PREVENTION OF BYZANTINE ATTACK IN MANET BY USING SHA FUNCTION

[1]Manohar B S, [2]Mr. Mahesh kumar N

[1]Student,MTech,Digital Electronics and Communication,[2]Asst Professor, Digital electronics and Communication
[1]Digital electronics Engineering, [2] Department of DEC,
[1&2] Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

Abstract : MANET (Mobile ad-hoc network) are widely used in wide 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 hash function solution to the problem of Byzantine attack that arises in most of network scenarios.

Index Terms - MANET, Byzantine attack, hash function.

I. INTRODUCTION

Mobile Ad-hoc network (MANET) is an end to end communication(data transmission) network it connects large number of wireless nodes it doesn't have decentralized structure means any particular node will not control the any nodes in the network these networks used to communication purpose among nodes with contionusly changing its topology.[1][2][3] Each nodes in the network performs sender and receiver and some times acts as router for transmission of data from source to the destination.the main characterstic of MANET are nodes will take an own decision while communication take place between nodes in the network.and also for the data transmission preferly used AODV routing protocol.

However the wireless network also as called shared wireless medium of ad hoc network make it susceptible to continuously evolving both inside and outside attacks. For that establish the defense mechanism against the attackers in the network is the one of the major tasks, there are various numbers of attacks will takes place in the network. In this paper mainly focused on one of the insider attack(attack takes place in among the nodes in the network) called as byzantine attack this attack has taken place in the network OSI layer, main characteristics of this attack will degrade the performance of the network and also altering the information transmitted between nodes so on. And it is hardly predicted in network, security attacks mainly classified into two types namely active and passive attacks the main goal of the active attack is to destroy the original data and it tries to vary the normal function of the network. passive attacks will do not alter the any original information but its aim to interfere in the network and read the data without modifying any original data. So for that this paper describes the security mechanism against the byzantine attack by using hash function .The attacks can be divided into insiders and outsiders where insiders attackers flooding the wrong messages on routing insiders attacks will compromised with nodes. And it is more hazardous compare to outsider attacks and difficult to mitigate in the network. Outsider attack will takes place when the malicious nodes from the outside of the network by snooping the IDs and act as an authorized node.

This paper outlines the "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 methodology work. Section 4 contains related work to solve the problem. Section 5 discusses proposed work , section 7 discuss References. Below table shows different types of attacks takes place in different OSI layers" [1].

OSI LAYERS	THREATS
Application layer	Cross site scripting attack, Data corruption
Transport layer	SYN flooding
Network layer	Byzantine attack wormhole attack
Data link layer	Monitor and disrupting MAC frames
Physical layer	Interceptions

Table 1:Different types of attacks on different OSI layers

II. BYZANTINE ATTACK

"Byzantine attack is the one of the insider attack takes place in the network it is hardly predict in the network it is more hazardous than outsider attack and it is too difficult to mitigate and trace. Once the attack takes place it will act has active member of the network ,once the attack take place it will corrupted the network and take the control of the overall network this leads to secure communication not possible, this is very dangerous attack in case mobile communication used in the field of military and medical for sending patients reports and confidential information.[2] Byzantine attack will prevent the route establishment by dropping the route request, this type attack will takes place by single node or group of nodes and main characteristics of the byzantine attack is forward the packets through non optimal paths this results leads the degradation of the performance of the network".

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

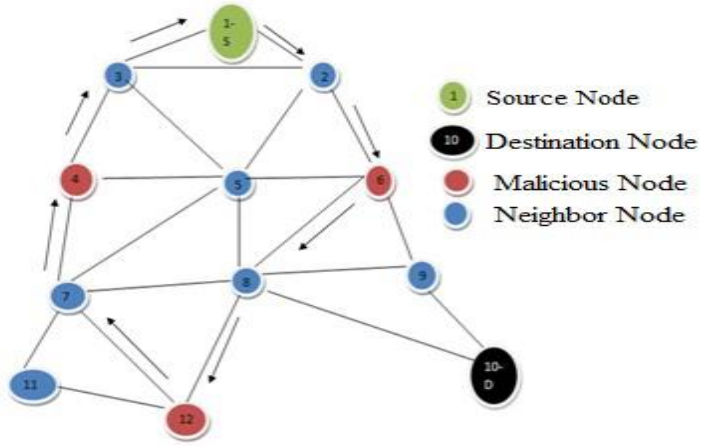

Figure 1: Structure of Byzantine Attack

II. LITERATURE REVIEW

In mobile ad-hoc network source node will must depends on other nodes to forward the packets to the destination secure transmission from the intermediate nodes is also important task in the ad-hoc environment. Author proposed a trust establishment scheme for MANETs to improve the realibility of packet forwarding over the multihop routes in the presence of malicious nodes[3].

A protocol that used in reputation mechanism to analyze the misbehaving node in the network by using watch dog and path rater. Here in this paper also the author tells about trusted node where the each node prepares the report about other nodes and the trusted nodes reports only will be processed.

In MANETs co-operatiuon between source and destination,The co-operation between the active nodes is more crucial mainly due to the resource constraint challenge of ad hoc networks. Upon the byzantine behavior of nodes in the network degrades the survivability. In this paper author propose a cohen kappa reliability co-efficient based reputation mechanism(CKRCRM) for detecting and mitigating the byzantine attack. Performance of the CKRCRM is analyzed using ns-2 simulator[5].

New security technology Hash function is used to avoid the byzantine attack ,the different types of authentication methods are digital signatures, MAC(message authentication code) and Hash function,In this paper SHA-1 (secure hash algorthim) one way encryption process,this implimation is very fast and very effective[7].

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. Each node forms an "opinion" about each of the other nodes based on both first and second-hand observation data collected from the network. The opinion metric can be incorporated into ad hoc routing protocols to achieve reliable packet delivery even when a portion of the network exhibits malicious behavior. This paper present numerical results which demonstrate the effectiveness of the proposed trust establishment scheme[8].

III. METHODOLOGY

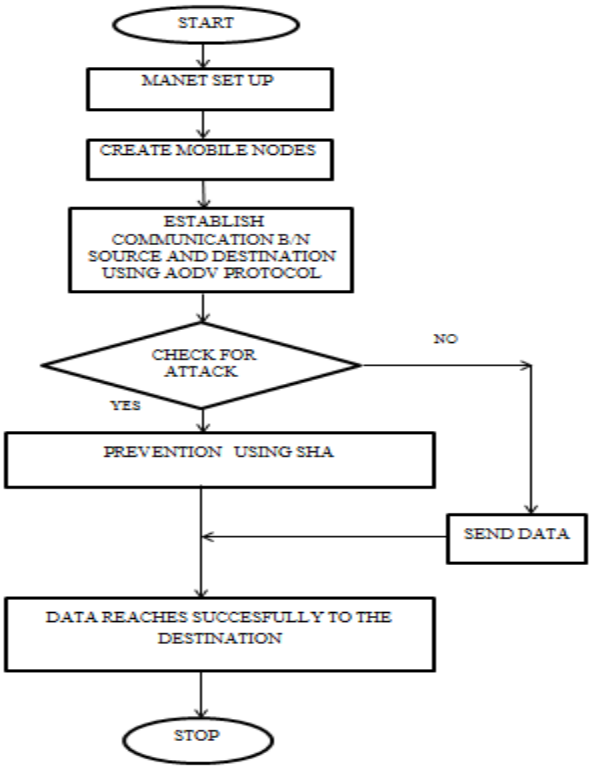

Fig 2: shows the flow Chart of the overall processes

1.MANET SET UP

Intially set up MANET requirements before data sent and receiving while in this I define the which channel is better for the transmission and propagation model, and type of interface used and which type of antenna is used for transmission and packet length and also number of mobile nodes is used and measurement of x and Y topography, and time of the simulation ends.

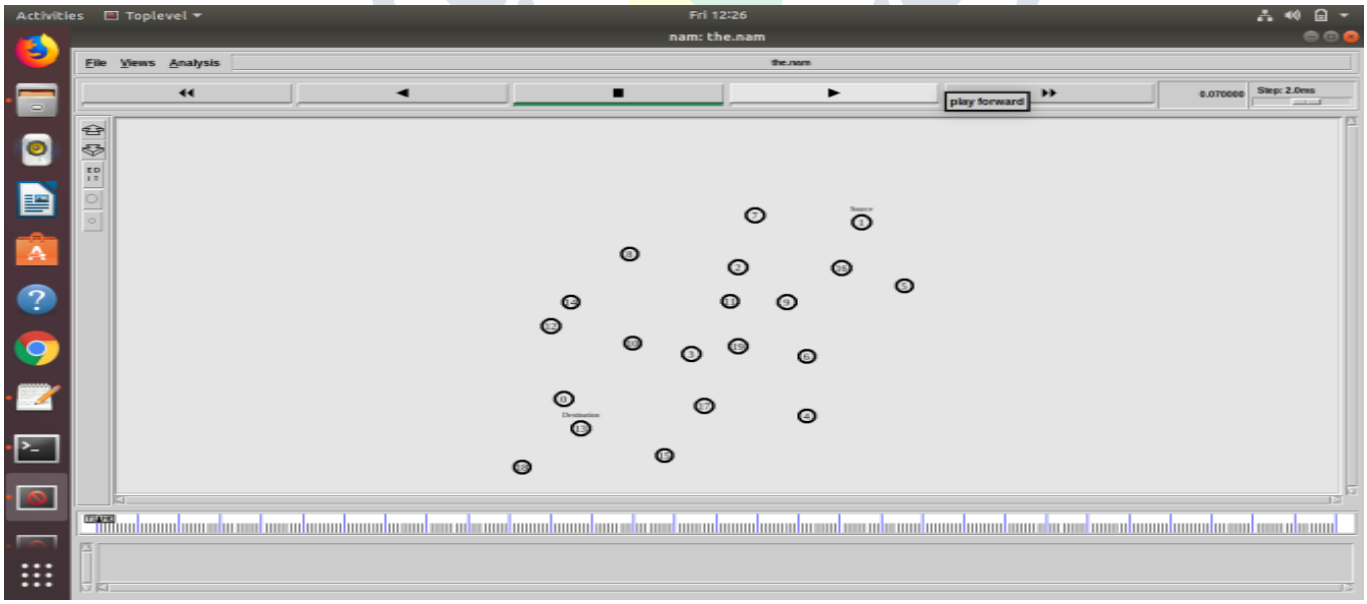

Fig3: Creation of mobile nodes

2.CREATE MOBILE NODES

After describe the basic requirments of MANET later describes the various number of mobile nodes by naming as source and destination for transmission of data by placing the nodes in X –Y co-ordinates. So before creating mobile nodes I have to set trace file for trace the path of every operation and create an animator file for simulation of the process.

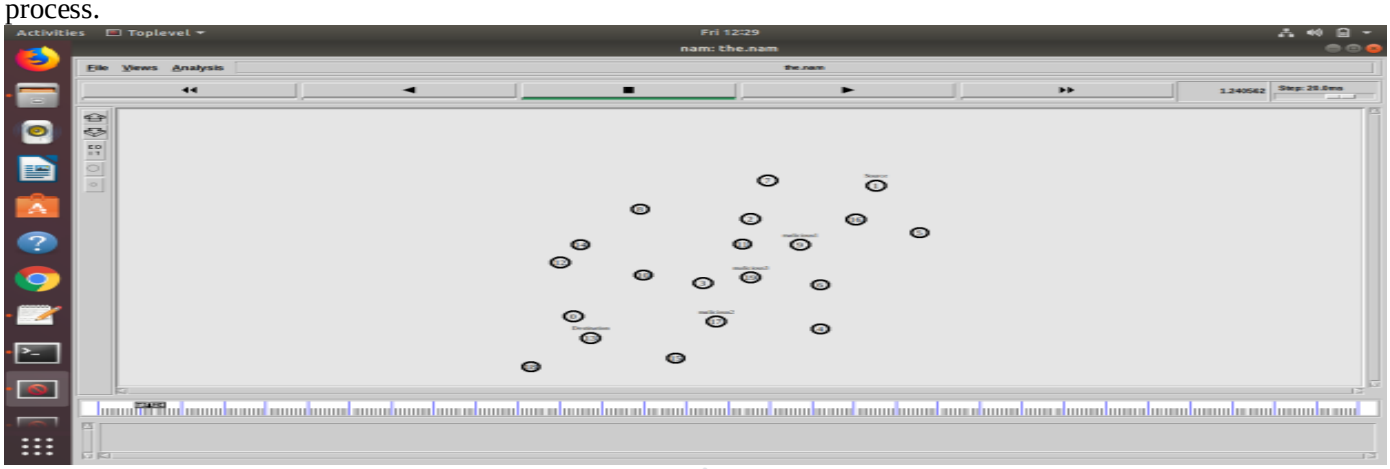

Fig 4:Define the malicious nodes

3.NODES SEND DATA TO DESTINATION USING AODV PROTOCOL

While after set above these parameters the nodes will send the data to destination through intermediate nodes using AODV protocol where source will send the RREQ to every nodes until it reaches to destination node. while receiving the RREQ The received nodes will reply back by sending RREP in form of acknowledgement. After these process completed the source node will send the data to the target through easy path.

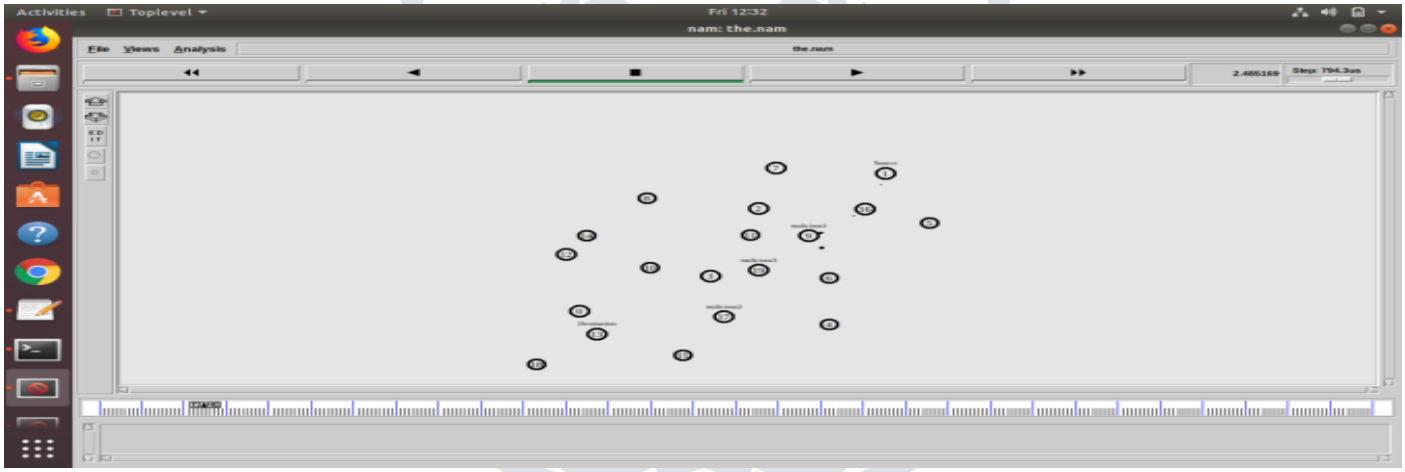

Fig 5:shows packets dropped in malicious node

4. OUTPUT OF BYZANTINE ATTACK LEADS PACKET DROPS

```
manohar@manohar-Lenovo-G510:~/MTech/pf/1$ ns 1.tcl
num_nodes is set 20
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
end simulation
manohar@manohar-Lenovo-G510:~/MTech/pf/1$ Cannot connect to existing nam instance. Starting a new one...
perl analyze.pl the.tr
Data Sent              : 556
Data Recv              : 496
Router Drop            : 59
Delivery Ratio         : 89.2086330935252
```

Fig 6:shows the output of packets dropped in malicious node in the network

5.PREVENTION USING SECURE HASH ALGORITHM

If the attacker will drop the packets it cause dropping of data so to prevent the attack by using SHA to secure the data This can be explain in proposed methodology.

IV. PROPOSED WORK TO SECURE THE DATA

It is the one of the new technique to give security for the data while data packets communicate between the nodes it can be achieved by using message authentication code(MAC) it is also known as keyed hash function.

Main features of Hash function

- Fixed output length(Hash value)-Hash function will converts the arbitrary length of the data to the fixed value between 160 and 512 bits.

Popular Hash Functions

Let us briefly see some popular hash functions

1.MESSAGE DIGEST(MD)
2.SECURE HASH FUNCTION(SHA)

SHA function mainly divided into Different families namely SHA-0,SHA-1,SHA-2,

- The original version of SHA-0 produces the 160 bit outputs, SHA-1 is most widely used in existing technology to secure the data it is also produces the fixed output length of 160 bits.
- It is difficult to break down the security given to the data.

3.RIPEMD
4.WHIRLPOOL

V. CONCLUSION

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 derives the defence system in the MANET which will be the individual nodes responsibility .The hash function provides a powerful tool for the secure the data in the network and it is hardly decrypt the data by the attackers and also it will defend the byzantine attack in the network.

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.