Secure Routng Scheme Against Byzantine Attack Over MANET

M. Lakshaga Jyothi[1]
M.E. (Final Year - CSE)
Annapoorna Engineering College
Salem, TamilNadu, India

O. Saravanan[2]
Professor (CSE)
Annapoorna Engineering College
Salem, TamilNadu, India

***Abstract*—Mobile ad-hoc network is a collection of semi mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnection between nodes are capable of changing on a continual basis. The primary goal of such a network is to serve the purpose of emergence situations or unexpected environment such as defense sectors. Due to these applications, security in MANET is a significant aspect. This paper is focused on Byzantine attack in MANET's. Byzantine attack can be defined as attacks against routing protocols, in which the attacker try to drop, fabricate, modify or misroute the packets, thus degrading the network performance. In this paper, a secure routing scheme has been designed and implemented to mitigate the attacks by the malicious or compromised nodes in the MANET environment.**

Keywords*— *Secure Zone Routing Scheme, Byzantine Attack, Zone Routing Protocol, MANET Routing Scheme, Black Hole Attack.

I. INTRODUCTION

A MANET network is an arbitrary topology where random nodes are chosen to transmit data. Nodes may be mobile/semi-mobile nodes with no pre-established infrastructure. Each node acquires wireless interface and communicate with each other via radio or infrared channels. Each node can act as both host and the router at the same time so that it can offer services or demanded applications as well as forward packets to the destination. Due to the dynamic nature of the network, minimal configuration and quick deployment which has made its applications ranging from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or interaction with a human. Some examples are: search-and-rescue missions, data collection, and virtual classrooms and conferences where lap-tops, PDA or other mobile devices share wireless medium and communicate to each other.

As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. Therefore, only one compromised node can cause the failure of the entire network. Considering the security impact, Proactive approaches such as cryptography and authentication were brought into consideration, and many techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in. Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity.

II. MOBILE AD-HOC NETWORK

Mobile ad-hoc network is a wireless infrastructure less network with no centralized admin (Client or server). MANET is an arbitrary topology where random nodes are chosen to transmit data from the source to the destination node. These nodes may be mobile or semi mobile nodes. Each node acquires a wireless interface. They communicate via radio or infrared channels. Each node can act as both host and the router. Host implies the device which can request for resources and then offer services, It can behave as both client and server program. So these nodes transmit and receive their own packets and also forward packets to other nodes.

A. MANET Protocol Stack

Due to the dynamic nature of the MANET network, each layer in the MANET Protocol stack is vulnerable to several sources of attacks.

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Eavesdropping, jamming, active interference

Fig.1. Attacks in MANET Protocol Stack

B. Network Layer Attacks

There are many attacks that are degrading the performance of the network system. As we consider the MANET layer

protocol stack, the following below attacks are considerably violating the network system.

In Network layer, the network layer protocols enable the MANET nodes to be connected with another through hop-by-hop. In MANETs every individual node takes route decision to forward the packet, so it's very easy for malicious node to attack on such network. The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic. The Network Layer Attacks include:

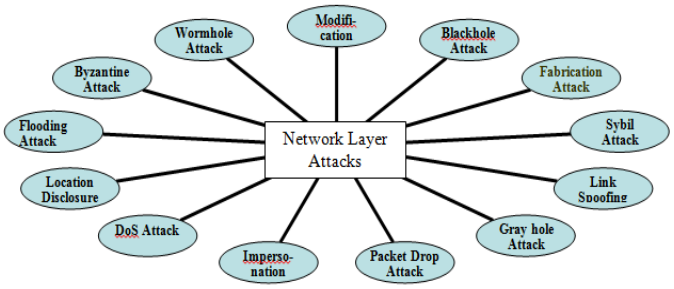

Fig.2. Classification of Network Layer Attacks

C. *Security Goals in MANET*

The goal of system security is to have controlled access to resources. The key requirements for networks are confidentiality, authentication, integrity, non repudiation, and availability etc. Let us examine them each.

Confidentiality*:* It protects data or a field in message. It is also required to prevent an adversary from traffic analysis.

Integrity*:* It ensures that during transmission the packets are not altered.

Authorization*:* It authorizes another node to update information or to receive information.

Availability*:* It ensures that services are available whenever required.

Resilience to attacks: It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

Freshness: It ensures that malicious node does not resend previously captured packets.

Anonymity: This service helps for data confidentiality and privacy.

Access control: It prevents unauthorized access to a resource.
Non- repudiation: No repudiation prevents the source from denying that it sends the packet.

III. OVERVIEW OF THE EXISTING SYSTEM

Zhao et al. [1] proposed an approach, which can be briefly named as 'Risk aware Response Mechanism'. With respect to the protocol used it has implemented the 'OLSR (Optimized Link State Routing) Protocol', which is a proactive protocol not for network with frequently changing nodes. The mathematical theory included, extract evidences based on two input factors namely: Binary Response Rule (BRR) and Fuzzy Response Rule (FRR).

Rajdeep Singh. [2] proposed an approach, such as 'AODV-IPS (Ad-hoc On Demand distance Vector with Intrusion detection and Prevention System)', which has been implemented in a simulation program against the Black hole attack on the AODV protocol.
Considering these systems, either the protocol is not suitable for the desired network implementation or the mechanism is not efficient for secure data transmission.
Weaknesses of the system:

1. BRR may form unexpected network partition, whereas FRR form uncertainty in countering network attacks.
2. All the evidences are treated equally without any priorities

IV. BYZANTINE ATTACK

The main focus of this paper is Byzantine attack of the network layer. It is an attack with a single or a set of compromised intermediate nodes behaving mischievously. The adversary model is implemented in the proposed system. The adversaries are those which do false things against the protocol used. This type of attack performs the following false activities, such as

- ✓ Routing loops
- ✓ Forward packets through non-optimal paths
- ✓ Selectively drop packets

A. *Black hole attack:*

It is the ***basic Byzantine Attack*** where the adversaries stop forwarding the data packets but still participates in the routing protocol correctly. This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination.

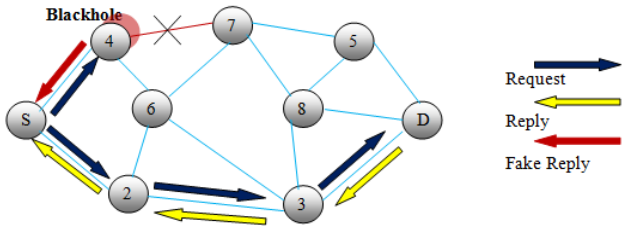

Fig.3. Black hole attack

B. *Countermeasures taken against the attack*

A secure on-demand MANET routing protocol, named Robust Source Routing (RSR) is proposed as countermeasure of Byzantine attacks. A Chord mechanism is proposed which is a distributed hash table (DHT).

A secure on-demand MANET routing protocol, named Robust Source Routing (RSR). In addition to providing data origin authentication services and integrity checks, RSR is able to mitigate against intelligent malicious agents which selectively drop or modify packets they agreed to forward. Simulation studies confirm that RSR is capable of maintaining high delivery ratio even when a majority of the MANET nodes are malicious.

V. PROPOSED SCHEME

A. PROTOCOL IMPLEMENTATION

This paper presents the Zone Routing Protocol. Initially, it discusses the problem of routing in ad-hoc networks and the motivation of ZRP. It describes the architecture of ZRP, which consists of three sub-protocols. It describes the routing process and illustrates it with an example.

The Zone Routing Protocol, as its name implies, is based on the concept of zones. A routing zone is defined for each node separately, and the zones of neighboring nodes overlap. The routing zone has a radius ρ expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most r hops.

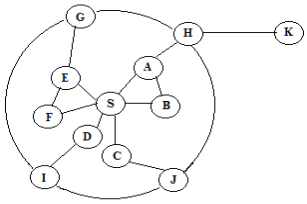

Fig.4. Sample node with hop radius r = 2

An example routing zone is shown in Figure 1, where the routing zone of S includes the nodes A–I, but not K. In the illustrations, the radius is marked as a circle around the nodes. It should however be noted that the zone is defined in hops, not as a physical distance. The nodes of a zone are divided into peripheral nodes.

1) ZRP Architecture:

The architecture of ZRP consists of three sub protocols namely, IERP, IARP and BRP

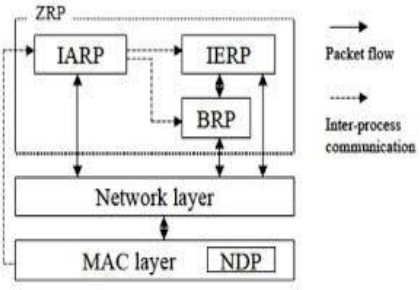

Fig.5. ZRP Architecture

IARP: Intrazone Routing Protocol

It is used for communicating with the interior nodes of the zone and maintains route table for nodes inside the zone, each node continuously needs to update the routing information in-order to determine peripheral nodes and maintain map of which nodes can be reached locally.

IERP: Interzone Routing Protocol

It is used to communicate between nodes of the zones. It helps to formulate route discovery. Route discovery is done through process called *bordercasting* that use BRP to only transmit route requests to peripheral nodes.

BRP: Bordercasting Routing Protocol

Direct route request from IERP to peripheral nodes and use topology information from IARP to construct bordercast tree. For route request from node outside zone, a query control mechanism is employed.

Using BRP, source sends RREQ packet to peripheral nodes. If node receiving RREQ packet knows destination sends a route reply to source, otherwise process continues by broadcasting packets. So, it may lead to more traffic due to overlapping zones and frequent requests from source to each node that are with the zone.

To overcome this, ZRP uses:-

Query detection: It is possible to detect query relay by other nodes in same zone to prevent them from reappearing in covered zone.

Early termination: A node can prevent route request from entering already covered regions using early termination.

***Query processing delay*:** It is employed to reduce probability of receiving same request from several nodes. Each broadcasting node wait a random time before constructing bordercast tree and early termination. During this waiting node detect queries from other broadcasting nodes and prune bordercast tree.

B. NETWORK IMPLEMENTATION

The proposed network architecture has to be implemented using a Java Swing Framework. This system helps in deriving an effective mechanism to mitigate risk levels against Byzantine attacks. And hence, analyze the network performance of the system and achieve major security goals in MANET. To mitigate the risk level a secure encryption (DSA + SHA-1) model has been implemented. Then on identified risk levels and isolation models further security has been proposed.

TABLE I. NETWORK CONFIGURATION

Components	*Configuration*
Server	WampServer 2.0
Database	MySQL
No. of Nodes	Sample of 20 nodes
Packet Size(Bytes)	512
Mobility Model	Random Node Point
Simulation Time	Min (as Reqd.)

C. PROPOSED SCHEME

The approach is defined as “Secure Zone Routing with Acknowledgement” Mechanism (Secure-ZRAM) includes the following steps. This is an Acknowledgement based Intrusion Detection System where it rely on the acknowledgement packets to detect behaviors in the network. Thus, it is extremely important to ensure all acknowledgement packets are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement packets, the proposed scheme will be vulnerable.

To overcome these loopholes, digital signature is implemented. In order to ensure the integrity of the IDS, Secure-ZRAM requires all acknowledgement packets to be

digitally signed before they are sent out, and verified until they are accepted.

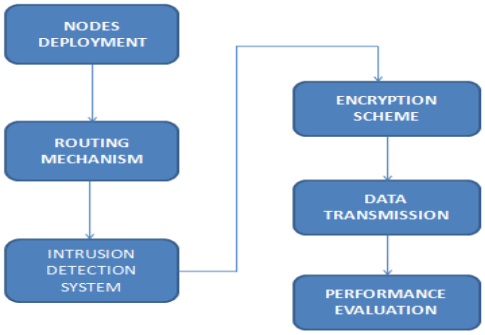

Fig.6. Secure ZRAM

Steps to be outlined briefly:

1. Randomly nodes are deployed so that each node can be a transmitter or receiver.
2. With the source and destination specified, they are initiated for data transmission based on the routing mechanism.
3. Based on the Acknowledgement report the network is checked against the intruder invasion from outside the network as well as the compromised node.
4. For more efficient transmission and authentication of the user, Digital Signature Scheme is implemented.
5. After the data transmission and once the data reach the destination, performance evaluation proceeds.
6. Based on the results, further enhancements have to be provided.

D. SECURITY MODEL

In this system model, an attempt is made using the following Digital Signature algorithm integrated with SHA1 (Secure Hash Function) in-order to achieve Authentication, Integrity, Confidentiality, Non-repudiation, Freshness and Anonymity.

1. Digital Signature Algorithm(DSA):

Digital signatures are essential in today's modern world to verify the sender of a document's identity. A digital signature is represented in a computer as a string of binary digits. The signature is computer using a set of rules and parameters (algorithm) such that the identity of the person signing the document as well as the originality of the data can be verified.

The signature is generated by the use of a private key. A private key is known only to the user. The signature is verified makes use of a public key which corresponds to (but not the same, i.e. mathematically infeasible to deduct private key from public) the private key. With every user having a public/private key pair, this is an example of public-key cryptography. Public keys, which are known by everyone, can be used to verify the signature of a user. The private key, which is never shared, is used in signature generation, which can only be done by the user.

2. Secure Hash function(SHA 1):

There are three algorithms that are suitable for digital signature generation under the DSS standard. They are the DS algorithm, the RSA algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA). Also in this standard is a hash function to be used in the signature generation process. It is used to obtain a condensed version of the data, which is called a message digest. This message digest is then put into the digital signature algorithm to generate the digitally signed message. The same hash function is used in the verification process as well. The hash function used in the DSS standard is specified in the Secure Hash Standard (SHS), which are the specifications for the Secure Hash Algorithm (SHA).

The SHA is based on principles similar to those used by Professor Ronald L. Rivest of MIT when designing the MD4 message digest algorithm and is closely modeled after that algorithm. When a message of any length $< 2^{64}$ bits is input, the SHA produces a 160-bit output (message digest). Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message.

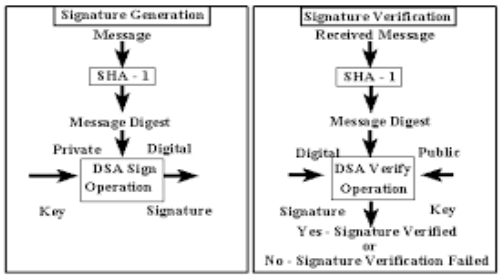

Fig.7. Using SHA-1 with DSA

VI. CONCLUSION

After successful implementation of the MANET environment, the system has to be analyzed against the network performance metrics of the system and the security goals in MANET. To mitigate the risk levels, a secure encryption model has been implemented. Based on the identification report, Isolation models are to be implemented for further security in the MANET network.

VII. REFERENCES

[1] Ziming Zhao, Hongxin Hu and Ruoyu Wu, "Risk Aware Mitigation for MANET Routing Attacks," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, March - April 2012.

[2] J. Clerk Maxwell, "Detection and Prevention from Blackhole Attack in AODV Protocol", IJCA, vol. 50. No.5 July 2012.

[3] Mangesh M Ghonge, Pradeep M Jawandhiya and Dr. M.S. Ali, "Countermeasures of Network Layer Attacks in MANETs," IJCA, Special Issue on "Network Security and Cryptography", NSC, 2011.

[4] Prasanth Mohapatra and Srikanth Krishnamurthy, "Adhoc Networks: Technologies and Protocols,".

[5] http://www.cs.gsu.edu/~cscazz/CS8550/Ad_Hoc_tutorial.pdf.

[6] http://www.antd.nist.gov/wahn_mahn.shtml.

[7] http://www.slideshare.net/sunitasahu101/attacks-in-manet.