Prevent Byzantine Attack on Manet Using Enhanced Co-Operative Bait Detection and Prevention Scheme

P. Anusuya
M.Tech, Deportment of IT, Dr Sivanthi Aditanar College of Engrineering,Tamilnadu.

R. Chithradevi
Assistant Professor, Deportment of IT, Dr.Sivanthi Aditanar College of Engineering,Tamilnadu.

S.Dhivya
M.Tech, Deportment of IT, Dr Sivanthi Aditanar College of Engrineering,Tamilnadu.

Abstract – A Mobile Ad hoc Network (MANET) is a dynamic wireless network that can be formed infrastructure less connections in which each node can act as a router. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using ECBDS (Enhancement Cooperative Bait Detection and Prevention scheme) technique to prevent Byzantine attacks in MANET.

Index Terms – MANET, Router, Byzantine Attacks, ECBDS.

1. INTRODUCTION

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. The loss of confidentiality and integrity and the threat of attacks are risks typically associated with wireless communications. An intermediate node can exhibit such routing misbehaviour either alone or in collusion with other nodes. The routing protocol in MANET which encompasses all-node-as router idea assume that the nodes will fully participate. Unfortunately, node misbehaviour is a common phenomenon. Misbehaviour is due to selfish, malicious, overload or broken reasons. The Byzantine behaviour culminates in scrambling of the auction services which leaves online trading community in lurch. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks these functions are carried out by all available nodes. Therefore MANETs, do not have a clear line of defence, and every node must be prepared for encounters with an adversary directly or indirectly.

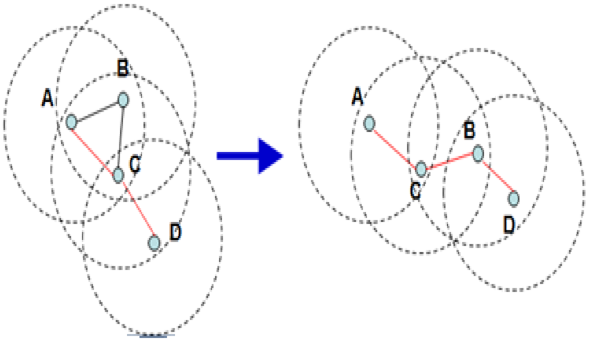

Figure 1 MANET for data routing

Figure 1 shows in MANET nodes are independent to travel in any bearing and will in this way change their connections to different nodes over and over. Each node will forward traffic to other nodes and acts as switch. The significant test in building a MANET is making every gadget to screen and keep up the data needed to movement steering. The target of this paper is to propose a helpful trap discovery plan to battle sleep deprivation and DoS assault over MANET. This plan blends the proactive and receptive resistance structural engineering in MANET by utilizing the first bounce neighbour deliver as destination location to trap the noxious hubs which were creating the assault. Infrastructure oriented system is more powerful as compared to MANET.

2. RELATED WORK

Authors [3] has designed a Dynamic Source Routing (DSR) scheme called as Cooperative Bait Detection Scheme (CBDS) to solve the issues of black hole and gray hole assaults initiated by suspicious hubs. It joins the upsides of both proactive and receptive recognition plans to identify malignant hubs as proactive location plan screens close-by hubs and keeping away from assaults in starting stage and responsive identification plan triggers just when discovery hub recognizes huge drop in conveyance proportion. It accomplishes its objective with Reverse tracing strategy. Cooperative Bait Detection plan is proposed to identify suspicious hubs in MANET for the black hole and gray hole assaults. Cooperative Bait Detection Scheme (CBDS) has been utilized to handle black hole and gray hole assaults brought on by malevolent hubs CBDS consolidates the benefits of both proactive and receptive discovery plans to recognize harmful hubs as proactive identification plan screens close-by hubs and staying away from assaults in starting stage and reactive detection scheme started just when recognition hub identifies critical drop in conveyance proportion. Nonetheless, the regular steering conventions in current, for example, DSR AODV thus on very nearly take account in execution. The related method about recognition and reaction are missing in these protocols.

In this paper [9] author proposed a safe and productive methodology for the identification of the black hole assault in the Mobile Ad hoc Networks taking into account AODV. The methodology is called as Local Intrusion Detection Security Routing (LIDSR) scheme. This methodology serves to lessen the security component overheads. In this scheme, with the assistance of the past hub just before the malicious hub as opposed to distinguishing the malicious hub with the assistance of the Source or the originator hub, the black hole node is identified.

3. PROPOSED WORK

Attack Defence System in MANET Using Enhancement Cooperative Bait Detection and Prevention scheme

The ECBDPS scheme is here to identify byzantine attacks and prevent them from interrupting data from reaching its destination. Identification of the attack is done on basis of symptoms. These symptoms are mention greedy node work alone or an arrangement of bargained intermediate node works between the sender and recipient and perform a few progressions, for example, making directing circles, sending parcel through non-ideal way or specifically dropping bundle, which bring about interruption or corruption of steering administrations.

Byzantine Attack

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services. Attacks where the adversary has full control of an authenticated device and can perform arbitrary behaviour to disrupt the system are referred to as Byzantine1 attacks. Although many Byzantine attacks share certain features with the “selfish” node problem (e.g. not forwarding the data packets of others), the intentions of nodes under these two models are different. The goal of a selfish node is to reap the benefits of participating in the ad hoc network without having to expend its own resources in exchange. In contrast, the goal of a Byzantine node is to disrupt the communication of other nodes in the network, without regard to its own resource consumption.

ECBDPS

A mechanism called “Enhancement cooperative bait detection scheme” (ECBDS) is presented that effectively detects the malicious nodes that attempt to byzantine attacks. In our 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 malicious node 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.

Figure 2: Below the figure first over all the set Manet framework. Then finding the overall packet sends the source and destination. Shortest path calculated for using dijkstra algorithm. Then a packet sends the data. If attack is occur then detecting byzantine attack using ECBDPS. Then attack are detected to prevent another path. If attack is not occured packets are sending to destination.

Proposed mechanism of ECBDPS can be easily understood through the following algorithm

1. Generate Placement of Nodes (N)
2. Communication of Each Node and Packet Transfer
3. Nodes randomly choose the address of neighbour node.
4. If any node reply from other route then Trigger the reverse program and send test packets and detect malicious node.
5. If there is a route lost then Detect the Faulty nodes by sending test packets.
6. Generate the faulty nodes list.
7. If generate the path on the basis of shortest path Detection algorithm
8. If there is a faulty node in the path then don’t send any packets to them and ignore them.
9. Continue transmission until packet received to destination.

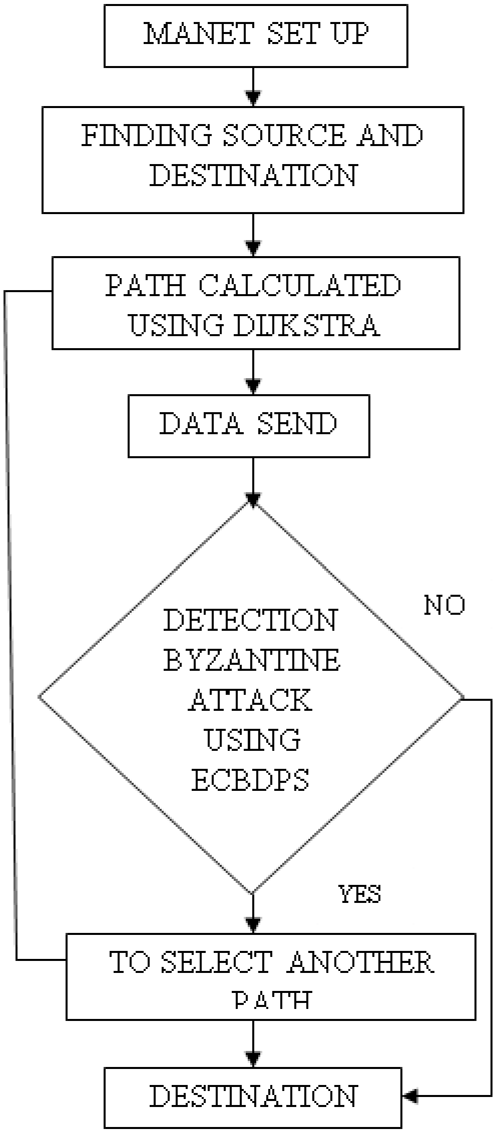
MANET SET UP
FINDING SOURCE AND DESTINATION
PATH CALCULATED USING DIJKSTRA
DATA SEND
DETECTION BYZANTINE ATTACK USING ECBDPS
NO
YES
TO SELECT ANOTHER PATH
DESTINATION

Figure 2: Flow diagram of proposed system

4. PERFORMANCE EVOLUTION

Basic CBDS and ECBDPS schemes have been executed utilizing NS2. The objective of this execution is to make correspondence more solid then Basic CBDS Approach therefore counteracting Byzantine Attack.

THROUGHPUT

Throughput is defined as the rate of successful message delivery in a given time. In case of ECBDPS the throughput is higher than the CBDS.

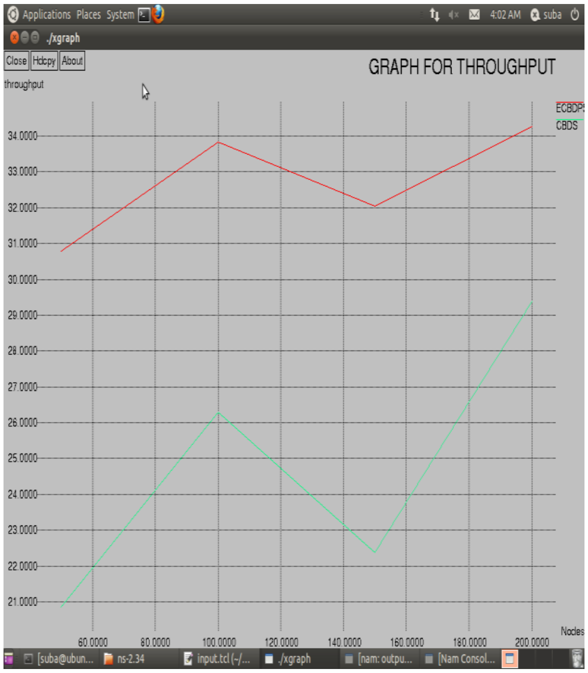

Figure 3: Comparison Graph in terms of Throughput

Figure 3 show that when number of malicious nodes increases the throughput of CBDS scheme reduces. The throughput is typically measured in bits per second, as in megabits per second or gigabits per second and sometimes in message delivered per time space. While in case of ECBDPS the throughput is much greater than basic CBDS.

5. CONCLUSION

The MANET security is still a big issue and the research work is also in initial stage. The current recommendations are normally assault situated in that they first distinguish a few security dangers and after that improve the current convention or propose another convention to defeat such dangers. Since the arrangements composed are unequivocally characterized. The CBDS system joins both proactive and responsive discovery plans which improve its effectiveness of identification.

ECBDPS has been effectively executed on different assaults like resource consumption before and has ended up being just as proficient in the event of byzantine attack identify and prevention as well. ECBDPS does not avoid malicious attack but there every node has individual

Responsibility for transmission and reception of packet data.

REFERENCES

[1] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010.
[2] C. E. Perkins and E. M. Royer, “Ad-Hoc On Demand Distance Vector Routing”, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb. 1999.

[3] Jian-Ming Chang, Po-Chun Tsou, Woungang, I., Han-Chieh Chao, Chin Feng Lai, Isaac Woungang and Po-Chun Tsou, “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach”, IEEE Systems Journal, Vol. 9(1), pp. 65-75, 09 January 2014.

[4] Mieso K. Denko, “Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme”, Journal Systemic, Cybernetics and Informatics, Vol. 3(4), pp. 1-9, 2005.

[5] Onkar V. Chandure, V. T. Gaikwad, “A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET”, IJCSIT, Vol. 2, No.6, pp. 2607-2613, Jul 2011.

[6] Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir, “Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation”, ICCIT, Saudi Arebia, March 2012.

[7] Waleed S. Alnumay and Uttam Ghosh, “Secure Routing and Data Transmission in Mobile Ad Hoc Networks”, International Journal of Computer Networks & Communications (IJCNC), Vol. 6, No.1, pp. 111-127, Jan. 2014.

[8] Nidhi Saxena,Vipul Saxena, Neelesh Dubey, Pragya Mishra, “Attack Analysis In Mobile Ad Hoc Network Based On System Observations”, IJARCSSE, Vol. 3, Issue 7, pp. 618-623, July 2013.

[9] Maha Abdelhaq, Sami Serhan,Raed Alsaqour and Anton Satria, “Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol”, Australian Journal of Basic and Applied over AODV MANET Routing Protocol”, Australian Journal of Basic and Applied Sciences, Vol. 5, Issue 10, pp. 1137-1145, 2011.

[10]Sowmya K. S., Rakesh T. and Deepthi P. Hudedagaddi, “Detection and Prevention of Blackhole Attack in MANET Using ACO”, International Journal of Computer Science and Network Security, Vol. 12, Issue 5, pp. 21-24, May 2012.