REVIEW ON BYZANTINE ATTACK IN MANET AND SOLUTION TO AVOID

Manohar B S[1], Mahesh Kumar N[2]

[1]M.Tech Student, ECE, DSCE, Bengaluru
[2]Asst. Professors, ECE, DSCE, Bengaluru

Abstract - MANET (Mobile ad-hoc network) are widely used in enormous number of applications especially in military and disaster measurement where secure communication is most important. The various threats or attacks are takes place on the network to degrade the network performance. This paper outlines the Byzantine attack and comparative analysis with different attacks among these attacks. And also presented the solution to the problem of Byzantine attack that arises in most of network scenarios.

Key Words: *MANET, byzantine attack, Hash function*

I.INTRODUCTION

Mobile ad-hoc network (MANET) is a peer to peer communication network that connects vast number of wireless nodes in decentralized structure[1] [2] [3]. Which is used to communicate through nodes with randomly change its topology. Each node in the network performs various functions i.e. it acts as a sender or receiver or acts as router between the path from sender to receiver in the network, where the each node make decision randomly the main characteristics of MANETs doesn't have centralized topology and weak physical protection of nodes, and randomly changing topology by its own decision.

However the open and shared wireless mediums of ad hoc network make it susceptible to continuously evolving both inside and outside attacks. So that establishing security mechanisms against the attacks in the network is one of the major tasks, when there are many attacks performed on the network. In this context mainly focus on one of the insider attacks on the network known as byzantine attack. This gives the potentially malicious nodes perform Byzantine attacks by altering the information intended for the destination, it is hard to predict in the network. Such attacks degrade the security of the network performance. Security attacks can be broadly classified in to two types: active and passive. The main aim of the active attacks is to destroy or modify the original data transmitted or tries to alter the regular functioning of the network. Passive attacks do not alter the normal network function; it aims to interfere the network and tries to read the data that is transmitted over the network without modifying any data. It challenges the confidentiality of the network if the actual data is interpreted. It is very difficult to detect the passive attacks as it won't affect the normal functioning of the network. For that establishing the security mechanism against the byzantine attack by using hash function method in this context.

In this paper, identification of the byzantine attacks and techniques to preventing the MANET from that attack. Section 1 discussed working of MANETs, and different types of attacks in different OSI layers Section 2 discussed problem of byzantine attacks in MANET. Section 3 contains proposed work to solve the problem. Section 4 contains result and conclusion obtained. Section 5 and 6 discusses conclusion, section 7 discuss References. Below table shows different types of attacks takes place in different OSI layers [1].

II. MAJOR TYPES OF ATTACKS AND CLASSIFICATION IN MANET

Table 1:Different types of attacks on different OSI layers

LAYERS	ATTACKS /THREATS
Application layer	Repudiation, cross site scripting attack, Data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, Information discloser attack, Black hole, Byzantine, Flooding, Routing attack,
Data link layer	Monitoring and Disrupting MAC frames.
Physical layer	Interceptions, Eaves Dropping

The attackers can be categorized into: Insiders and outsiders. If the malicious nodes from outside of the network attacks the network nodes by snooping the IDs and pretend to be an authorized node, the privacy and authenticity of the network can be compromised and are called as outsider attacks. The active or passive attacks that are performed by the compromised internal nodes by tracking its neighbors, flooding the wrong false message on routing and so on is called are as insider attacks. These are more hazardous than outsider attack and are too difficult to trace and mitigate such attacks as they are the active members of the network.

III. BYZANTINE ATTACK

It is one of the insider attack in mobile ad hoc network compare to other attacks it is hardly predict in the network, These are more hazardous than outsider attack and it is too difficult to trace and mitigate such attacks as they are the active members of the network. These attacks are also known as byzantine attacks. Once the active set of insider nodes in the network will corrupted by the attacker then the whole network will be control over attacker and further secured data transmission is not possible .this is very dangerous in case of mobile devices used in military and medical for transferring patients and reports, A byzantine attack can prevent the route establishment by dropping the route request or response packets, the attacks in which a single node or a set of nodes works together to create loops ,forwards packets through non optimal paths or selectively drops the packets which results in disruption or degradation of the routing services and network performance[2].

Some Features of Byzantine attack are as follows:

- Directing circles within the nodes with no definite ends.
- Sending parcel through non-ideal way.
- Specifically dropping of packets

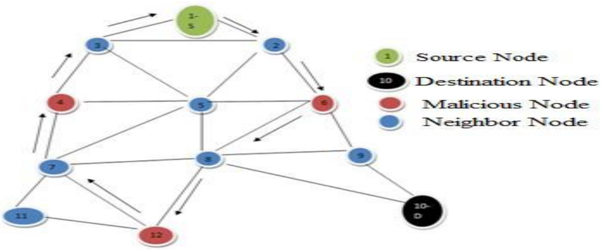

Fig 1 :Byzantine attack in the network

IV. RELATED WORK

In mobile ad hoc networks (MANETs), a source node must rely on other nodes to forward its packets on multi-hop routes to the destination. Secure and reliable handling of packets by the intermediate nodes is difficult to ensure in an ad hoc environment. They propose a trust establishment scheme for MANETs which aims to improve the reliability of packet forwarding over multi-hop routes in the presence of potentially malicious nodes[3].

Paper[4] proposed a protocol that uses a reputation mechanism to detect the misbehaving nodes using watchdog and path rater. A trust manager estimates the level of trust of alert reports and the reputation system estimates the each node's reputation. Each node prepares a report about other nodes and the trusted nodes reports only will be processed. Drawback of this paper it is not clear how the trusted nodes turned to be as compromised nodes and the reputation systems do not provide any protection against false accusations.

In mobile ad hoc networks, the co-operation of the intermediate nodes that exists between the source and destination. The co-operation among the active mobile nodes is more crucial mainly due to the resource constraint challenge of ad hoc networks. Besides, the byzantine behaviour of mobile nodes degrades the survivability of the network. In this paper, we propose a Cohen Kappa Reliability Coefficient based Reputation Mechanism (CKRCRM) for detecting and mitigating byzantine attack through a statistical reliability coefficient. The performance of CKRCRM is analysed using ns-2 simulator and is observed[5].

Paper[6] they implemented secure packet transmission in mobile adhoc network (MANET) through Adhoc On Demand Multipath Distance Vector (AOMDV) routing protocol. AOMDV, a multipath extension of AODV (Adhoc on Demand Distance Vector) routing protocol, is more reliable than its parent protocol, though not completely restraint from attacks. Elliptic Curve Cryptography (ECC) has been chosen to secure the packets against byzantine attack. Elliptic Curve Cryptography provides security with smaller key size compared to other public-key encryption.

Hash function generation which is a one-way encryption code used for security of data. The main examples include digital signatures, MAC (message authentication codes) and in smart cards. Keccak, the SHA-3 (secure hash algorithm) has been discussed in this paper which consists of padding and permutation module. This is a one way encryption process The implementation process is very fast and effective[7].

V. PREVENTION OF BYZANTINE ATTACK USING HASH FUNCTION

It is one of the advance technique to secure the data while data packets communicate between the nodes using cryptography functions Message authentication is a mechanism to verity the integrity of a message and it can be achieved using Message Authentication code (MAC) also called as keyed hash function.

Features of Hash Functions

The typical features of hash functions are

- Fixed Length Output (Hash Value)Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
- In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions.
- Hash function with n bit output is referred to as an n-bit hash function. Popular hash functions generate values between 160 and 512 bits.

Popular Hash Functions

Let us briefly see some popular hash functions

1) Message Digest (MD)

- The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.

2) Secure Hash Function (SHA)

Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.

- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.
- SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.

SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.

- Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.

3) RIPEMD

The RIPEND is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was designed by open research community and generally known as a family of European hash functions.

4) WHIRLPOOL

This is a 512-bit hash function.

- It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.

VI. CONCLUSION

In this paper mainly described how the communication is takes place in mobile ad-hoc network and for secure communication, this work is going to deal with the derivation of hash security mechanisms in distributed MANET's. It will help in improving the security of MANET from the attacks, one of the insider attacks in the network is Byzantine attack and it is very difficult to detect and similar types of attacks are mentioned above. This paper proposes the attack defense system that will strengthen the defense mechanism in MANET which will be the responsibility of individual nodes. The mean field hash function provides a powerful tool for problems in network. This scheme can enable an individual node in MANETs to make strategic security defense decisions without centralized administration to defend and detect the Byzantine attack.

REFERENCES

[1]. Ad-HocNetworking towards Seamless Communication book by L. Gavrilovska and R. Prasad, published by Springer, 2006.

[2]. Geetha, A and Sreenath, N., "Cohen Kappa Reliability Coefficient Based Mitigation Mechanism For Byzantine Attack In Manets". International Journal of Applied Engineering 2015.

[3]. Zouridaki C,Mark BL,Hejmo M,Thomas RK.A quantitative trust establishment framework for reliable data packet delivery in MANETs.In:Proc,of 3r ACM workshop on security of adhoc and sensor networks,vol .1,no.1,p.1-10.2009

[4]. S. Buchegger and J-Y.L. Boudec , "Performance analysis of the CONFIDANT protocol", In Proceedings of the 3rd ACM Symposium on Mobile Ad Hoc Networking and Computing, pp. 226-236, 2010.

[5]. Geetha, A and Sreenath,N., "Cohen Kappa Reliability Coefficient Based Mitigation Mechanism For Byzantine Attack In Manets". International Journal of Applied Engineering 2016

[6]. Jeenat Sultana and Tasnuva Ahmed "Securing AOMDV Protocol in Mobile Adhoc Network with Elliptic Curve Cryptography" International Conference on Electrical, Computer and Communication Engineering (ECCE), February 16-18, 2017

[7]. Madhura A. Patil, Pradeep. T. Karule, Member, "Design and Implementation of Keccak Hash Function for Cryptography" This full-text paper was peer-reviewed and accepted to be presented at the IEEE ICCSP 2015

[8]. Zouridaki C,Mark BL,Hejmo M,Thomas RK.A quantitative trust establishment framework for reliable data packet delivery in MANETs.In:Proc,of 3r ACM workshop on security of adhoc and sensor networks,vol .1,no.1,p.1-10.2013.