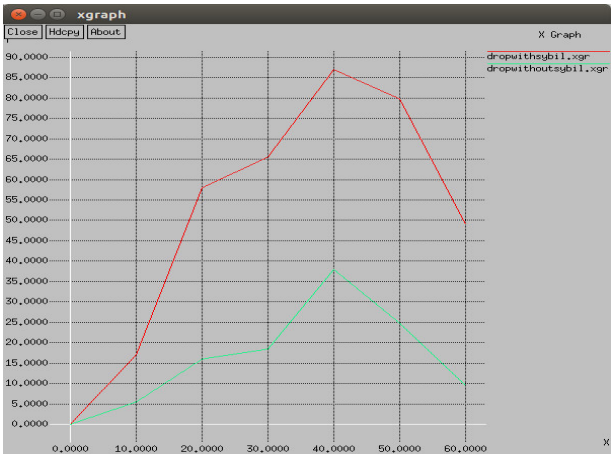


Figure: 5.3 Packet drop with and without Sybil attack

## 6. CONCLUSION

The research on MANET security is still in its early stage. In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved.In this paper, a survey on detection and prevention techniques Sybil attack in MANET ispresented.Mainly this involves detection of SYBIL attack where a malicious node do not forward the data packets to the destination and causes serious threat for Wireless MANETS. This paper focused on the discovery of topology in MANETS using routing protocols DSDV and DSR with NS2 simulator using RSS detection algorithm.In addition to this various factors affecting the detection accuracy, a loss of packet rate is also shown. This includes mainly improving throughput and packet delivery ratio with security in the network in addition with detection of Sybil attacks. Also packet delivery fraction has tackled with and without Sybil attacks in the network.

## 7. FUTURE WORK:

The future work can include more efficiency and security without Sybil attack in the network which gives better packet delivery rate and other tackling issues related to variable transmit powers and masquerading attacks in the network.

## REFERENCES:

[1] Pankaj Rohal1, Ruchika Dahiya2, Prashant Dahiya3 “Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV)” , Vol. 1, Issue II,

 

Mar. 2013
[2] Priyanka Goyal,Sahil Batra , Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.
[3] Aniruddha Bhattacharyya Arnab Banerjee Dipayan Bose "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques".
[4] Gagandeep, Aashima, Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012 269.
[5] Himadri Nath Saha # 1 , Dr. Debika Bhattacharyya # 2 , Dr. P. K.Banerjee *3"Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack",Volume 1, Issue 4, December 2010
[6] Manjeet Singh1 Gaganpreet Kaur 2 "A Surveys of Attacks in MANET", Volume 3, Issue 6, June 2013
[7] J. Newsome, E. Shi, D. Song, and A. Perrig. " The Sybil attack in sensor networks: analysis &defences, In Proceedings of the third international symposium on Information processing in sensor networks", pages 259–268, 2004
[8] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.
[9] Nor Surayati Mohamad Usop, Azizol Abdullah, Ahmad Faisal Amri Abidin. "Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environ
ment".

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

## CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

**Prospective authors of journals can find the submission instruction on the following page:** http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

## MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

## IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar