International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 7, July 2014

Design an Efficient Security Protocol for Wireless Networks

K. Stalin[1], S. Thirumal[2]

[1]M.Phil research Scholar A. A. A. Govt .Arts College, Cheyyar, T. V. Malai Dt, India.

[2]Assistant Professor & Head, of Computer Science, A.A.A govt. Arts College, Cheyyar, T. V. Malai Dt, India.

Abstract: ***Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes which dynamically forms a temporary network without the use of any existing network infrastructure or centralized administration. The security in MANETs has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. In this paper, we present the Secure Message Transmission (SMT) protocol, which safeguards the data transmission against arbitrary malicious behavior of other nodes in multipath environment. The basic idea is to transform a secret message into categories of information in multiple paths. In our study, we have found that necessity of multipath along with secure routing protocol is mandatory when the path get disconnected. We present the overall system architecture and algorithm for message dispersion and message transmission. We also consider the routing stability in MANET because its environment is more selfish. So we extended the data dispersion along with Multipath Optimized Link State routing protocol. Our simulation study shows that this approach is useful as it enhances the security in multipath routing.***

Keywords: MANET, Security, Multipath, MP-OLSR, Secure message transmission

1. Introduction

"A mobile ad hoc network" (MANET) is an autonomous system of mobile routers where it provides optimal security but with the price of too much computation and transmission cost as well as time delay. Since all the nodes in Ad hoc network collaborate to forward the data, the wireless channel is prone to various types of attacks [1]. Therefore implementing security is of prime importance in such networks. The ultimate goal of the security solutions for MANETS is to provide security services such as authentication, confidentiality, integrity, anonymity, and availability to mobile users. Multi-path routing protocols need to be properly enhanced with cryptographic means which will guarantee the integrity of a routing path and the authenticity of the participating nodes. The nodes in MANET depend on one another for transmitting the packets from source to destination node via the routing nodes. Based on route discovery routing protocols fall into three categories. a) Proactive or Table Driven routing protocol which gives complete picture of the network and in maintained at every node, b) Reactive or On Demand routing protocol as the name suggest on demand it finds a route to destination when there is a need to send data, and c) Hybrid routing protocol which use the mix of both proactive and reactive routing protocol. The rest of the paper is organized as follows. Section 2 describes works related to multipath and security issues and challenges in MANET. Section 3 discusses the architecture of the secured multipath system. Section4 describes the simulation setup; Section 5 compares the performance evaluation of the protocols with and without security, finally the conclusion.

2. Literature Survey and Related Works

In the last few years, researchers have actively explored many mechanisms for enhancing the security in multipath network. Multipath routing allows use of multiple paths between from source to destination. There are three elements to multipath routing, namely path discovery, traffic distribution, and path maintenance. The multipath used can be non-disjoint, link-disjoint or node -disjoint. Performance of MANETs depends on the routing protocol scheme employed. Traditional routing protocols do not work efficiently in MANETs due to its dynamic nature. A lot of multipath routing protocols have been proposed for MANET where many of them are based on the famous distance vector routing and link state routing protocol [2]. Most of the multipath routing protocols like AOMDV, MP-OLSR and MP-DSR are the extension of unipath protocols like AODV, OLSR and DSR. The unique characteristics of MANET poses number of nontrivial challenges to security design such as shared wireless medium and highly dynamic network topology. The ultimate goal of the security solutions for MANET is to provide security services such as authentication, confidentiality, integrity, anonymity and availability to mobile user. There are many proposed security protocols for both single path and multipath. There are several types of attacks have been mounted on the routing protocol which are mainly aimed at disrupting the operation of the network. Various attacks on the routing protocol may be either an active attack or passive attack. We can categories MANET security in 5 layer such as application layer, transport layer, network layer, link layer and physical layer. However, we only focus on the network layer which is related to security issues to protect the ad-hoc routing and data forwarding. Some of the attacks like Wormhole, Black hole and Byzantine attack involved in network layer.

3. Proposed Secured Multipath System Architecture

In our Proposed system, the Multipath Routing Protocols (MRP) are used to find and maintain routes between source and destination nodes and also allow the establishment of multiple paths between a single source and single destination node. (i) The routing protocol provides multiple, loop-free,

and preferably node-disjoint paths to destinations, (ii) the multiple paths are used simultaneously for data transport and (iii) multiple routes need to be known at the source. The existence of multiple paths between end-nodes to statistically enhance data confidentiality and data availability [3]. Due to the absence of infrastructure and consequent absence of authorization these networks are vulnerable to diverse types of attacks where routing is a critical operation. The Secure Multipath Routing Protocol (SMRP), the essential issue is to protect our transmitted message from adversaries and attacks. The security of the route discovery is a prerequisite for secure communication in the self-organizing, open ad hoc networking environment. Our Secure Multipath Routing Protocol addresses exactly this problem. SMP discovers one or more correct routes across an unknown, frequently changing network, in the presence of adversaries. It guarantees the acquisition of correct topological information in a timely manner, i.e. route replies that are validated and accepted by the node provide accurate connectivity information despite the presence of attack.

Some of the authors have suggested that there is no security issues relate with routing protocol. More over there are some security flaws present in the OLSR. So in order to overcome that we have consider multipath routing protocol which is an extension of single path OLSR. The MP-OLSR can be regarded as a kind of hybrid multipath routing protocol which combines the proactive and reactive features as it extended from OLSR [4]. MP-OLSR act as Reactive Routing, also called on-demand routing, a node only tries to find a route when necessary sometimes which may leads to longer delay. MP-OLSR act as the proactive routing protocols also called table driven routing, each node maintains a routing table containing routes to all nodes in the network. Nodes must periodically exchange messages with routing information to keep routing tables up-to-date. Information proactively and compute the routes on-demand. It sends out HELLO and TC messages periodically to detect the network topology, just like OLSR and does not always keep a routing table. It only computes the multiple routes when data packets need to be sent out.

The main function of the Multipath Optimized Link State Routing Protocol is (i) Topology Sensing and (ii) routing computation .Topology Sensing is to find to make the nodes aware of the topology information of the network using Multipoint Relay Set (MPR) like OLSR. Through topology sensing, each node in the network can get sufficient information of the topology to enable routing. The link stat protocol tries to keep the link information of the whole network [5]. The route computation uses the Multipath Dijkstra Algorithm to calculate the shortest multipath based on the information obtained from the topology sensing. The routes are determined by nodes each time they receive a new Topology Control message (TC or HELLO). The routes to all possible destinations are saved in the routing table. The situation will be much more complicated due to the change of the topology and the instability of the wireless medium. So route recovery and loop detection are also proposed as auxiliary functionalities to improve the performance of the protocol.

Fan Hong, Liang Hong, Cai Fu have suggest some of the flaws present in OLSR [6]. In which OLSR don‟t protect the routing packets in network so attacker can easily modify the data and won‟t be able detected. Once an attacker become his MPR node then the attacker can create a black hole which drops all packet selectively or temper the packet contents and then relay it. In our proposed system we have introduced black hole attacks in which malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack leads to packet drop while sending the message from source to destination. In order to over that (SMT) protocol which encodes the message while forwarding the packets and decodes in the destination node.

The goal of the Secure Message Transmission Protocol (SMT) is to safeguards pair wise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior. It combines four elements: end-to-end secure and robust feedback mechanism, dispersion of the transmitted data, simultaneous usage of multiple paths, and adaptation to the network changing conditions. SMT detects and tolerates compromised transmissions, while adapting its operation to provide secure data forwarding with low delays. A different approach is taken by the Secure Message Transmission (SMT) [7, 8] protocol, which, given a topology view of the network, determines a set of diverse paths connecting the source and the destination nodes. Then, it introduces limited transmission redundancy across the paths, by dispersing a message into N pieces, so that successful reception of any M-out-of-N pieces allows the reconstruction of the original message at the destination. Each piece, equipped with a cryptographic header that provides integrity and replay protection along with origin authentication and is transmitted over one of the paths. Upon reception of a number of pieces, the destination generates an acknowledgement informing the source of which pieces, and thus routes, were intact. If less than M pieces were received, the source re-transmits the remaining pieces over the intact routes. If too few pieces were acknowledged or too many messages remain outstanding, the protocol adapts its operation, by determining a different path set, re-encoding undelivered messages and re-allocating pieces over the path set. Otherwise, it proceeds with subsequent message transmissions.

We have integrated secure multipath routing and secure data transmission protocols and showed how to achieve highly reliable and low-delay attack we used secure message transmission communication in a hostile networking environment.

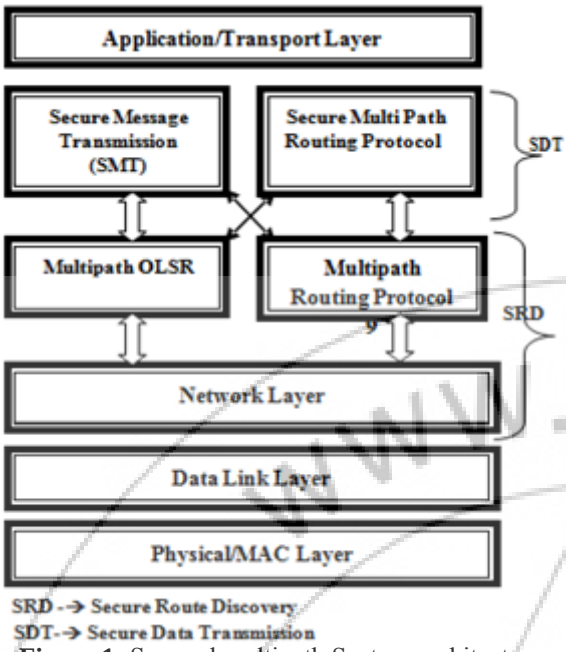

Figure 1: Secured multipath System architecture

The figure below shows the work flow model of our proposed system.

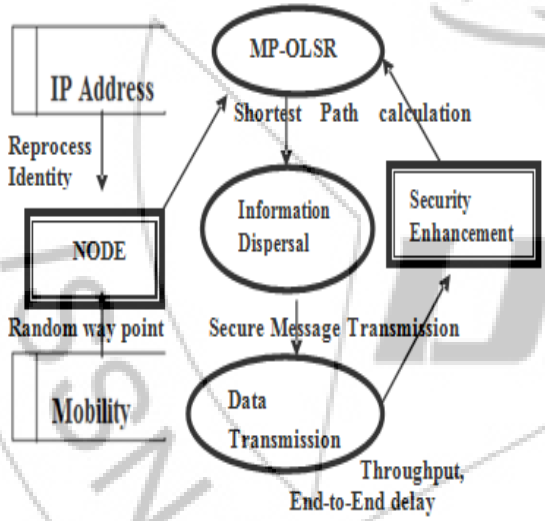

Figure 2

4. Simulation Setup

The evaluation is carried out with the Network simulator (NS-2) by performing several experiments that illustrate the performance of the system. The simulation parameters like number of nodes, terrain range etc. as given in table 1 along with their respective values are used to examine the performance of the network. The values can be adjusted according to requirements in this file.

Table 1: Simulation Parameters

Parameter	*Value*	*Description*
Simulator	NS2	Simulator Tool
Simulation time	300	Maximum execution time
Terrain Dimensions	500 X 500	Physical area in which the nodes are placed in meters
Number of Nodes	25	Nodes participating in the network
Traffic Model	CBR	Constant Bit Rate link used
Node Placement	Uniform	Node placement policy
Mobility	0-10(m/s)	Speed of node
Performance Parameter	Through put, End to End delay, Packet ratio, Speed	Parameter consider in evaluating
Routing Protocol	MP-OLSR	Routing protocol used

5. Performance Analysis

We compare the performance of MP-OLSR and Secure MP-OLSR according to the following performance metrics. In the below figure we have shown system model where the nodes send data from one node to other node.

***A)* Packet Delivery Ratio (PDR):**

Packet Delivery Ratio (PDR) is number of successfully delivered legitimate packets to number of generated legitimate packets. A higher value of PDR indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance.

PDR=Total number of packets received (TPR)/Total number of packets sent (TPS)

As we can see from the result, during the attack, the target node in OLSR can hardly receive data packets. Our approach can achieve much higher packet delivery ratio. From these experiments, itis easy to see that in the secured OLSR protocol, attackers can easily prevent a target node from receiving data packets from other nodes and it also indicates that our approach can provide effective protection against the malicious attack.

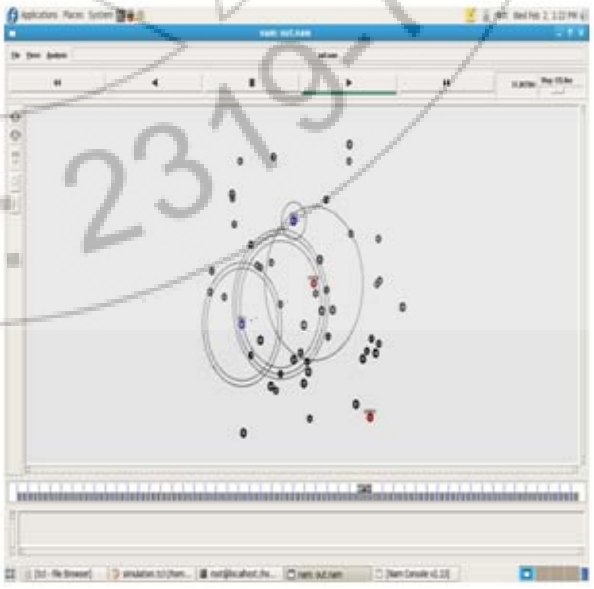

Figure 3: System model

B) **Average End-to-end delay (AED):**

End-to-end delay indicates how long it took for a packet to travel from the CBR source to the application layer of the destination. It represents the average data delay an application or a user experiences when transmitting data.

AED = Total Delay (TD) / PacketReceived (PR)

From the figure 2 we can say that average end to end delay is more or less same in the both MP-OLSR and secured MP-OLSR because before while sending the data, it has to be encrypted and has been sent in multiple paths.

C) Package Dropping Rate:

It shows the number of data packets which were dropped during their journey to destination. From the figure 3, we can say that the packet drop is less because the data can be reconstructed from the redundancy even thought small amount of packet loss occurs.

D) Node Mobility:

Node mobility indicates the mobility speed of nodes.

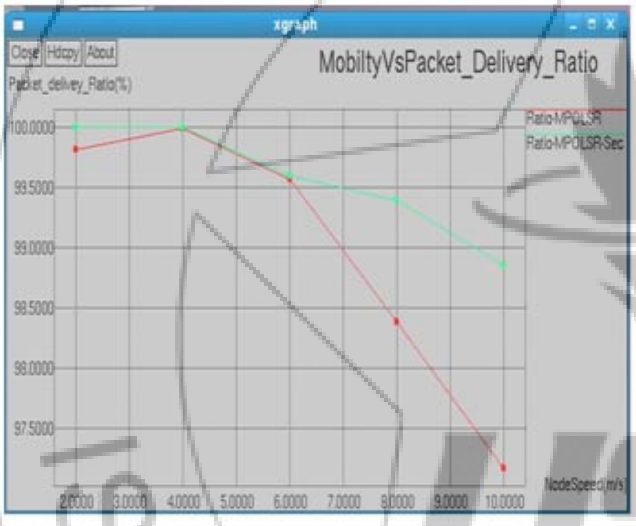

Figure 4: Speed Vs Packet Delivery Ratio

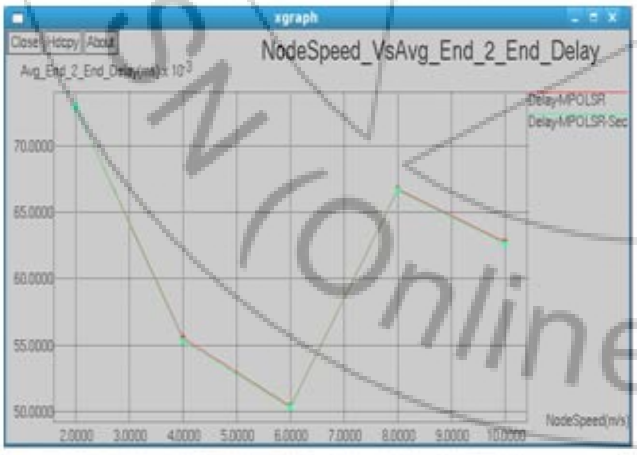

Figure 5: Speed Vs Average End to End delay

Figure 7: Speed Vs Packet Drop

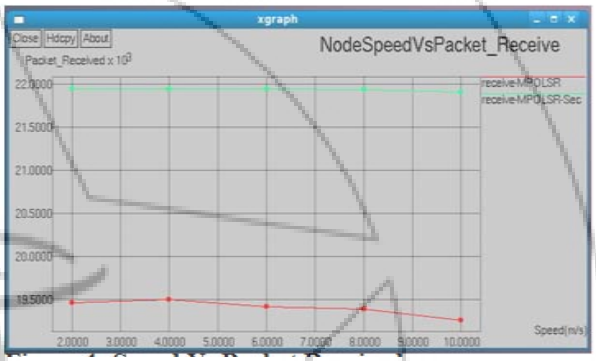

Figure 8: Speed Vs Packet Received

6. Conclusion

In this paper, we have presented a Secured Multi Path OLSR along with secured message transmission in multipath. Our approach is based on enhancing the security while sending the data from source to destination in multiple paths. Comparison was based on of packet delivery ratio, routing overhead incurred, average end-to-end delay and number of packets dropped, we conclude that Secured Multi Path OLSR performs better than the normal MP-OLSR even when the attacks have been introduced.

References

[1] Rashid Sheikhl Mahakal Singh Chandee, Durgesh Kumar Mishra," Security Issues in MANET: A Review", 2010

[2] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges", Lecture Notes in Computer Science, Volume 2965, April 2004, Pages. 209 – 234.

[3] Li Zhao and José G. Delgado- Frias,"Multipath Routing Based Secure Data Transmission in Ad Hoc Networks"

[4] Jiazi YI, Asmaa ADNANE, Sylvain DAVID, Benoˆıt PARREIN ,"Multipath Optimized Link State Routing for Mobile ad hoc Networks", hal- 00521710, version 1 - 28 Sep 2010.

[5] J. Yi, E. Cizeron, S. Hamma, B. Parrein, and "Simulation and performance analysis of MP- OLSR for mobile ad hoc networks", in: IEEE WCNC: Wireless Communications and Networking Conference, Las

Vegas, USA, 2008.
[6] Fan Hong, Liang Hong, Cai Fu," Secure OLSR", Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA"05), 2005
[7] Panagiotis Papadimitratos and Zygmunt J. Haas,"Secure Data Transmission in Mobile Ad Hoc Networks", WiSe"03, San Diego, California, USA, September 19, 2003
[8] M.O. Rabin, "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance," Journal of ACM, Vol. 36, No. 2, pp. 335-348, Apr. 1989
[9] L. Zhao and J. Delgado-Frias, "Multipath Routing Based Secure Data Transmission in Ad Hoc Networks", Proceedings of WiMob, 2006
[10] W. Lou, W. Liu and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks", Proc. IEEE INFOCOM 2004, Volume 4,7-11 pp. 2404 – 2413, Hong Kong, China, March 2004.