Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.586 – 597

RESEARCH ARTICLE

SECURE MESSAGE TRANSMISSION AGAINST ARBITRARY MALICIOUS NODES IN MULTIPATH ATMOSPHERE

PriyaDharshini. R[1], Rajeshsingh. S[2], Muruganandam. A[3]

[1]Research Scholar, Don Bosco College, Dharmapuri, TamilNadu, India

[2]Assistant Professor, PG and Research Department of Computer Science, Don Bosco College, Dharmapuri, TamilNadu, India

[3]Assistant Professor, PG and Research Department of Computer Science, Don Bosco College, Dharmapuri, TamilNadu, India

priyaravip@yahoo.com, rajessing@rediffmail.com, murugan.andam@yahoo.co.in

Abstract: 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 goal of Secure Message Transmission (SMT) is to discover routes in ad hoc network and to ensure secure data forwarding, after the discovery of routes between the source and the destination and although such discovered routes may not be free of malicious nodes. It exploits the redundancy of multipath routing and adapts its operation to remain efficient and effective even in highly adverse environments. The basic idea is to transform a secret message into categories of information in multiple paths. The message and the redundancy are divided into a number of pieces, so that even a partial reception can lead to the successful reconstruction of the message at the receiver. We present the overall system architecture and algorithm for message dispersion and message transmission. We also consider the routing stability in Mobile Ad-hoc Network (MANET) because its environment is more selfish. So we extended the data dispersion along with Multipath Optimized Link State Routing Protocol (MOLSRP). Our simulation study shows that this approach is useful as it enhances the security in multipath routing.

Keywords: Secure Message Transmission, MANET, MP-OLSR

INTRODUCTION

1.1 Mobile Ad Hoc Network

"Mobile Ad Hoc Network" (MANETs) is a kind of Wireless Ad hoc Network that usually has a routable networking environment on top of a Link Layer Ad hoc Network. Mobile Ad hoc Network (MANET) refers to a form of infrastructure less network connecting mobile devices with wireless communication capability. Each node behaves as a router as well as an end host, so that the connection between any two nodes is a multi-hop path supported by other nodes. Mobile Ad Hoc Network (MANET) represents a system of wireless mobile nodes that can freely and dynamically self-organize in to arbitrary and temporary network topologies, allowing people and devices to communicate without any pre-existing communication architecture. Each node in the network also acts as a router, forwarding data packets for other nodes. They communicate directly with devices inside their radio range in a peer-to-peer nature. If they wish to communicate with a device outside their range, they can use an intermediate device or devices within their radio range to relay or forward communications to the device outside their range. An ad hoc network is self-organizing and adaptive Mobile Ad Hoc Network (MANET) is an autonomous system of mobile routers (and

associated hosts) connected by wireless links-the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Mobile Ad Hoc Network (MANET) exhibits some of the properties like:

Autonomous and infrastructure less….

- Multi-hop routing
- Dynamic network topology
- Variation on link and node capabilities
- Energy-constrained operation
- Network scalability

For providing secure communication in Wireless Ad Hoc Network; there are two ways:

1. Using the multiple paths available in between the two nodes.
2. Using the cryptographic methods to secure the communication in between two nodes.

In first approach all the multiple paths between two nodes need to be node disjoint. Multipath routing allows building and use of multiple paths for routing between a source-destination pair. Multipath routing can provide a range of benefits like bandwidth aggregation, minimizing end-to-end delay, increasing fault-tolerance, enhancing reliability, load balancing, and so on. This approach is cost effective as it does not include any computation or transmission overhead and hardly inject delay in the network. But it does not ensure a certain level of security as there are not always multiple paths between two end nodes.

The second approach is security consideration 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 the ad hoc network collaborate to forward the data, the wireless channel is prone to various types of attacks. Therefore implementing security is of prime importance in such networks. The ultimate goal of the security solutions for Mobile Ad Hoc Network (MANET) 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. Mobile Ad Hoc Network (MANET) often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism[1].

1.1.1 Characteristics

The general issues of MANETs, will be discussed:

- Dynamic Configuration: Since MANET nodes move randomly in the network, the topology of MANET changes frequently, leading to regular route changes, network partitions, and possibly packet losses.
- Autonomous and infrastructure less: Mobile Ad Hoc Network (MANET) is self-organized and independent of any established infrastructure and centralized network administration. Each node runs as a router and operates in distributed manner.
- Network scalability: Many Mobile Ad Hoc Network (MANET) applications may involve large networks with tens of thousands of nodes especially that can be found in tactical networks. Scalability is crucial to the successful deployment of Mobile Ad Hoc Network.

1.1.2 Applications of Mobile Ad Hoc Network

Ad hoc networks have several interesting applications ranging from battlefield to class rooms. In this section, some scenarios of deployment are discussed.

- Battlefield: In a battlefield, communication between soldiers and vehicles can be carried out using ad hoc networks. In such networks, the soldier troops might communicate with each other using hand-held devices. The vehicle mounted devices can be equipped with power sources for "recharging" these mobile devices.
- Rescue Operation: In scenarios such as fire fighting or avalanche rescue operations, a quick deployment of nodes is required. Ad hoc networks can be used in such scenarios for communication between the workers.
- Event Coverage: Scenarios such as a press conference might entail reporters to share data amongst other reporters. In such cases, multimedia traffic might be exchanged between nodes such as laptops, PDAs, etc.

1.2 Wireless Sensor Networks

Sensor networks can contain hundreds or thousands of sensing nodes. It is desirable to make these nodes as cheap and energy- efficient as possible and rely on their large numbers to obtain high quality results[2]. Network protocols must be designed to achieve fault tolerance in the presence of individual node failure while minimizing energy consumption. In addition, since the limited wireless channel bandwidth must be shared among all the sensors in the network, routing protocols for these networks should be able to perform local collaboration to reduce bandwidth requirements. Communication between the sensor nodes and the base station is expensive, and there are no "high energy" nodes through which communication can proceed[3].

1.2.1 Characteristics of Sensor Networks

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use broadcast communication paradigm
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

1.2.2 Application of sensor network

- Military applications
- Environmental applications
- Health applications
- Home applications
- Industrial applications

1.3 Routing Objectives

Sensor network applications only require the successful delivery of messages between a source and a destination. However, there are applications that need even more assurance. These are the real-time requirements of the message delivery, and in parallel, the maximization of network lifetime.

- **Non-real time delivery:** The assurance of message delivery is indispensable for all routing protocols. It means that the protocol should always find the route between the communicating nodes, if it really exists. This correctness property can be proven in a formal way, while the average-case performance can be evaluated by measuring the message delivery ratio.

- **Real-time delivery:** Some applications require that a message must be delivered within a specified time, otherwise the message becomes useless or its information content is decreasing after the time bound. Therefore, the main objective of these protocols is to completely control the network delay. The average-case performance of these protocols can be evaluated by measuring the message delivery ratio with time constraints.

- **Network lifetime:** This protocol objective is crucial for those networks, where the application must run on sensor nodes as long as possible. The protocols aiming this concern try to balance the energy consumption equally among nodes considering their residual energy levels. However, the metric used to determine the network lifetime is also application dependent. Most protocols assume that every node is equally important and they use the time until the first node dies as a metric, or the average energy consumption of the nodes as another metric. If nodes are not equally important, then the time until the last or high- priority nodes die can be a reasonable metric.

1.4 Problem Statement

Security in Mobile Ad hoc Networks (MANETs) is a major issue. The data is delivered from source to the destination in a proper way without putting additional burden on the network. Sensitive information, such as related to defense, intelligence, transmitted across a hostile MANET needs to be protected from both active and passive attacks. More over in Ad hoc networks are typically subjected to two different levels of attacks. In the first level of attack, the adversary focuses on disrupting the basic mechanisms of the ad hoc network, such as routing, which are essential for proper network operation, and in the second level of attacks, the adversary tries to damage the security mechanisms employed by the network. By attacking the routing, attacker could affect the performance of the network by altering the topological information in the route packet. There are various reasons behind such attacks. The use of multiple paths between a source and destination can facilitate load balancing, fault tolerance, higher aggregate bandwidth, and enhanced data security. Based on these observations, this work contends that the use of directional transmission and intelligent multipath routing is necessary to take full advantage of the proposed multipath routing schemes with respect to data security.

1.5 Motivation

The aim of this paper is how data can be forward in a secured manner from one node to another node without being attacked or modified by the intruders in multipath environment. The communication in mobile ad hoc networks comprises two phases, the route discovery and the data transmission. In an adverse situation both phases are vulnerable to a variety of attacks.

1.6 Objective

The various tasks carried out in achieving the objective can be outlined as follows:

- The study focus on the secure transmission on message between the nodes.
- Implementing SMT protocol along with routing protocol Multipath OLSR on 25 mobile nodes by the use of OTCL script in NS-2.
- Simulating the black hole attack using routing protocol.
- Analyzing the behavior of Multipath protocol with and without enhancing the security with the help of X graph in NS2 simulator.

RELATED WORKS

Since Mobile Adhoc Network changes their topology frequently, routing in such network is a challenging task. Generally, the main function of routing in a network is to detect and maintain the optimal route to send data packets between source and destination via intermediate nodes.

- Multipath Routing
- Multipath Based secure data Transmission

- Multipath optimized link state Routing protocol
- Routing attack in Mobile ad hoc network

2.1 Multipath Routing

Multipath routing allows the establishment of multiple paths between a single source and single destination node. It is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance) or to provide load balancing [2]. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Routing is a process of exchanging information from one station to other stations of the network. Routing protocols of mobile ad-hoc network tend to need different approaches from existing Internet protocols because of dynamic topology, mobile host, distributed environment, less bandwidth, less battery power. Multipath routing consists of three components:

- Route discovery
- Route maintenance and
- Traffic allocation

Multipath as some of its benefits like; Fault tolerance, Load balancing, Bandwidth aggregation, reduced delay this results in a route discovery delay. The delay is minimized in multipath routing because backup routes are identified during route discovery. A lot of multipath routing protocols have been proposed for MANET where many of them are based on the famous distance vector and link state routing protocol. Most of the multipath routing protocols like AOMDV, MP-OLSR, and MP-DSR are the extension of unipath protocols like AODV, OLSR, and DSR.

2.2 Multipath Routing Based Secure Data Transmission

Recently, several studies have been conducted on providing protection on data transmission by using multiple node disjoint paths between the source and the destination. The Secure Message Transmission (SMT) protocol[3,5] which fights against malicious behavior of intermediate nodes on data transmission in the network. Much like the SPREAD scheme, SMT uses multipath routing to statistically enhance the confidentiality and availability of exchanged messages between the source and destination nodes. SMT provides an explicit end-to-end secure and robust feedback mechanism that allows for fast reconfiguration of the path-set in case of node failure or compromise. SMT uses these ratings in conjunction with a multipath routing algorithm to determine and maintain a maximally secure path-set and adjust its parameters to remain efficient and effective. In fact, SMT can successfully deliver more than twice the number of packets that can be delivered by a protocol employing secure route discovery but no secure data forwarding.

2.3 Multipath Optimized Link State Routing

Multipath Optimized Link State Routing protocol (MPOLSR) presented in[6] which was thoroughly revisited and upgraded. First, a major modification of Dijkstra algorithm allows for multiple paths both for sparse and dense topology. Two cost functions are used to generate node-disjoint or link-disjoint paths. Second, the OLSR proactive behavior is changed for an on-demand computation. MPOLSR becomes a source routing protocol. Third, to support the frequent topology changes of the network, auxiliary functions, i.e. ***route recovery*** and ***loop check,*** are implemented. The cooperation between the two protocols is expected here to facilitate the application and deployment of the new protocol. The MP-OLSR can be regarded as a kind of hybrid multipath routing protocol which combines the proactive and reactive features. 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. Hence, MP-OLSR is to get the topology 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 core functionality of MP-OLSR has two parts:

***Topology sensing* and**

***Route computation*.**

2.4 Routing Attacks on Mobile Ad hoc Network

We evaluate the security flaws in OLSR and attacks related with that in the network layer. Any attack in routing phase may disrupt the overall communication and the entire network[7]. Thus the security in network layer plays an important role. The main target is to provide secure communication and remove flaws in existing protocols. Network layer vulnerability fall into two categories:

- Routing attacks and
- Packet forwarding attacks.

The specific attacks behaves are related to the routing protocol used by the MANET. Some of the attacks like Wormhole, Black hole, Flooding, Byzantine, Resource Consumption comes under network layer. The black hole attack is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as OLSR, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets. In second step, the attacker consumes the packets and never forwards. In an advanced form, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. OLSR is proactive routing protocol that is also known as table driven protocol by the fact that it updates its routing tables. OLSR has also three types of control messages which are describe below.

- Hello
- Topology Control (TC)
- Multi Point Relaying (MPR)

Since OLSR has no security mechanisms, malicious nodes can perform many attacks by these ways as follows:

1. There is no security mechanism for a good node to distinguish an attacker from his neighbors, once an attacker becomes his MPR node, then the attacker can create a black hole which drops all packets from or to the selector, or just drops the packets selectively, or temper the packet contents and then relay it. All of those behaves can cause the good node cannot work normally;
2. An attacker can generate lots of false Topology Control Message to broadcast. Because there is no source authentication, other nodes will accept it and update the global topology information.
3. OLSR doesn't protect the routing packets in networks, so an attacker can easily modify them and won't be detected.

OVERVIEW OF THE PROPOSED SCHEME

We have developed a protocol suite to secure message transmission in mobile ad hoc networks. We propose a complete security solution at the network layer, with building blocks selected among:

(a) The Multipath Routing Protocol (MRP), and the Multipath Optimized Link State Protocol (MP-OLSR) to secure the discovery of routes, and

(b) The Secure Message Transmission (SMT) protocol and the Secure Multi Path (SMP) protocol to secure data transmission.

As a derivate of the classical link-state algorithm, OLSR maintains state by keeping a variety of databases of information. These information repositories are updated upon processing received control

messages and the information stored is used when generating such messages. Here follows a brief look at the different information repositories used in core OLSR. The information repositories in OLSR and their relations to message processing, message generation and route calculation. Received HELLO messages trigger updates in the link set which again triggers updates in the neighbor set, which then again triggers recalculation of the MPR set. The 2 hop neighbor set is also updated based on received HELLO messages again triggering a recalculation of the MPR set. Finally the MPR selector set is updated according to information received in HELLO messages. Received TC messages triggers updates in the topology set while the MID set is updated upon receiving MID messages. All received messages will also be registered in the duplicate set if not already registered. When generating HELLO messages, the link set, neighbor set and MPR set is queried. When generating TC messages, the MPR selector set is queried. When forwarding control traffic, the MPR selector set and the duplicate set is used. Finally, route calculation is based on information retrieved from the neighbor set, the 2 hop neighbor set, the TC set and the MID set.

Multiple interface association information Base contains information about node using more than one communication interface. All interface addresses of such nodes are stored here. Link Set repository is maintained to calculate the state of links to neighbors. This is the only database that operates on non-main-addresses as it works on specific interface-to-interface links. Neighbor Set registered one-hop neighbors are recorded here. The data is dynamically updated based on information in the link set. Both symmetric and asymmetric neighbors are registered. 2-hop Neighbor Set contains all nodes, not including the local node that can be reached via a one-hop neighbor is registered here. Notice that the two hop neighbor set can contain nodes registered in the neighbor set as well. MPR set contains all MPRs selected by the local node is registered in this repository. MPR Selector Set contains all neighbors that have selected this node as a MPR are recorded in this repository. Topology Information Base repository contains information of all link-state information received from nodes in the OLSR routing domain. Duplicate set contains information about recently processed and forwarded messages. MID contains Multiple Interface Declaration messages are transmitted by nodes running OLSR on more than one interface. These messages list all IP addresses used by a node.

3.1 Introduction of Problem and its Related Concepts

Standard routing protocols in ad hoc wireless networks, such as AODV and OLSR, are mainly intended to discover a single route between a source and destination node. Multipath routing consists of finding multiple routes between a source and destination node which results in larger routing tables at intermediate nodes and packet reordering. In unipath routing, traffic allocation is not an issue, since only one route is used. The main disadvantage of OLSR is don't protect the routing packets in networks, so an attacker can easily modify them and won't be detected, and an attacker can generate lots of false Topology Control Message to broadcast because there is no source authentication, other nodes will accept it and update the global topology information. The communication in mobile ad hoc networks comprises two phases, the route discovery and the data transmission. In an adverse environment, both phases are vulnerable to a variety of attacks. In the current system for secure message transmission SMT Protocol uses Rabin proposed the Information Dispersal algorithm to facilitate data redundancy. This algorithm was proposed to improve the reliability of communication networks and disk storage systems in the presence of failures. The amount of redundancy introduced should be proportional to the probability of failure.

3.2 Detailed Description of Proposed Secured System Architecture

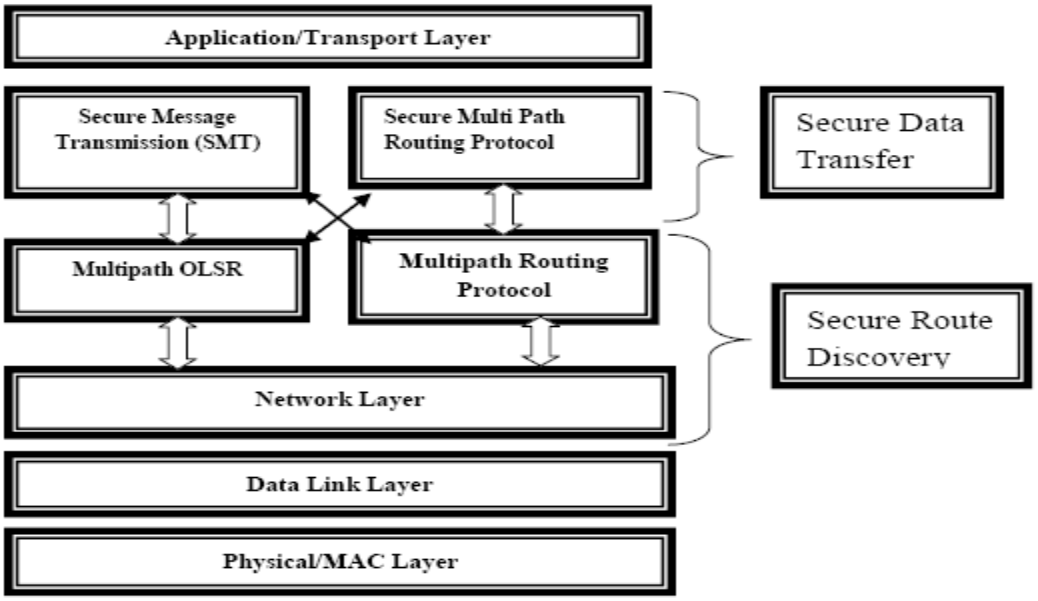

Figure 3.1: Architecture of the proposed system

Figure 3.1: shows the architecture of our Proposed system, in which 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. 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. 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. 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. Hence, MP-OLSR is to get the topology 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.

In order to over that attack we used Secure Message Transmission (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) protocol, which, given a topology view of the network, determines a set of diverse paths connecting the

source and the destination nodes. We have integrated secure multipath routing and secure data transmission protocols and showed how to achieve highly reliable and low-delay communication in a hostile networking environment.

- ✓ Implementation of Multipath OLSR.
- ✓ Information Dispersal
- ✓ Data Transmission

Algorithm:

BEGIN
INTIALIZE_SOURCE&DESTINATION NODE
DELETE THE ALL ENTRIES IN ITS ROUTING TABLE. BASED ON ITS NEIGHBOR TABLE,
INSERT THE NEW ENTRY TO ITS ROUTING TABLE;
BASED ON THE NODE'S TOPOLOGY TABLE, FOR EVERY ENTRY: IF R_DEST-=T_DEST && R_DEST==T LAST R_DEST=T_DEST;
R NEXT=R NEXT OF R DEST==T LAST; R_DIST=L+R_DIST OFR DEST==T_LAST;
R_BUFFER=THE MAXIMUM SIZE OF QUEUE OF INTERMEDIATE NODE; RECORD THE COMPLETE PATH INFORMATION IN THE ROUTING TABLE; DELETE THE RELATIVE NODE AND LINK INFORMATION IN NEIGHBOR AND TOPOLOGY TABLE, THEN CALCULATE ANOTHER PATH TO T_DEST ACCORDING TO REMAIN INFORMATION.
IF NO ANOTHER PATH TO T_DEST, REPEAT SAME PROCEDURE
IF THE CALCULATING SUCCEED, THEN
DELETE RELATIVE INFORMATION AND CALCULATE THE NEXT ONE, UNTIL FAILING.

3.2.1 Implementation of Multipath OLSR

The main function of this module has two parts: topology sensing and route computation. The topology sensing is to make the nodes aware of the topology information of the network. The route computation uses the Multipath Dijkstra Algorithm to calculate the multipath based on the information obtained from the topology sensing.

The route computation uses the Multipath Dijkstra Algorithm to calculate the multipath based on the information obtained from the topology sensing. The source route is saved in the header of the data packets. The aim of the multipath algorithm is to build a set K of N path, with no loops, joining a source node (noted s) and a destination node (noted d). Initially, for every node i, the updated Flag i is set to false, which means the route to the corresponding destination does not exist or needs to be renewed. When there is a route request to a certain node i, the source node will first check the updated Flag i.

If the updated Flag i equals false, the node will perform Algorithm 1 to get the multiple paths to node i, save it into the multipath routing table, and renew the corresponding updated Flag i to true.

If the updated Flag i equals true, the node will find a valid route to node i in the multipath routing table.

Every time the node receives a new TC or HELLO message and results in the changes in the topology information base, all the updated Flags will be set to false. The proposed algorithm is applied to a graph G = (V, E, c), two vertices (s, d) ∈ E2 and a strictly positive integer N. It provides an N-tuple (P1, P2... PN) of (s, d)-paths extracted from G. Dijkstra (G, n) is the standard Dijkstra algorithm which provides the source tree of the shortest paths from vertex n in graph G; Get Path (Source Tree, n) is the function that extracts the shortest-path to n from the source tree Source Tree; Reverse (e) gives the opposite edge of e; Head (e) provides the vertex edge to which e points. The nodes are created and shortest path is calculated from source node to destination node and data is sent in that shortest path.

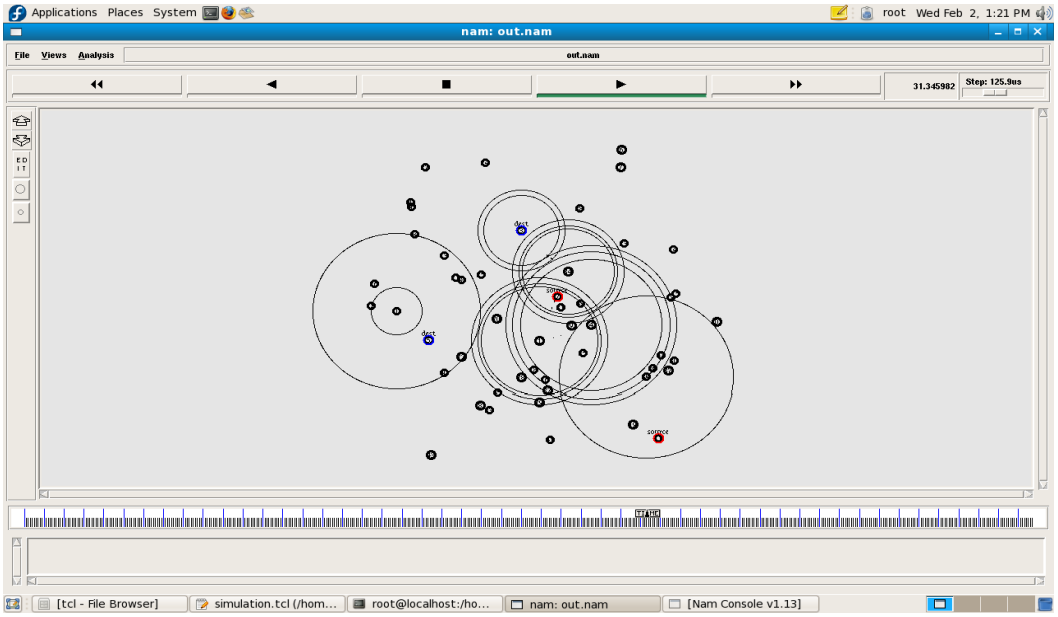

Figure 3.2 Implementation of MP-OLSR

3.2.2 Information Dispersal (Id)

In this module the Secure Message Transmission (SMT) scheme addresses data confidentiality, data integrity, and data availability in a highly adverse and mobile MANET environment. The SMT scheme operates on an end-to-end basis, assuming a Security Association (SA) between the source and destination nodes, so no link encryption is needed. This SA between end-nodes is used to provide data integrity and origin authentication, but it could also be utilized to facilitate end-to-end message encryption. The simulation results for SMT show that this scheme can successfully cope with a large number of adversaries in the network. Rabin purposes Information Dispersal Algorithm (IDA) in which proposed algorithm is based on simple matrix operations.

Suppose that the File F consists of N bytes: F = b1, b2... bn, where 0 _ bi _ 255. A prime number p > 255 is chosen; for example p = 257.

Next, n random vectors ai of length m are chosen and structured as rows of an n × m matrix A, such that any m different vectors are linearly independent: ai = (ai1,ai2, ..., aim).

The file F is divided into byte sequences of length m: F = (b1, bm), (bm+1, b2m), = S1, S2,

The vectors Si are multiplied by the vectors ai to form the set of dispersed file pieces: F1, F2, Fn. i.e. (vectors Si * vectors ai, -> F1, F2, F3….)

All arithmetic operations are performed in the finite field Zp, that is, modulo p. To reconstruct the original file F, only m pieces are required: F1, F2... Fm.

Each of the m pieces is multiplied by A−1, the inverse of matrix A containing only rows corresponding to the indices of the available pieces. i.e. (m pieces * A−1).

This algorithm has reasonable time complexity O (n3) since the necessary matrix operations can be implemented in a simple and efficient manner. The space overhead required by the algorithm for data redundancy is optimal since each of the n pieces is of size |F|/m, where |F| denotes the size of F.

3.2.3 Data Transmission

In this module the source transmits the dispersed messages across the *APS*; it updates the ratings of the utilized paths based on the feedback provided by the destination. Each path is associated with two ratings:

- Short-term and
- Long-term rating

The short-term rating, r_s, is decreased by a constant at each time a failed transmission is reported, and it is increased by a constant b for each successful reception.

The long-term rating, r_l, is a fraction of successfully received pieces over the total number of pieces transmitted across the route.

If either ***rs*** or ***rl*** or both drops below a threshold value, rs^{thr} and rl^{thr} respectively, the corresponding path is discarded. Both thresholds and constants are protocol selectable parameters.

The ***rs*** rating takes values in the interval *I = [rs thr, rsmax]*, with *rsth 0*, *rsmax* the maximum value for the path rating, and *rs(0)* its initial rating, assigned when a path is first added to the APS.

The constants a and b take values in the *(0, rs max]* interval. After the *i-th* transmission across a path that is not deemed failed yet, its rating is updated:

$$r_s(i) = \begin{cases} \max\{r_s(i-1) - \alpha, r_s^{thr}\}, & \text{if a piece is lost} \\ \min\{r_s(i-1) + \beta, r_s^{\max}\}, & \text{if a piece is received} \end{cases} \rightarrow 1$$

If *i* transmissions across a path include *s* successfully received pieces and *l* lost ones, then *i = s + l*, with *s*, *l* integers. If $r_s(i)$ has already reached the maximum value, then, additional successive acknowledged pieces do not increase the rating any further. If *s0* denotes the number of such successful receptions, and *s1* denotes the number of successful receptions while the path rating is below rsmax, then *s=s0+s1*. Thus, the rating of the path can be written as $r_s(i) = r_s(0) + s1 - l$.

For any route that is not deemed failed yet, $rs(i) \geq rs^{t}$. Then, $s1\beta - l\alpha \geq rs^{thr} - rs(0)$, (for S*1*, *l* integers not simultaneously zero). If we set $d = rs(0) - rs^{thr} \geq 0$, we can re-write the previous inequality as:

$$BSl - \alpha l + d \geq 0 \rightarrow 2$$

CONCLUSION AND FUTURE WORK

In our study, 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. Since it provides better statistics for packet delivery and number of packets dropped. Simulation results show that the attack can bring a devastating impact on the current MP-OLSR. It also shows that the proposed security mechanism provides an effective protection against this kind of attack. More over research is needed on secure routing protocol, robust key management, trust based systems, integrated approaches to routing security, data security in different level and cooperation enforcement. Cryptography is one of the most common security mechanisms and its strength relies on the secure key management. The public cryptography scheme depends upon centralized CA (Certificate Authority) which is known as a security weak point in MANET.As the future work we can change the key size and it enable more security as the key size increases the crypto analysis can be made more secure.

REFERENCES

1. Law and W. Kelton, "Simulation Modeling and Analysis," McGraw-Hill, 2000 [20] Trace graph URL: http://www.tracegraph.com/download.html
2. E. Cizeron, S. Hamma, A multiple description coding strategy for multipath in mobile ad hoc networks, in: International Conference on the Latest Advances in Networks (ICLAN), Paris, France, 2007.
3. 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.
4. Jiazi YI, Asmaa ADNANE, Sylvain DAVID, Benoıt PARREIN, "Multipath Optimized Link State Routing for Mobile ad hoc Networks", version 1, 28 Sep 2010.

5. K.P.Manikandan, Dr.R.Satyaprasad and Dr.Rajasekhararao "Analysis and Diminution of Security Attacks on Mobile Ad hoc Network" in IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.
6. Ko, Y., Vaidya, N. (2000). Location-Aided Routing (LAR) in Mobile Ad hoc Networks. Wireless Network (WINET), 6(4), 307-321, ACM.
7. L. Zhao and J. Delgado-Frias, "Multipath Routing Based Secure Data Transmission in Ad Hoc Networks", Proceedings of WiMob, 2006.
8. Li Zhao and Jose G. Delgado-Frias, "Multipath Routing Based Secure Data Transmission in Ad Hoc Networks".
9. Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks", San Diego, California, USA, September 19, 2003.
10. Q.V.M. Ernesto, M.M. Marta and L.E.S Jose, "The K shortest paths problem," Research Report, CISUC, June 1998.
11. Rashid Sheikhl Mahakal Singh Chandee, Durgesh Kumar Mishra, "Security Issues in MANET: A Review", 2010.
12. 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.

AUTHORS' PROFILES

Mrs. R. Priyadharshini received the M.Sc., in Government Arts College, Dharmapuri in 2009 respectively, doing her M.phil., in the specialization of Computer Science in Don Bosco College, Dharmapuri, Tamilnadu. She got a university seventh rank in M.Sc., She is a Research Scholar in the field of Mobile Ad hoc Networks. Her ongoing research focused on Routing Protocol in Wireless Sensor Network.

Mr. S. Rajesh Singh received the M.Sc., in PEE GEE College of Arts and Science, Dharmapuri in 2001 and M.Phil., degree in the specialization of Computer Science from Manonmaniam Sundaranar University, in 2003 respectively. He is an Assistant Professor in Department of Computer Science, Don Bosco College, Sogathur, Dharmapuri, Tamilnadu, India. He is very much interested in Digital Image Processing and Networking era.

Mr. A. Muruganandam received the M.Sc., in Thanthai Hans Roever College, Perambalur, and M.Phil., degree in the specialization of Computer Science from Manonmaniam Sundaranar University, in 1999 and 2004 respectively. He is an Assistant Professor cum Head in the Research Department of Computer Science, Don Bosco College, Sogathur, Dharmapuri, Tamilnadu, India. Presently pursuing Doctorate Degree [Ph.D.] in Computer Science at Bharathiar University, Coimbatore. He is a Research Scholar in the field of Wireless Sensor Networks.

