Efficient Shortest Path Routing Using Rtos In Mobile Ad Hoc Networks

T. Priyadharshini*

PG Scholar

CSE&Bharath University

Ar. Arunachalam

Assistant professor

CSE&Bharath University

Abstract

The performance and reliability of the Internet depend in large part on the operation of the underlying routing protocols. The IP routing protocols compute paths based on the network topology and configuration parameters. Increase the number of the nodes in the wireless computing environment leads to different issues are power, data rate, quality of services and security. The security is the peak issue faced by most of the wireless networks. The networks without having a centralized system (MANETS) are facing severe security issues. The major security issue is the wormhole attack while finding the shortest path. The aim of this paper is to propose an algorithm to find a secure shortest path against wormhole attack. The proposed algorithm is both software and hardware. RTOS is included to make the ad hoc network a real time application.

Key words*:* ***Mobile ad hoc networking, routing, security, wormhole, shortest path, real time operating system (RTOS).***

1. Introduction

Mobile ad hoc networks (MANETS) have a wide range of applications, especially in military Operations, e-commerce and entertainment. Mobile ad hoc networks are self Configuring network sometimes called mesh networks. Different protocols are then evaluated based on packet drop rate, overhead introduced by routing protocol, security etc. The paper security issue faced by the routing protocol is taken into consideration. The routing protocol of mobile ad hoc networks faces different security issues. This paper concentrates on wormhole attack. The effect of wormhole attack created malicious node there by deleting the legitimate path. The secure *routing* protocols against wormhole have been proposed for an efficient routing on a general purpose routing environment. This paper focus on monitoring and isolation through cryptographic methods in a real time operating system *(RTOS)* environment.

Mobile Ad Hoc Networks are wireless networks which do not require any infrastructure support for transferring data packet between two nodes. In these networks nodes also work as a router that is they also route packet for other nodes. Nodes are free to move, independent of each other, topology of such networks keep on changing dynamically which makes routing much difficult. The routing is one of the most concern areas in these networks. The routing protocol works well in fixed networks does not same performance in Mobile Ad Hoc Networks. In these networks routing protocols should be more dynamic that they quickly respond to topological changes.

There is a lot of work done on evaluating performances of various MANET routing protocols for constant bit rate traffic but there is very little work done for variable bit rate traffic. In our paper we have evaluated performances of most widely used MANET routing protocols namely AODV, DSDV, DSR and OLSR using RTOS.

2. Routing Protocol In MANET

Routing is an activity or a function that connects a call from origin to destination in telecommunication networks and also plays an important role in architecture, design and\operation of networks. Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node acts as a router for forwarding and receiving packets to/from other nodes. Routing in ad-hoc networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility.

Routing in general involves two entities, namely the *routing protocol* and the *routing Algorithm*. The routing protocol manages the Dynamics of the routing process: capturing testate of the network and its available network Resources and distributing this information Throughout the network. The routing algorithm uses this information to compute paths that optimize a criterion and obey constraints.

2.1.-**Pro-active routing**:

In this approach, Routes to various destinations are maintained at all times (pre-computed), whether they are required or not. Some of the types of proactive routing protocols are DSDV (Destination sequenced distance vector), WRP (Wireless Routing Protocol).

2.2-Reactive routing:

In this approach, Routes to destinations are computed when they are needed (on-demand). This approach Reduces overhead, at the expense of slower response times. The most popular reactive algorithm is AODV (Ad-hoc On Distance Vector).

3. Secure In Routing Protocol

In ad hoc network, from the point of view of a routing protocol, there are two kinds of messages: the routing messages and the data messages. Data messages are point-to-point and can be protected with any point-to-point security system (IP). On the other hand, routing messages are sent to immediate neighbours, processed, possibly modified, and resent. The result of the processing of the routing message, a node might modify its routing table. This creates the need for the intermediate nodes to be able to authenticate the information contained in the routing messages to be able to apply their import authorization policy.

3.1. Import authorization

It is important to note that in here it is not referring to the traditional meaning of authorization.

3.2. Source authentication

Nodes need to be able to verify that the node is the one it claims to be.

3.3. Integrity

In addition, nodes need to be able to verify that the routing information that it is being sent to us has arrived unaltered.

3.4. Modification

The attack tries to modify the data by doing packet misrouting.

3.5. Fabrication

The deprivation is one of the attacks in mobile ad hoc networks which put the battery in exhaust condition.

3.6. Interruption

An intruder tries to drop packets during forwarding of packets. One more attack is flooding of packets.

3.7. Interception

Block whole attacks and worm whole attacks. Out of these attacks this paper evaluate wormhole Attack scenario.

4. Worm Whole Attack

Wormhole attack is the most severe attacking MANET routing.

Wormhole attack is based attack that can disrupt the routing protocol and disrupt or breakdown a network.

The 4 steps to explain about a general wormhole attack.

1. An attacker has two trusted nodes (or two colluded attackers each has one node) in two different locations of a network with a direct link between the two nodes.

2. The attacker records packets at one location of a network.

3. The attacker then tunnels the recorded packets to a different location.

4. The attacker re-transmits those packets back into the network location from step 1.

5. Related Work

In [2] wormhole scenario is explained. A wormhole is created in the mobile ad-hoc network Which can able to defend against any type of counter measures this attack can create a malicious path even if the attacker has not malpractice the other host that is even if the other hosts path is good. Similarly the attack can happen even if there is a good encryption and decryption is happening.

In [3] surveys the types of complex wormhole attack in wireless Ad-hoc networks. This paper refers attacks like spoofing, eaves dropping and packet leashes. In this paper the wormhole is identified as two phase process launched by one or several malicious nodes, called wormhole nodes. The wormhole attack mode and classes, and point to its impact and threat on ad hoc networks.

In [4] the wormhole attack is detected using the topology changes. The algorithm is independent on wireless communication models. The proposed algorithm detects the wormhole by using the information collected in the upper layer like routing layer. The detection algorithm looks for forbidden structures which are not present in the legal connectivity.

In [5] introduces a light weight countermeasure for mobile ad-hoc networks. This algorithm listens to the neighbour node. In this algorithm every malicious node is detected and isolated and it's specially concentrates on resource constraints.

In [6] examines the wormhole attack in WAHAS (Wireless Ad-Hoc and Sensor networks).
This paper introduces a protocol called SECOS which provides a secure route between any two nodes despite of compromise of any number of other node.
.

In [7] proposed an efficient algorithm called (Wormhole attack prevention algorithm) WAP.
This algorithm avoids the use of specialized hardware.
.

In [8] runs the AODV in a secure way. The AODV is made to run against wormhole attack.

A mechanism called Wormhole Attack Detection Reaction (WADR) is made to run with Conventional AODV.
.

6. RTOS (real time operating system)

The routing algorithm is made to run on a geographical area of few kilo meters. The area is small the nodes assumed to be less. A wormhole scenario will be created. The malicious activity created by the wormhole attack. The real time environment using a real time Operating system.

7. Expected Result

The proposed RTOS based security algorithm to implement in a MATLAB. To finding the shortest path from source to destination nodes for optimal routing in mobile ad hoc networks.

8. Conclusion

This work presents a routing protocol for mobile ad hoc network using RTOS based security algorithm. The proposed techniques for RTOS to find the optimal path from source and destination nodes. The process of to finding shortest path in optimal routing in MANET. We simulate our routing protocol using MATLAB and obtain the result that shows the optimal routing path.

9. ACKNOWLEDGMENT

The authors would like to thank the management of Bharath University for their support and the department of Computer Science and Engineering for their encouragement towards a research work.

10. References

[1] Dr.R. Ramesh, Ms.S. Gayathri "RTOS Based Secure Shortest Path Routing Algorithm In Mobile Ad- Hoc Networks" Department of Electrical and Electronics Engineering, Anna University, India, Vol.3, No.4, July 2011.

[2] Yih-Chun Hu, Adrian Perrig, Member, & David B. Johnson, (2006) "Wormhole Attacks in Wireless Networks" IEEE *Journal on selected areas in Communications*, Vol. 24, No. 2.

[3] Mohit Jain &Himanshu Kandwal, (2009)"A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks". *International Conference on Advances in Computing, Control, and Telecommunication Technologies.*

[4] Ritesh Maheshwari, Jie Gao & Samir R Das," Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information".http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04068262.

[5] Issa Khalil, Saurabh Bagchi& Ness B. Shroff,(2007) "LITEWORP: Detection and Isolation of the Worm whole Attack in Static Multihop Wireless Networks". *The International Journal of Computer and Telecommunications Networking*, Vol. 51, Issue 13, pp 3750- 3772.

[6] Issah Khalil,(2008)"Mitigation of Control and data traffic attacks in wireless ad-hoc and sensor networks" IEEE Vol. 6, Issue 3, pp 344-362.

[7] Sun Choi, Doo-young Kim, Do-hyeon Lee &Jae-il Jung(2008) **"**WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" IEEE *International* Conference on Sensor Networks, *Ubiquitous, and Trustworthy Computing SUTC'08*. pp 343- 348

[8] Emmanuel A. Panaousis, Levon Nazaryan & Christos Politis (2009) "Securing AODV Against Wormhole Attacks in MANET" *Proceedings of the 5th International ICST Mobile Multimedia Communications Conference***,** Article 34.

[9] Manel Guerrero Zapata, "Securing and Enhancing Routing Protocols for Mobile Ad hoc Networks".

[10] Issa Khalil, Saurabh Bagchi & Ness B. Shroff, "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks". http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4198824.