WWJMRD 2018; 4(1): 392-395
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
E-ISSN: 2454-6615

Navdeep Lata
Assistant Professor
Department of Information and Technology
MIMIT,Malout, Punjab, India

Rajan Goyal
Assistant Professor
YCOE,Talwandi Sabo,India

Correspondence:
Navdeep Lata
Assistant Professor
Department of Information and Technology
MIMIT,Malout, Punjab, India

Review Paper on 'To Detect Sybil Attack in MANET'

Navdeep Lata, Rajan Goyal

Abstract
MANET is infrastructure less and independent network which consists various nodes.These nodes uses wireless links to communicate with each other.The infrastructure less nature of MANET makes vulnerable to various attacks. Sybil attack is one of the attacks which cause many serious effects to the network. In Sybil attack, attackers or malicious nodes uses many identities or IP addresses to gain control over the network. It creates lots of misconception among nodes present in the network. In this paper the aim is to present practical evaluation of efficient method for detecting Lightweight Sybil attack. This kind of attack results the major information loss and hence misinterpretation in the network. There are many methods previously presented by different researchers with aim to mitigate Sybil attack with having their own advantages and disadvantages. The technique which i am using is not required any additional resources such as third party and any other hardware. The method which i am using is based on RSS (Received Signal Strength) to detect Sybil attack. This method uses RSS in order to distinguish the legitimate identity and Sybil identity. The practical analysis of this work is done by using Network Simulator (NS2). I will use CBDS approach to detect Sybil attack and comparing the results with the RSS method.

Keywords: Mobile Adhoc Network, RSS: Received Signal Strength, Sybil Attack, Threshold, UB: upper bound.

I. Introduction

MANET is infrastructure less and self configurable network where various users can communicate on temporary basis. It is collection of nodes that communicate with each other by the wireless links. Each node will work as source, destination and intermediate node ie work as switch**.**

A. **Architecture of MANET:** There is no such appropriate architecture of MANET due to its wireless nature [1].

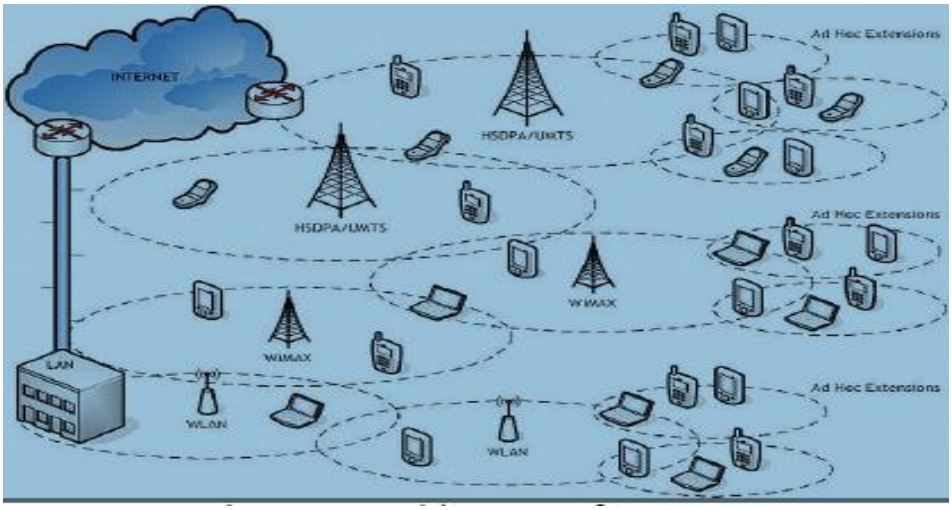

Fig.1: Architecture of MANET [1]

B. **MANET Vulnerabilities**

Vulnerabilities mean weakness in the security system. MANET is more vulnerable than the wired networks. The system may be vulnerable to unauthorized data manipulation because it allows the data access without knowing the user‟s identity. Some major vulnerabilities are [1]

1. No predefined boundary
2. Lack of Centralized Management
3. Resource availability
4. Scalability
5. Limited power supply
6. Dynamic topology

Attacks in Manet: Security in MANET is a major issue. For the better and secure network we must know the possible forms of attacks. So, that we will able to secure our network from that particular attacks. Various attacks on MANET are given below [1]:

Denial of Service attack (DOS): This attack aims to attack the availability of a node or the entire network
If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

Black hole Attack: In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

Wormhole Attack: In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole.

Replay Attack: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

Man- in- the- middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

Snooping: Snooping is unauthorized access to another person's data. It is similar to eavesdrop but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.

Sybil Attack: Sybil is named after the woman identified as multiple personality disorder. Sybil attack is implemented when a malicious node claim multiple fabricated or stolen identity and effect the network operations.sybil attack is harmful for security and trust of network in peer toper and distributed network. Sybil node gain disproportional amount of resource in network using multiple identity.

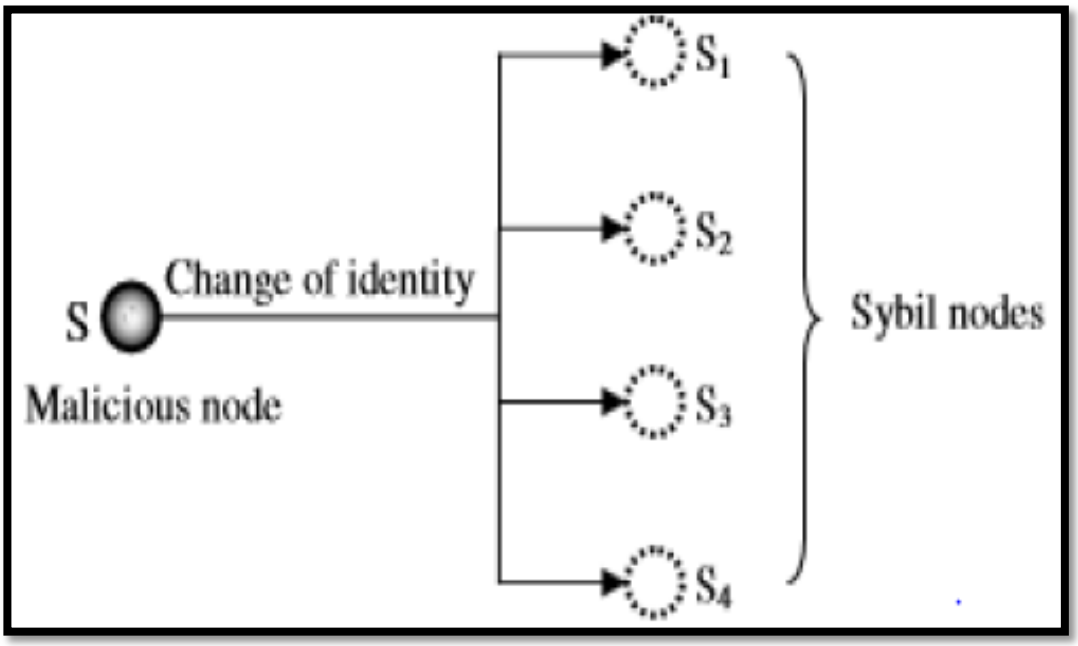

Fig.2: Sybil attack with multiple identities [1]

Types of Sybil Attack: There are different types of Sybil attack as mentioned below [2]:

1. **Direct and Indirect Communication**
2. **Stolen and Fabricated Identities**
3. **Simultaneous and Non Simultaneous Attack**

Bait: The source node stochastically select an adjacent node with which to cooperate, in the sence that the address of this node is used as bait destination address to bait malicious node to send a reply RREP message. Malicious nodes are there by detected and prevented from participating in the routing operations using reverse tracing technique. **CBDS (Cooperative Bait Detection Scheme):** CBDS is a technique to detect the malicious nodes in MANET for the gray hole and black hole.it merge the Advantages of both Proactive and Reactive schemes to detect the malicious nodes in network. Proactive detection scheme maintain the fresh list of destination and their routing table by periodically changing the table and Reactive scheme start only when route on demand in which there is no need of updating the routing table.CBDS is used only to detect the malicious node Neither prevent the node.Sometimes if the packet delivery ratio of the node below the threshold value then it consider the normal node as malicious node. It achieves its goals with reverse tracking.

II. Literature Survey

1. In [3] Sybil attack, network attackers disturbs the accuracy count by increasing its trust and decreasing others or takes off the identity of few mobile nodes in MANET.The method to detect the Sybil attacks RSS. Practical analysis of this work is done using NS2 by measuring throughput, end to end delay, packet delivery ratio under different network conditions [3].
2. In [3], Trusted Certification solution is presented. It is considered to be one of a good preventive solution for Sybil attacks in which a centralized authority is employed for establishing a Sybil-free area of identity. Each unit in the network is bound to a single identity certificate. But trusted certification suffers from costly initial setup, lack of scalability and a single point of attack or failure.
3. In [4] a Sybil attacker can cause damage to the networks several ways. Into this approach the **Cryptographic based authentication** is used to detect the Sybil attack in MANET.It is based on the Trusted certification method which is traditional approach. But the disadvantage of this method is that it required some costly hardware. The RSS based localization is considered one of the promising solutions.
4. In [6] Sybil attack the interloper tries to confine and cooperation some nodes and insert them into several locations throughout the network in order to conduct other types of attacks.
5. A method was introduced in [10] to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is much large difference between the sequence number of source node or intermediate node who has sent back RREP or not. The first route reply will be from the malicious node with high destination sequence number. It is stored as the first entry in the RR-Table.
6. In [11] a mechanism CBDS (cooperative bait detection scheme) is presented that effectively detects the malicious nodes that attempt to launch grayhole/collaborative blackhole attacks. In this scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list.

III. Related Work

Work can be enhanced by implementing the RSS (Received signal strength) method to detect the Sybil attack in the MANET network. This technique uses the RSS in order to differentiate the Sybil identity and legitimate identity. By using this technique all nodes storing history of all nodes in the network and if there will be any misbehaviour of the node then the other node will come to know about the attacker node. These techniques better because it needs not any hardware. In further enhancement i will use CBDS ie collaborative bait detection approach to detect the Sybil attack in the MANET network. In my research part i will use **Bait** to detect the Sybil node in the MANET. After these implementations i will compare the the results of RSS method with CBDS approach to detect the Sybil attack.

Conclusion

It is concluded that Sybil attack which takes identity of some other node can be identified using RSS technique. This technique no doubt increases the time to arrive the packet. But if other technique is followed then this time can also be decreased.

References

1. Detection and Optimisation Techniques against Sybil Attack on MANET, International Journal of advanced Research in Computer Science and Software Engineerig4(8),August-2014,pp. 369-375
2. Architecture for detection of Sybil attack in MANET MAC address, International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 6, Volume 2 (June 2015)
3. Efficient Analysis of Lightweight Sybil Attack Detection Scheme in Mobile Ad hoc Networks IEEE SYSTEMS JOURNAL International Conference on Pervasive Computing (ICPC) 2015
4. Lightweight Sybil Attack detection in MANETs IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013 Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat
5. Comparison between Sybil Attack Detection Techniques: Lightweight and Robust RoopaliGarg1,Himika Sharma2,Coordinator, Dept. of IT, UIET, PanjabUniversity,Chandigarh, India 1 PG Student, Dept.of IT, UIET, PanjabUniversity, Chandigarh, India2
6. Detection And Prevention Of Sybil Attack Using A Thershold Elgamal Key Management Scheme S.Krishna Kumar,V.Shalini, V.Shiva and P.Vijayakanth International Journal of Advances in Engineering, 2015, 1(3), 319 – 322
7. Secure Authentication Protocol to Detect Sybil Attacks in MANETs Nidhi Joshi et al. / International Journal of Computer Science & Engineering Technology (IJCSET)
8. Impact of Sybil Attack and Security Threat in Mobile Adhoc Network International Journal of Computer Applications (0975 – 8887) Volume 124 – No.9, August 2015

9. "A Novel Mechanism for Detection of Sybil Attack in MANETs" International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18, 2014 Dubai (UAE)

10. Combating against Byzantine Attacks in MANET using Enhanced Cooperative Bait Detection Scheme (ECBDS)
11. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015