Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Protecting Packets against Malicious Nodes in Mobile Ad Hoc Network

[1]R.Devi, [2]C.Jayakumar
[1]PG Student, R.M.K Engineering College, Chennai, India
[2]Professor, R.M.K Engineering College, Chennai, India

Abstract: Malicious drops is one of the attack to drop the packets. It affects the transfer of data from source to destination and sends a fake acknowledgement as received. The acknowledgement that is forwarded will reach the source and wait for the response. Till the timeout it waits and start to transmit the packet again. Malicious nodes does not have any intension to drop the packets. We proposed a system to reduce malicious nodes prevailing in the transmission path. To avoid these malicious nodes we also propose on-demand routing protocol and digital signature acknowledgement. After the detection of the malicious nodes packet blocking is implemented and secure routing is done.

Keywords: *Attack Detection, On-Demand Routing Protocol, Digital Signature, Secure Routing.*

I. INTRODUCTION

Mobile ad hoc network is the collection of two or more devices or nodes with wireless communication and networking capacity that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically from a network to exchange information without using any existing fixed network infrastructure [9]. A wireless mobile node can functions both as a router for routing packets from other nodes and as a network host for transmitting and receiving packets. The network consists of peer-to-peer, self-forming and self-healing. The working of ad hoc network is to find a path or route between source node and destination node.

Sometimes, the destination node may not have any path to receive packets. The ad hoc network has to be implemented to find a new path for the packet transmission [10].

The characteristics of an ad hoc network has no background network for the central control of the network operations .The network is distributed among the nodes. These nodes in a network should co-operate each other among themselves. When a node tries to communicate to other nodes which is out of its communication radio range, the packets should be forwarded with one or more intermediate nodes [10]. The nodes in the ad hoc network dynamically establish routing among themselves, establishing their own network. Mobile ad hoc network is more vulnerable to malicious nodes having a chance of dropping the packets. There are several vulnerabilities in dropping the packets as all the drops are intended to denial the service (DOS).

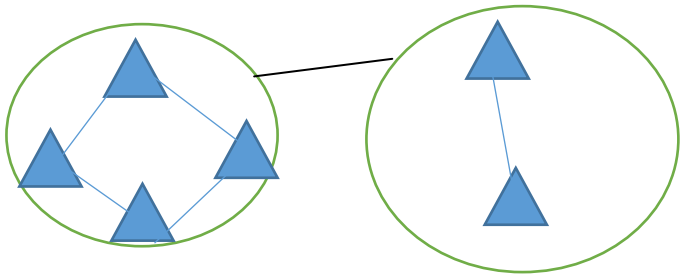


Fig 1 Describes About The Ad Hoc Network Communication.

II. PROBLEM STATEMENT

Selectively detecting packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty lies in the requirement that we need to detect the place where the packet is dropped but also identify whether the hop is intentional or unintentional. The existing system consists of public auditing for storage. However, this is not suitable for application of homomorphic linear authentication (HLA) because there can be more than one malicious node along the route. Public auditing does not reduce the malicious packet drop instead they can provide a valid proof for the dropping of packets.

III. PROPOSED SYSTEM

We have taken this problem in mobile ad hoc network and proposed a method to overcome the problem. To reduce the malicious node invasion we have proposed on-demand multicast routing protocol and digital signatures. The nodes that send the packets are need to be acknowledged to conform that the nodes reach the destination. Acknowledgements is like a token that the packets are sent safely. If there is no response then we use digital signatures and on-demand routing protocol for security purpose. This protocol helps in providing the security against the attackers.

To improve the security in sending the packets we propose a method of, on-demand routing protocol for transmitting the packets. This will reduce the malicious nodes to drop the packets. Simulation results have been demonstrates the effectiveness of proposed scheme with improved performance as compared to the existing protocol and verifications of the packets.

IV. SYSTEM ARCHITECTURE

The system architecture shows the overall design of the modules like packet generation, packet dropping, attack detection, digital signature verification, malicious node identification, packet blocking and secure routing. The nodes describes about the activities undergo in the proposed system.

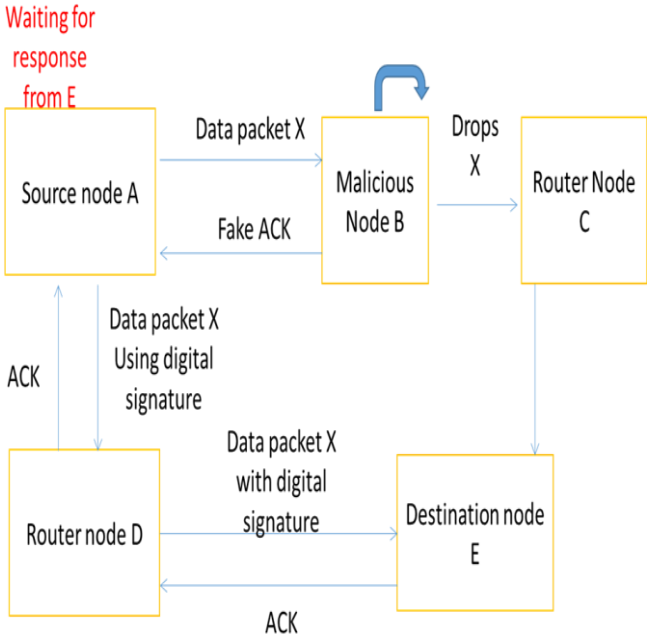


Fig 2: Architecture Diagram

V. MODULE DESCRIPTION

A. Packet Generation

Packets are the files that are to be send from source to destination. A source node has to send these packets through intermediate nodes to reach destination. The intermediate nodes will send the generated packets to the destination node or it will pass to the next nearby node. The source will have a timeout for these packets to be delivered. According to the timeout and delay the packet will be detected as delivered or dropped. If it does not receive the acknowledgement then it proceeds with the verification of where the packets gone.

B. Packet Dropping

Malicious packet drop

On sending a packet it may drop due to a malicious node invasion. It may act like a legitimate node and drop the packets intentionally or to denial the service. Link error is caused due to any internal failure or the failure may occur on any of the link that is connected. Due to the failure of configuration also link errors may occur.

Attack detection

Attack detection is detecting at which stage the attack is done. It may happen at the state where the intermediate nodes pass the packets to the destination nodes. It may occur in two ways.1.Denial of service attack. 2. Suspicious packet drop.

C. Digital Signature Verification

A digital code which is attached to verify its contents and the sender's identity. Digital signatures can be used to certify or to approve documents. Certifying signatures verify the documents creator and show that the document has to been altered since it was signed. Therefore, only the original creator of a document can add a certifying signature. Approved signatures can be added to anyone with a digital id and are used to approve documents, track changes, and accept terms stated with a document. This is applied only for the acknowledgement to verify whether it is from the legitimate node or from a malicious node.

D. Malicious Node Identification

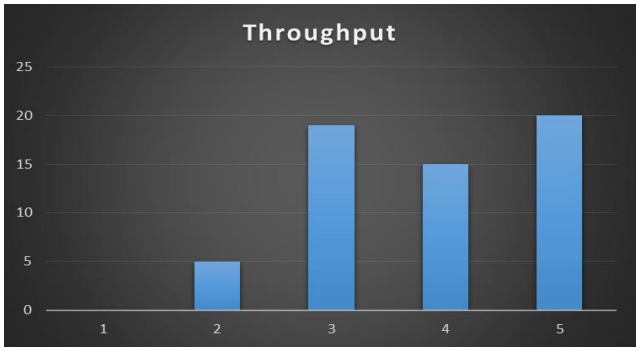
Malicious node identification is that it detects the malicious node that are dropping the packets and causing the disruptions in the network. This can be identified by the activity of blocking the packets that are coming its way. A malicious node will only drop the packets and simply sends the acknowledgement as valid that indicates as a legitimate node. A timer is set for the acknowledgement and the response to the sender by this activity malicious node can be found. Once it is identified, it is blocked from further receiving or sending the packets or acknowledgement.

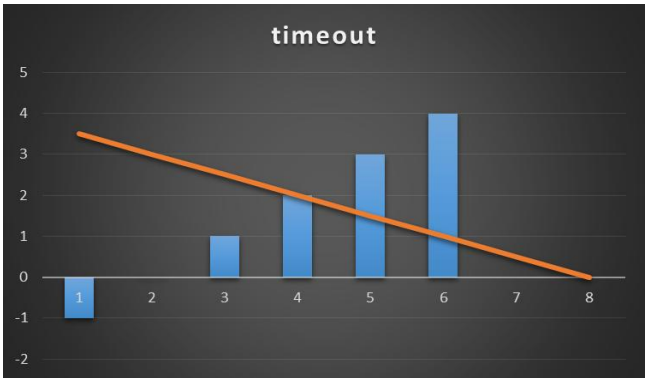
E. Packet Blocking

This is the last stage of the implementation. Packet blocking is done to which the node acts as a malicious node and that node is identified and reported. The reported node will be broadcasts as an infected node and that node will be blocked by sending or receiving any packets furthermore. The blocked node will not be used by any of the nodes for their packets transaction. The malicious node will remain idle for the rest of the time.

F. Secure Routing

For secure routing, we are using an on-demand routing protocol along with the digital signatures to find the malicious nodes that are dropping the packets. Digital signatures are used for secure routing as it ensures the sender and the receiver about the original node. These digital signatures verifies the original sender by generating certificates. On-demand routing protocol helps to determine the malicious node in an efficient way such that the nodes can be identified.





These graphs describes the throughput, timeout and delay to reach the destination from the source.

Throughput

The graph shows that how efficient the packets are delivered successful from source to destination.

Timeout

The graph shows within the time to reach the destination. This may vary but does not change the effectiveness in reaching the destination.

Delay

The graph shows the time delay. The time it had taken to reach the destination form the source.

These graphs may vary according to the files we are sending.

These graphs shows the deviation after there is a malicious attack in the packet transmission.

There will be variation in all the graphs showing that a malicious node has dropped the packets and stopped the transmission of packets temporarily.

CONCLUSION

In this project, protecting packets against malicious nodes is investigated, with the secure routing protocols. The project describes about the problem of compromising nodes and security in mobile ad hoc network. Protecting packets against malicious dropped down because of the existence of malicious nodes. By this protecting of packets, existence of malicious nodes will be reduced and a secure way of routing the packets can be achieved. In future work, it can be implemented with cost effective and can be implemented in other domains.

References

[1] Zhiming Xu, Yu Wang, Jingguo Zhu (2009),"A reliable multicast routing protocol for high speed mobile ad hoc network in R-ODMRP, in IEEE journal of software vol.5,no.1.

[2] Tuan T.Tran, Ganying Ru, Robert J.Kerczewski, Lingjialiu, Samee U.Khan (2013) secure wireless multicast for delay-sensitive data via network coding", on IEEE transaction on wireless communication pp-1536-1276, 2013.

[3] Zhiguo Wan, Kui Ren, And Ming Gu "USOR: An Unobservable Secure On-demand Routing Protocol For Mobile Ad Hoc Network", IEEE Transaction On Wireless Communication., Vol: 11, no.5, pp.1536-1276, may2012.

[4] Trust T. Mapoka , Simon J. Shepherd, Raed A. Abd-alhameed , "Anew Multiple Key Management Scheme For Secure Wireless Mobile Multicast", IEEE Transaction On Mobile Computing, Vol:14, No.8,pp.1536-1233,august 2015.

[5] Amol Bhosle, Yogadhar Pandey ,"Review of authentication and digital signature methods in Mobile ad hoc network" on IEEE conference ISSN: 2278 – 1323 ,vol:2,no.3,march 2013.

[6] Muthumanickam Gunasekaran, Kandhasamy Premdatha, "Teap:truse –Enhanced Anonymous On-demand Routing Protocol For Mobile Adhoc Networks", IET On Information Security Vol:7,issue:3,pp.203-211,on 2013.

[7] Yavuz,A.A , Robert Bosch LLC, " An efficient real-time broadcast authentication scheme for command and control messages", IEEE transaction on information forensics and security, vol:9,no.10 august 2014.

[8] Denh Sy, Rex Chen and Lichun Bao, "ODAR: On-Demand Anonymous Routing in Ad Hoc Networks", on IEEE international Conference on 2012.

[9] Hui Xia, Jia Yu1, Zhi-yong Zhang, Xiang-guo Cheng, Zhen-kuan Pan, "Trust-enhanced multicast routing protocol based on node's behavior Assessment for MANETs", on 13th International Conference on Trust, Security and Privacy in Computing and Communications,2014.

[10] C. Siva Ram Murthy and B. S. Manoj(2006), "Ad hoc Wireless Networks: Architecture and Protocol", First Edition, Pearson Education India.