Table of Contents

I. INTRODUCTION

A. GENERAL

Multi-hop wireless ad hoc networks have attracted much attention in the field of research in modern times. In mobile ad hoc networks, nodes can be connected dynamically in a random fashion. Infrastructure of the network is not stationary in such networks. Each node works as a router and takes part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks have found use in different applications. For example, a rescue team communicates with each other in a disaster recovery scene using mobile devices and Impromptu communications among groups of people like secure business issues discussions, government secret issues discussions in parliament house etc. Another example is that a military group coordinates in a battlefield where there is no existing communication network available.

Generally speaking, we can visualize a multi-hop wireless ad hoc network as a collection of mobile nodes which are capable of communicating and networking. These nodes don’t need any intervention or an infrastructure to establish and maintain a network. As nodes move around, they make and break links between them. This means that compared to a wired network, the connections between nodes in the network make and break more frequently and dynamically. Consequently, network topology changes with time. The routing protocols designed for wired networks (for instance, the Internet) generally make use of either distance vector or link state routing algorithms. In distance vector routing, each router periodically broadcasts to its neighbor routers its view of the distance to all hosts. In link state routing, each router instead periodically broadcasts to all1other routers in the network its view of the status of its adjacent network links. Due to the frequent changes of link status and network topology, these routing protocols will incur high overhead to update and maintain the route information between any pair of nodes in a mobile ad hoc network (MANET). Therefore, the routing protocols used in wired networks are rather inefficient if used in MANETs.

In recent times, many new routing protocols have emerged for MANETs to handle such dynamic network topology changes. Although a current fashion is to approve ad hoc networks for commercial uses, there are silent alarms with respect to their openness to security attacks- The objectives of authenticity, confidentiality, availability, integrity and non-reputability are especially complicated to accomplish in MANETs because each node contributes in the actions of the network uniformly and it is very difficult to detect and delete a malicious node. In Ad hoc network the nonexistence of centralized and of infrastructure services, all stations of an ad hoc network drive as routers, all the routers are have the ability to shift randomly and sort out themselves arbitrarily, which decline the routing function with respect to security .

B. MOTIVATION

A Mobile Ad-hoc Network (MANET) is an Autonomous system of wireless nodes aimed at information exchange and resource sharing without any central infrastructure like Access point (AP). The Routing protocols in MANET have the capability of dynamic utilization of wireless nodes locations. As we already discuss that all of the M ANET routing protocols are used in open Environment without infrastructure, hence they come across a lot of security attacks. Some well-known attacks are denial of service (DoS), replay, modification, routing table over flow, impersonation, energy consumption, link spoofing ,identity spoofing, masquerading, and so on [1]. These Attacks are categorized into two parts; first category includes impersonation, traffic sniffing, modification or replay while category two includes link spoofing, identity spoofing and so on. Category I attacks are caused to classic wireless network due to the absence of centralized entities. These attacks are limited by cryptographic mechanism of authentication. But on the other hand, second category is only inherent to Ad-hoc network and can’t be controlled by authentication. In this category neighbor’s nodes pass false information and messages to other nodes, which further destroy routing tables of each node in MANET. This category can be eliminated by specific intrusion detection mechanism [2].

The motivation of my thesis is to design a secured routing mechanism for Optimized link state routing (OLSR) that may be applied for Secret Conventional Meeting and for emergency disaster management when other existing communication system are destroyed.

C. SCOPE AND PERPOSE

In our thesis work, we will deals with the security system for Impromptu communications among groups of people. For example, Secure Conventional meetings like secure business issues discussions in company board of governors meeting, government secret issues discussions in core commanders meeting and in parliament house etc. In this thesis we will identify and design a strong routing mechanism using Optimized link state routing (OLSR). Which will deals with the secure exchange of control messages by including secure MAC values (generated by using hash function on 1-hop neighbors) and Global secret key in both HELLO messages and TC messages. In this manner no malicious user can become part of meeting. We will configure a simulation of an ad hoc network using the extension for first responders in a conventional meeting scenario in the NS-2 simulation platform. The new protocol will be implemented through modification of the protocol definitions for NS-2 written in C++. The task will involve adjustment and experimentation with simulation parameters.

D. OBJECTIVE

Simulation can provide an insight into the basic operations and performance of an experimental protocol prior to performing a prototype implementation. Our goal is to implement the protocol so that,

- We can determine the appropriateness of the security extension through simulation.
- How much is the network performance affected by the deployment of the secured routing protocol compared to the original protocol or other routing protocol?
- Provide input to further development of the protocol and recommendations for real-world implementations.

E. THESIS OUTLINE

The rest of thesis is organized as follows.

- Chapter II discusses on existing routing protocols for MANETs and their security issues.

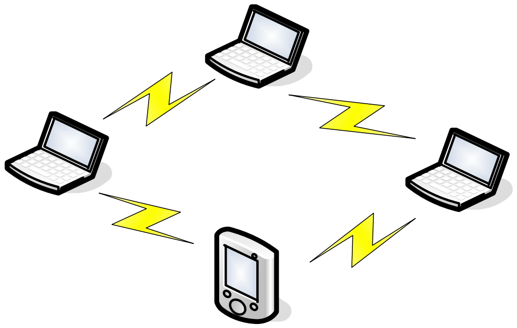
- Chapter III presents the Optimized Link State Routing protocol (OLSR), on which the security extension is based.
- Chapter IV discusses the vulnerabilities of OLSR and their Scenarios and the new security extension to OLSR. A brief overview of the access control, authentication mechanism and key establishment process is presented
- Chapter V outlines the details of the implementation in the source code of NS-2 to add the functionalities of the new security extension to OLSR. It presents the data structures and functions which handle new message formats and the security establishment process.
- Chapter VI presents the simulation procedures, parameters, results from our simulation of the new protocol and the performance of the new protocol in wireless ad hoc networks.
- Chapter VII discusses on the simulation result, their effects and reasons to choose the parameters used in the simulations.
- Finally chapter VIII briefly outlines the opportunities for further work and chapter ten concludes

the thesis.

Chapter 2

An Overview of Existing Routing Protocols for MANETs

Mobile Ad hoc networks or MANETs are the kind of wireless networks which do not need any fixed infrastructure or base stations. They can be easily installed in places where it is difficult to establish any wired infrastructure. As shown in Figure.2.1, there are no base stations and every node must take part in forwarding the packets in the network.



Mobile

Figure 2.1: A Mobile ad hoc network

Thus, each node works as a router which makes routing complicated when compared to Wireless LANs, where the central access point works as the router between the nodes.

Before discussing the general issues in MANETs, we will discuss why they are so popular as well as their benefits.

(a) *Low Installation Cost*: As is clear from the name, ad hoc networks can be installed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.

(b) *Fast and easy installation:* When compared to WLANs, ad hoc networks are very easy to install requiring less manual intervention since there are no cables involved.

(c) Dynamic Configuration: Ad hoc network configuration can vary dynamically with time. This is a useful feature in many situations such as data sharing in classrooms, etc. When compared to configurability of LANs, it is very easy to change the network topology.

MANET is going to be prominent part of many application areas such as

(a) *Uses in warfare*: Soldiers and vehicles can communicate using ad hoc networks during war. In such networks, the soldiers might communicate with each other using hand-held devices. Power sources can be installed in the vehicles for “recharging” these mobile devices.

(b) *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 situations through which the workers can communicate.

(c) *Event Coverage*: Situations such as a press conference might require reporters to share data amongst other reporters. In such cases, multimedia traffic might be conveyed between nodes such as laptops, PDAs, etc.

(d) *Classroom*: Students and instructors can establish an ad hoc wireless network to communicate using laptops.

2.1 ROUTING PROTOCOLs IN MANETs

As we are already familiar that ad hoc network routing protocols have very complex nature and designing issues like dynamic topology, Bandwidth constraint, Error prone broadcast channel, Hidden and exposed terminal Problems, Resource limitations, Quos limitations, Security. An ample amount of effort has been made in the research society to tackle the problem for wireless ad hoc networks. As a consequence of research a number of routing protocols which can be categories as position-based routing protocols and topology-based routing protocols as shown in Figure 2.2. And there is a wide difference between these two protocols i.e. Topology based routing protocol uses the concept of conventional routing such as distributing link state information or maintaining a routing table while geographical routing or Position based routing protocol relies on geographical physical position of the mobile stations to route the desire data packets to the destination.

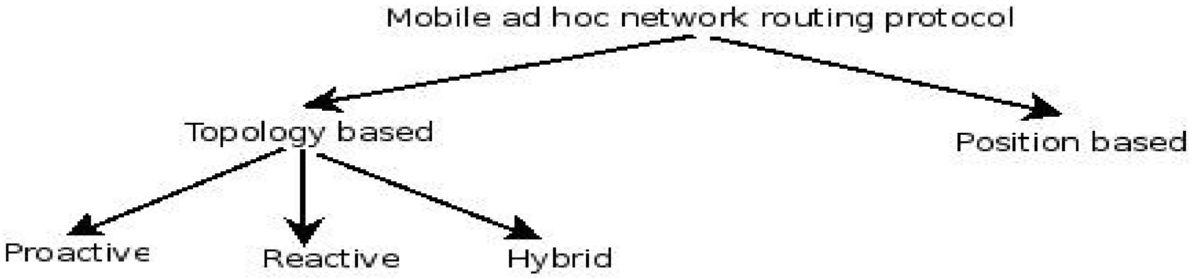


Figure 2.2: Classification of MANET routing protocols

We can further divide Topology based routing protocols into two more groups i.e. proactive and reactive protocols. As the name indicates Proactive protocols try to maintain fresh and regular information within the system according to their destinations and routes, in proactive routing protocols the route must be established before the data transmission therefore in such communication the source node have predefine route to the destination node while in reactive routing protocols they do not need to search for a predefine route because they establish route on demand. In the nut shell we can also call it is on-demand routing protocols.

As stated earlier, Proactive routing protocols maintain information according their routes and destinations, in spite of of whether or not these destinations and routes are needed. In order to gain update information about the links, a node must periodically exchange the control messages.

So in that case a lot of wastage of bandwidth occurs because of unnecessary exchange of messages and this problem become serious when less number of nodes are communicating in a network. The main advantage of proactive base routing protocols is that nodes can quickly obtained link information and rapidly set up a session and packet can be transfer to the destination without any delay. In contrast to this, reactive protocols can dramatically decrease the routing overhead because they do not need the exchange of messages for the search and maintain routes on which that time there is no data traffic. On the other hand the delay is a problem which arises here because nodes spent allot of time and waste resources to search the routes when a communication is necessary. The tradeoffs between reactive and proactive routing protocols are reasonably multifaceted. Therefore the concept of hybrid protocol are exists which is basically the combination of reactive and proactive protocol. Hybrid protocols use the combine approaches of these routing strategies to search and maintain the routes. The hybrid protocol is proactive within a limited geographic area while reactive if a packet must be passing through several of these geographic areas. Zone routing protocol (ZRP) is well known example of Hybrid routing protocols.

In position Based routing the source uses the destination physical location to send a data packet instead of using the destination network address. Position based routing requires that each node is aware of its own location and the source also aware of the destination position with help of GPS (Global Positioning System). When a source sending a data packet to a destination, the first step is to obtain the location of the destination with help of any location service and then in the 2nd step the source includes this information in the packet headers. Then there are various strategies like single path, multi path and flooding strategies are used to transfer the packet from source to destination. In this communication each transitional node behaves as router that collect the packet obtains the position information of the desire destination from the packet header and uses this information to forward the packet towards the destination without any knowledge of the network topology or route. The main advantage of position bases routing is that the traffic overhead is greatly reduces and on the other hand the disadvantage of the position base routing is that the network nodes need some hardware and software installation to find out the location of each other for example monitoring devices like GPS device and another problem is also link with this strategy that is the unavailability of satellite coverage in underground area, for example if there is a fire inside a tunnel then in such situation fiber brigade employees cannot rely on the Global Position system for position identification.

In this chapter our objective is to present an overview of some basic routing protocols for MANETs and their working principle. A comprehensive description of all existing ad hoc network routing protocols is considered out of scope.

2.1.1 Table-driven/Proactive Routing Protocols

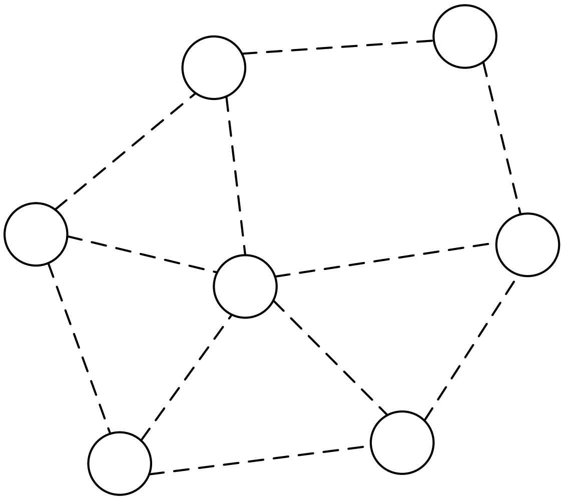
Proactive protocols or in table-driven, the nodes preserve an active list of routes to every other node in the network in a routing table. They update these tables are periodically by broadcasting information to other nodes in the network. Thus, they are similar to the wired network routing protocols such as the Routing Internet Protocol (RIP). Any node wishing to communicate with another node has to obtain the next hop neighbor on the route to the destination from its routing table. Some instances of table-driven routing protocols are Destination Sequenced Distance-Vector routing protocol (DSDV) , Wireless Routing Protocol (WRP) , Cluster Switch Gateway Routing protocol (CGSR) , etc. In the following sections we explain working of DSDV and WRP, and the general pros and cons of table-driven routing protocols are enlisted.

2.1.1.1 Destination Sequenced Distance Vector (DSDV) Routing Protocol

The Destination Sequenced Distance Vector (DSDV) protocol is a proactive routing protocol based upon the distributed Bellman Ford algorithm. In this routing protocol, each mobile host maintains a table consisting of the next-hop neighbor and the distance to the destination in terms of number of hops. It uses *sequence numbers* for the destination nodes to determine “freshness” of a particular route, in order to avoid any short or long-lived routing loops. If two routes have the same sequence number, the one with smaller distance metric is advertised. The sequence number is incremented upon every update sent by the host. All the hosts periodically broadcast their tables to their neighboring nodes in order to maintain an updated view of the network. The tables can be updated in two ways – either *incrementally* or through a *full dump*. An incremental update is done when the node doesn’t observe any major changes in the network topology. A full dump is done when network topology changes significantly or when an incremental update requires more than one NPDU (Network Packet Data Unit).

Let us consider an example to understand the routing mechanism better. Consider the network topology shown in figure 2.3. The routing table for this network is shown in table 2.1. As shown in the table, each node maintains a route to every other node in the network during the route establishment phase. Whenever there is a link break in the network, the end node of the broken link propagates a routing table update message with the broken link’s weight assigned to infinity.

This message is broadcasted by every node to its neighbors. A broken link is denoted by an odd sequence number and an ordinary link by an even sequence number. When node 1 wants to send data to node 7, it checks the next hop neighbor for node 7, which is 2 and passes the data packet to it.



6

Figure 2.3: Topology graph of the network

Destination	Next hop	Metric	Sequence number
1	-	0	S40_1
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	2	3	S94_7

4

3

Table 2.1: Routing table for node 1

1

Source node

Figure 2.4 shows the case when node 7 moves out of range of nodes 6 and 5. Thus the link 6-7 and 7-5 are broken and the routing table at 1 is now reorganized as shown in Table 2.2. When node 4 hears the update request from node 7 with a higher sequence number, it broadcasts this information to all nodes. This eventually reaches node 1 which changes the next hop, metric and the sequence number entry in routing table for

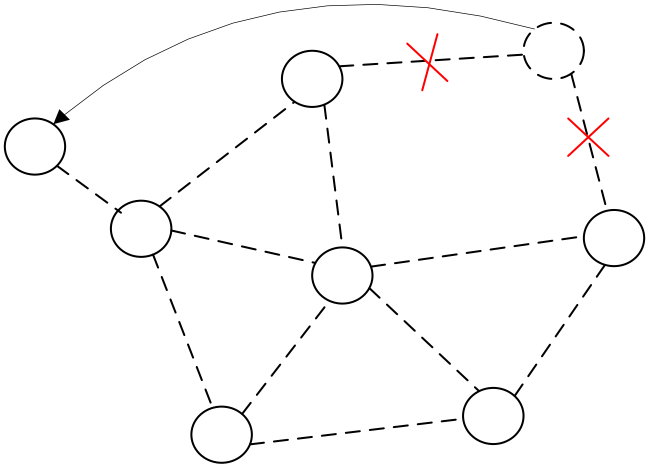


Figure 2.4: Topology graph of the network when node 7 moves

Destination	Next hop	Metric	Sequence number
1	-	0	S40_1
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	4	2	S98_7

Table 2.2: Modified routing table for node 1

DSDV guarantees loop free routes to each destination and also finds the optimal path. It uses an *average settling delay* to prevent frequent routing table updates and any fluctuations caused by two similar routing advertisements which are in an incorrect order of the sequence numbers.

2.1.1.1.1 Pros and Cons of Table-driven Routing protocols

One of the main benefits of table-driven routing protocols is that the routing information to any node is available at all times since routes to all the nodes are stored in the routing table. But this also means that the routing tables may contain routes to destinations which are not required. Due to this, there is more memory consumption at each node as the size of the network increases. Further, it has been found that table-driven protocols such as DSDV fail to converge at higher mobility rates of the nodes. This issue will be explored further next, where the simulation study of performance in MANETs is explained.

2.1.2 On-Demand/Reactive Routing Protocols

In contrast to table driven routing protocols, on-demand routing protocols find route to a destination only when it is required. The on-demand protocols have two phases in common – route discovery and route maintenance. In the route discovery procedure, a node wishing to communicate with another node initiates a discovery mechanism if it doesn't have the route already in its cache. The destination node replies with a valid route. The route maintenance phase involves checking for broken links in the network and updating the routing tables. The working of a few reactive routing protocols is now described.

2.1.2.1 Dynamic Source Routing (DSR) Protocol

The Dynamic Source Routing Protocol is an on-demand routing protocol which is based on the concept of *source routing*. In source routing, a sender node specifies in the packet header, the complete list of nodes that the packet must traverse to reach the destination node. This essentially means that every node just needs to forward the packet to its next hop specified in the header and need not check its routing table as in table-driven routing protocols. Furthermore, the nodes don't have to periodically broadcast its routing tables to neighboring nodes. The DSR protocol works in two phases as described below-

2.1.2.1.1 Route Discovery

In the route discovery phase, the source node establishes a route by broadcasting route request (RREQ) packets to all its neighbors. Each neighboring node, in turn rebroadcasts the packets to its neighbors if it has not already done so, or if it is not the destination node, provided that the TTL (Time to Live) counter is greater than zero. Further, *request ids* are used to determine if a particular route request has been previously received by the node. Each node maintains a list of recently received <*initiator, request id*> pairs. If two route requests with the same <*initiator, request id*> are received by a forwarding node, it broadcasts only one of them and drops the other. This also prevents formation of routing loops in the network. When the packet reaches the destination intended, the destination node uncast a reply packet (RREP), which contains the route to that destination on the reverse path back to the sender. Figure 2.5 shows an example of the route discovery mechanism. When node 1 wants to communicate with node 7, it initiates a route discovery mechanism and broadcasts request packet RREQ to its neighboring nodes 2, 3 and 4 as shown. However, node 3 also receives the broadcast packets from nodes 4 and 2 with the same <*initiator, request id*> *pair*. It drops both of them and broadcasts the packet to its neighbors. The other nodes follow the same procedure. When the packet reaches node 7, it inserts its own address and reverses the route in the record and uncast it back on the reverse path to the destination.

The destination node uncast the best route (received first) and caches the other routes for future. A *route cache* is maintained at every node so that, whenever a node receives a route request and finds a route for the destination node in its own cache, it sends a RREP packet itself without broadcasting it further.

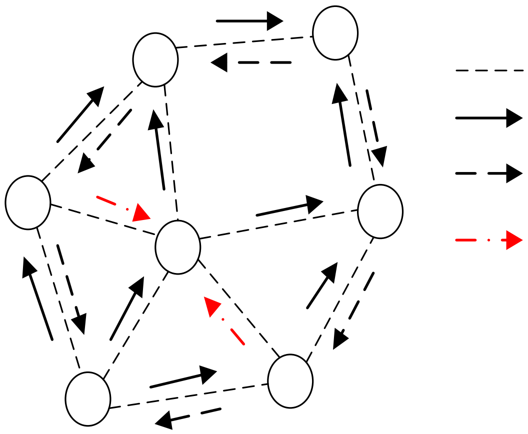


Figure 2.5: Route Discovery in DSR

2.1.2.1.2 Route Maintenance

The route maintenance phase is carried out whenever there is a broken link between two nodes. A failed link can be detected by a node by either passively monitoring in promiscuous mode or actively monitoring the link. As shown in Figure 2.6, when an intermediate node in the path moves away, causing a wireless link to break (6-7), a route error packet (RERR) is sent by the intermediate node back to the originating node. The source node re-initiates the route discovery procedure to find a new route to the destination. It also removes any route entries it may have in its cache to the destination node.

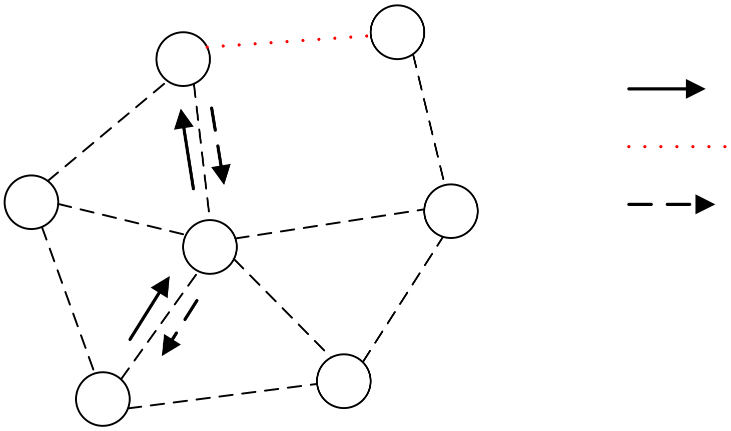


Figure 2.6: Route Maintenance in DSR

DSR benefits from source routing since the intermediate nodes need not maintain up-to-date routing information in order to route the packets that they forward. There is also no need for any periodic routing advertisement messages. However, as size of the network increases, the routing overhead increases since each packet has to carry the entire route to the destination with it. The use of route caches is a good mechanism to reduce the propagation delay but overuse of the cache may result in poor performance. The disadvantage of DSR is that whenever there is a link break, the RERR packet propagates to the original source, which in turn initiates a new route discovery process. Thus the link is not repaired locally. Several Optimizations to DSR are possible such as *non- propagating route requests* (when sending RREQ, nodes set the hop limit to one preventing them from re-broadcasting), *gratuitous route replies* (when a node over hears a packet with its own address listed in the header, it sends a RREP to the originating node bypassing the preceding hops), etc. A detailed explanation of DSR optimizations can be found in.

2.1.2.2 Ad hoc On-demand Distance Vector (AODV) Routing Protocol

The Ad hoc on-demand Distance Vector routing protocol [9] inherits the good features of both DSDV and DSR. The AODV routing protocol uses a reactive approach to finding routes and a proactive approach for identifying the most recent path. More specifically, it finds routes using the route discovery process similar to DSR and uses destination sequence numbers to compute fresh routes. The two phases are discussed in more detail-

2.1.2.2.1 Route Discovery

In the route discovery process, the source node broadcasts RREQ packets similar to DSR. The RREQ packet comprises the source identifier (Sid), the destination identifier (Did), the source sequence number (See), the destination sequence number (Desk), the broadcast identifier (Bid) and TTL fields. When an intermediate node collects a RREQ packet, it either forwards it or makes a Route Reply (RREP) packet if it has a valid route to the destination in its cache. The (Sid, Bid) pair is used to determine if a particular RREQ has already been received in order to exclude duplicates. Every intermediate node goes in the previous node's address and its Bid while forwarding a RREQ packet. The node also keeps a timer related with every entry in order to erase a RREQ packet if the reply is not received before it terminates.

Whenever a RREP packet is received by a node, it stores the information of the previous node in order to forward the packet to it as the next hop towards the destination. This acts as a "forward pointer" to the destination node. Thus each node keeps only the next hop information unlike source routing in which all the intermediate nodes on the route towards the destination are stored.

Figure 2.7 shows an instance of route discovery mechanism in AODV. Let us assume that node 1 needs to send a data packet to node 7 but it doesn't have a route in its cache. Then it starts a route finding process by broadcasting a RREQ packet to all its neighboring nodes.

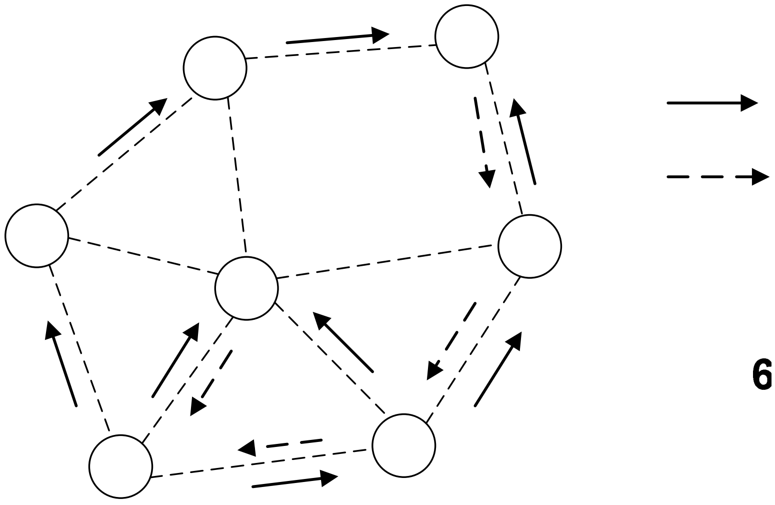


Figure 2.7: Route discovery in AODV

It inserts the SId, DId, SSeq, DSeq, Bid, and TTL fields in the RREQ packet. When nodes 4, 3 and 2 receive this, they check their route caches to see if they already have a route. If they don't have a route, they forward it to their neighbors, else the destination sequence number DSeq in the RREQ packet is compared with the DSeq in its corresponding entry in route cache. If the DSeq in RREQ packet is greater, then it answers to the source node with a RREP packet containing the route to the destination. In figure 2.4.2.1, node 3 has a route to 7 in its cache and its DSeq is higher compared to that in RREQ packet. So, it sends a RREP back to the source node 1. Thus the path 1-3-6-7 is stored in node 1. The destination node also sends a RREP back to the source. For example, one possible route is 1-2-5-7. The intermediate nodes on the path from source to destination update their routing tables with the latest DSeq in the RREP packet.

2.1.2.2.2 Route Maintenance

The route maintenance mechanism works as follows – Whenever a node senses a link break by link layer acknowledgements or HELLO beacons, the source and end nodes are informed by spreading an RERR packet similar to DSR. This is shown in Figure 2.8. If the link between nodes 3 and 5 disrupts on the path 1-3-5-7, then both 5 and 3 will send RERR packets to inform the source and destination nodes.

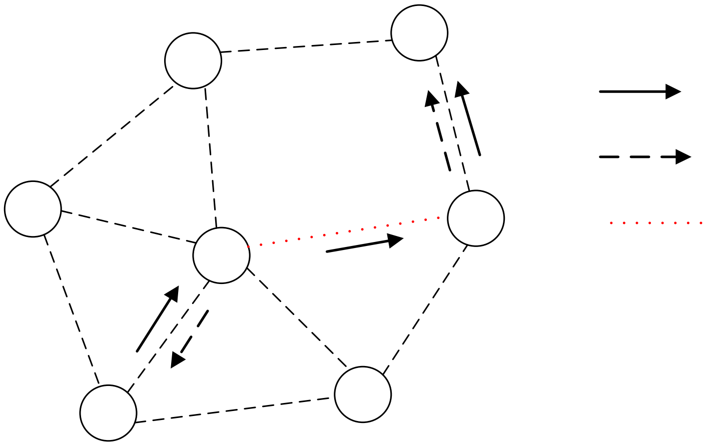


Figure 2.8: Route Maintenance in AODV

One optimization possible in AODV route maintenance is to use an expanding ring search to control the flood of RREQ and determine routes to unknown destinations . The main advantage of AODV is that it evades source routing thereby reducing the routing overload in large networks. Further, it also offers destination sequence numbers which allows the nodes to have more up-to-date routes. However, AODV needs bidirectional links and periodic link layer acknowledgements to sense broken links. Further, it has to keep routing tables for route maintenance unlike DSR.

2.1.2.3 Comparison of DSR and AODV

Table 2.3 provides a comparison of the features of DSR and AODV

Protocol **Feature**	**DSR**	**AODV**
Destination sequence numbers	Not used	Used
Link Layer acknowledgements	Not Required	Required (using HELLO beacons) for link breakage

		detection
Routing mechanism	Source routing – Multiple route caches for each destination	Table driven – one entry per destination. Sequence numbers used for
Route storage mechanism	Using route caches	Using routing tables
Timers	Not Used	Used
Multiple Routes	Yes	No
Optimizations	Salvaging, Gratuitous route replies (RREP) and Route Error (RERR), non-propagating route requests [11]	Expanding ring search [10]

Table 2.3: Comparison of the features of DSR and AODV

The chief difference is the source routing used by DSR in contrast to table-driven routing used by AODV. Due to this, DSR has a higher routing burden when the size of the network rises since each packet header has typically more information when compared to AODV. Another key difference is that AODV requires link layer acknowledgements or HELLO beacons at periodic intervals in order to detect link breaks. However, DSR avoids this feature and hence more efficient. Further, DSR stores multiple route caches for a destination whereas AODV does not. It has been established that this has an influence on the end-to-end delay and the delivery fraction as the size of the network increases. DSR has been found to do well in lightly loaded networks, whereas AODV performs well in more demanding networks (with higher density of nodes). AODV also profits from its timer mechanisms by keeping fresher route entries as compared to DSR, which doesn't implement any timers. Besides, in DSR all requests reaching a destination node are replied to, whereas in AODV the destination replies only once to the request arriving first and ignores others.

2.1.2.4 Optimized Link State Routing Protocol

The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol adjusted for mobile ad-hoc networks, which can also be used on other wireless ad-hoc networks. OLSR is a proactive link-state routing protocol, which uses *hello* and *topology control* (TC) messages to find out and then distribute link state information throughout the mobile ad-hoc network. Different nodes use this topology information to work out next hop destinations for all nodes in the network using shortest hop forwarding paths. We will discuss this protocol in detail in chapter 4 of this thesis because security extension is based on this protocol.

Chapter 3

Attacks over Ad-hoc Network

Wireless network is more multipurpose than a wired one, but it is also more susceptible to attacks. This is due to the extremely nature of radio transmissions, which are made on the air. The susceptibility nature of wireless communication is only its exposed environment; malevolent nodes could easily attack over establishing wireless environment.

On a wired network, an intruder would need to force an entry into a machine of the network or to physically bug a cable. On a wireless network, an adversary is able to overhear on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer (and possibly a directional antenna). There is a wide range of tools available to detect, monitor and penetrate an IEEE 802.11 network, such as NetStumbler1, Air Peek, Kismet, Air Snort, and

Ethereal. Hence, by simply being within radio range, the intruder has access to the network and can easily interrupt transmitted data without the sender even knowing (for instance, imagine a laptop computer in a vehicle parked on the street spying on the communications inside a nearby building). As the intruder is potentially invisible, it can also store, change, and then retransmit packets as they are released by the sender, even acting as if those packets come from a legitimate party. Furthermore, due to the restrictions of the medium, communications can easily be disturbed; the intruder can execute this attack by keeping the medium busy sending its own messages, or just by overcrowding communications with noise.

In a mobile ad hoc network, all the nodes co-operate amongst each other to forward the packets in the network and hence, each node works as a router. Thus one of the important issues is routing and security of the routing protocol. Security in an ad hoc network is of great importance in situations like battlefield. The three goals of security - confidentiality, integrity and authenticity are very difficult to achieve since every node in the network takes part equally in the network. In the areas of ad hoc networks security is the main mile stone towards the protection of the data integrity and confidentiality. To maintain a secure communication between nodes, we have to eliminate both Passive attacks (over hearing of transmitted data packets) and Active attacks (external attacks whose aims to shut down the continuity of communication). In short, for Secure Routing Mechanism during communication using MANET routing protocols, we have to take the following vulnerabilities under consideration during system designing.

- Route discovery inconsistency by Link spoofing or identity spoofing
- Changing packet contents
- Packet dropping/invalidating packet
- Modifying route replying
- Invalidating route cache

2.1 Attacks against the Routing Layer in MANETs

We now emphasize on assaults against the routing protocol in ad hoc networks. These attacks may have the aim of changing the routing protocol so that traffic runs through a specific node controlled by the attacker. An attack may also aim at hampering the formation of the network, making legitimate nodes store incorrect routes, and more generally at disturbing the network topology. Attacks at the routing level can be classified into two chief groups: incorrect traffic generation and incorrect traffic relaying. Sometimes these overlap with node misbehaviors that are not due to malevolence, e.g. node malfunction, battery exhaustion, or radio interference.

2.1.1 Incorrect Traffic Generation

This category comprises attacks which consist in sending false control messages: i.e. control messages sent on behalf of another node (identity spoofing), or control messages which contain incorrect or outdated routing information. The network may display Byzantine conduct, i.e. conflicting information in different parts of the network. The consequences of this attack are degradation in network communications, inaccessible nodes, and possible routing loops.

2.1.1.1 Cache Poisoning

As an example of incorrect traffic generation in a distance vector routing protocol, an attacker node can publicize a zero metric for all destinations, which will cause all the nodes around it to route packets toward the attacker node. Then, by discarding these packets, the attacker causes a large part of the communications exchanged in the network to be lost. In a link state protocol, the attacker can incorrectly publicize that it has links with distant nodes. This causes incorrect routes to be stored in the routing table of legitimate nodes, also known as *cache poisoning*.

2.1.1.2 Message Bombing and other DoS Attacks

The attacker can also try to carry out Denial of Service on the network layer by soaking the medium with a storm of broadcast messages (*message bombing*), reducing nodes' good put and possibly obstructing nodes from communicating. (This is not possible under hybrid routing protocols, where nodes cannot issue broadcast communications.) The attacker can even send invalid messages just to keep nodes busy, wasting their CPU cycles and exhausting their battery power. In this case the attack is not aimed at altering the network topology in a certain style, but rather at generally disturbing the network functions and communications.

On the transport layer, Kuzmanovic and Knightly prove the efficacy of a low-rate Do's attack done by sending short surges repeated with a slow timescale frequency (*shrew attack*). In the case of severe network cramming, TCP functions on timescales of Retransmission Time Out (RTO). The throughput (Composed of legitimate traffic as well as DoS traffic) activates the TCP cramming Nodes' throughput is composed of two kinds of traffic: control packets and data packets.

2.1.2 Incorrect Traffic Relaying

Network communications coming from legitimate, protocol-compliant nodes may be contaminated by misbehaving nodes.

2.1.2.1 Blackhole Attack

An attacker can discard received routing messages, instead of relaying them as the protocol requires, in order reducing the quantity of routing information available to the other nodes. This is called *blackhole attack*, and is a "passive" and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a specified destination, a packet every packets, a packet every _ seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

2.1.2.2 Message Tampering

An attacker can also change the messages sent from other nodes before relaying them, if a process for message integrity (i.e. a digest of the payload) is not used.

2.1.2.3 Replay Attack

As topology varies, old control messages, though valid in the past, present a topology configuration that no longer exists. An attacker can carry out a replay attack by copying old valid control messages and re-sending them, to make other nodes update their routing tables with stale routes. This attack is fruitful even if control messages carry a digest or a digital signature that does not include a timestamp.

2.1.2.4 Wormhole Attack

The *wormhole attack* is very strong, and consists in copying traffic from one region of the network and replaying it in a different region. It is carried out by an intruder node located within transmission range of legitimate nodes □ and where □ and _ are not themselves within transmission range of each other. Intruder node % merely tunnels control traffic between □ and _ (and vice versa), without the modification presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that % is virtually invisible.

The strength of the wormhole attack is because it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are protected. Furthermore, on a distance vector routing protocol, wormholes have greater probability to be chosen as routes because they provide a shorter path –

although compromised – to the destination. Marshall Points out a similar attack, called the *invisible node attack* by Carter and Yasinsac, against the Secure Routing Protocol.

2.1.2.5 Rushing Attack

An offensive that can be carried out against on-demand routing protocols is the *rushing attack*. Typically, on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are bypassed. This is done for reducing cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is started. If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker.

2.2 Attacks against the OLSR Protocol

Wireless Environment has a lot of holes for security due to its openness and dynamic membership of the nodes. An intruder can very easily join the MANET because of the many attach points. In OLSR the neighbors frequently exchange HELLO messages in order to select its MPR, while the TC messages are exchanges only between MPR's for sharing its MPR's selectors. The exchange of these messages causes to OLSR vulnerabilities. Controls messages can be tamper in two categories, in category 1 include identity spoofing (change its identity) while category 2 include link spoofing (change its contents) [5]. Some well known attacks belong from these categories will be discus in chapter 5 in detail.

Chapter4

Optimize Link State Routing Protocol (OLSR)

Optimized link state routing protocol (OLSR) is a link state proactive/table-driven protocol developed by INRIA. OLSR is a modified version of Link state routing protocol (LSR) design for MANET. OLSR got optimization over LSR by using special nodes called MPRs (Multi point relays). The neighboring nodes select their MPRs. Using LCR every node advertises its links while in OLSR only MPRs advertises their links. Secondly in LSR each node forward messages for its neighbors while in OLSR the case is different. In OLSR only MPR's forward messages to those nodes, which select them as their MPR. Each node of MANET selects its MPR in such a manner that it can reach to its two hop neighbors through it. Through this way MPRs minimizes the broadcast of packets in the whole network by reducing the number of duplicate transmissions of messages in the same region. The neighbor's nodes advertise HELLO messages with each other. Each node further finds two hop neighbors from HELLO message of its one hop neighbor. A node also gets HELLO message from the node that has selected it as MPR. The neighboring nodes become MPRs selector set for this selected MPR node. Topological control (TC) messages are periodically advertised by the MPRs to the whole MANET in order to declare its MPR selector set for the construction of routing tables in every MANET node.

OLRS Differ from LSR, in the sense that OLSR routing selection is localized. In the construction of routing table, OLSR keeps MPRs as a last hop to destination instead of all nodes to the destination. Simply each node takes its own MPR instead of taking decision that which neighbor serve as last hop to the destination. The optimization of OLSR has a big advantage of limiting the broadcast/flooding of routing messages and updates. But along with this, it also creates security threads to MANET. It provides a lot of attack points for the malicious users. However we can get control over it through Distributed intrusion detection mechanisms.

The Optimization link state routing protocol (OLSR) is one of the secure protocols used in MANET. A lot of the research is going on for the strong security on OLSR. Because of the secure nature of OLSR, this protocol is in wide utilization.

4.1 Applications

OLSR is a proactive routing protocol for mobile ad-hoc networks (MANETs). It is well suited to large and dense mobile networks, as the optimization achieved using the MPRs works well in this context. The larger and more dense a network, the more optimization can be achieved as compared to the classic link state algorithm. OLSR uses hop-by-hop routing, i.e., each node uses its local information to route packets.

OLSR is well suited for networks, where the traffic is random and sporadic between a larger set of nodes rather than being almost exclusively between a small specific set of nodes. As a proactive protocol, OLSR is also suitable for scenarios where the communicating pairs change over time: no additional control traffic is generated in this situation since routes are maintained for all known destinations at all times. The Application areas in which this protocol can work better than others are given below:

- Military or Police Exercises
- Disaster Relief
- Secure Conventional Meeting
- Personal area network (PAN)
- Mince site operation

The research aims to the application of OLSR in a Secure Conventional Meeting like online discussion on secret business issues or discussion of Ministers over government issues. In this case how the OLSR provides a secure environment from any sort of attacks from malicious or unauthorized users. In this chapter, we will briefly present the working principal of the OLSR routing protocol and a selection of the proposed extensions to secure the protocol.

4.2 OLSR Protocol Overview and Working Principle

OLSR is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol, tailored for mobile ad hoc networks.

OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called MPRs, to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, OLSR requires only partial link state to be flooded in order to provide shortest path routes. The minimal set of link state information required is that all nodes, selected as MPRs, MUST declare the links to their MPR selectors. Additional topological information, if present, MAY be utilized e.g., for redundancy purposes.

OLSR MAY optimize the reactivity to topological changes by reducing the maximum time interval for periodic control message transmission. Furthermore, as OLSR continuously maintains routes to all destinations in the network, the protocol is beneficial for traffic patterns where a large subset of nodes are communicating with another large subset of nodes, and where the [source, destination] pairs are changing over time. The protocol is particularly suited for large and dense networks, as the optimization done using MPRs works well in this context. The larger and more dense a network, the more optimization can be achieved as compared to the classic link state algorithm.

OLSR is designed to work in a completely distributed manner and does not depend on any central entity. The protocol does NOT REQUIRE reliable transmission of control messages: each node sends control messages periodically, and can therefore sustain a reasonable loss of some such messages. Such losses occur frequently in radio networks due to collisions or other transmission problems.

Also, OLSR does not require sequenced delivery of messages. Each control message contains a sequence number which is incremented for each message. Thus the recipient of a control message can, if required, easily identify which information is more recent - even if messages have been re-ordered while in transmission.

Furthermore, OLSR provides support for protocol extensions such as sleep mode operation, multicast-routing etc. Such extensions may be introduced as additions to the protocol without breaking backwards compatibility with earlier versions.

OLSR does not require any changes to the format of IP packets. Thus any existing IP stack can be used as is: the protocol only interacts with routing table management.

4.1.1 Multipoint Relay (MPR)

The idea of multipoint relays is to minimize the overhead of flooding messages in the network by reducing redundant retransmissions in the same region. Each node in the network selects a set of nodes in its symmetric 1-hop neighborhood which may retransmit its messages. This set of selected neighbor nodes is called the "Multipoint Relay" (MPR) set of that node. The neighbors of node N which are *NOT* in its MPR set, receive and process broadcast messages but do not retransmit broadcast messages received from node N.

Each node selects its MPR set from among its 1-hop symmetric neighbors. This set is selected such that it covers (in terms of radio range) all symmetric strict 2-hop nodes. The MPR set of N, denoted as MPR (N), is then an arbitrary subset of the symmetric 1-hop neighborhood of N which satisfies the following condition: every node in the symmetric strict 2-hop neighborhood of N must have a symmetric link towards MPR (N). The smaller a MPR set the less control traffic overhead results from the routing protocol. Gives an analysis and example of MPR selection algorithms.

Each node maintains information about the set of neighbors that have selected it as MPR. This set is called the "Multipoint Relay Selector set" (MPR selector set) of a node. A node obtains this information from periodic HELLO messages (HELLO message is described in section 4.1.2) received from the neighbors.

A broadcast message, intended to be diffused in the whole network, coming from any of the MPR selectors of node N is assumed to be retransmitted by node N, if N has not received it yet. This set can change over time (i.e., when a node selects another MPR-set) and is indicated by the selector nodes in their HELLO messages.

4.1.2 HELLO Message

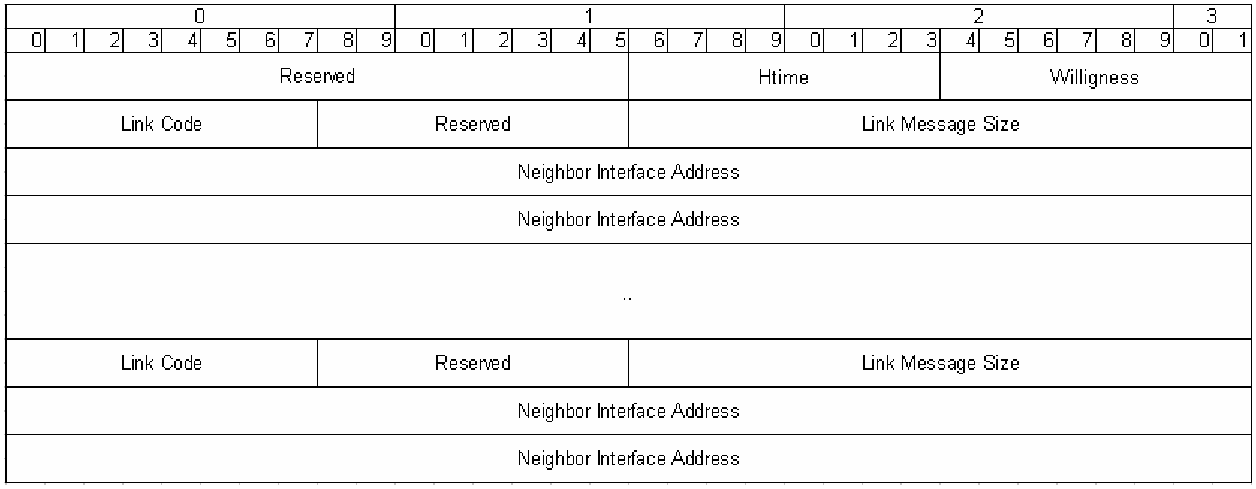
HELLO messages are sent periodically by a node and are used for neighbor sensing and Multipoint Relay (MPR) selection. HELLO messages are broadcasted within only 1-hop neighbor and are not retransmitted further.

It contains the list of neighbors from which control traffic is being heard, the list of neighbors with which a symmetric link is established and the list of MPR set that has been selected by the originator of the message.

Upon receiving the HELLO message, a node examines the list of addresses. If it finds its own address in the list then the node assumes that a bi-directional link can be established with the originator of the message. Besides sensing the link status with the neighbors, periodical exchange of HELLO messages gives information about the nodes that are two-hops away. This information is stored as 2-hop neighbor set and is used for the selection of MPR set.

To accommodate for link sensing, neighborhood detection and MPR selection signaling, as well as to accommodate for future extensions, an approach similar to the overall packet format is taken. Thus the proposed format of a HELLO is show in figure 4.1 which we will be discus in chapter 6th.

HELLO Message Packet Format



<table>
<tr><td colspan="10">0</td><td colspan="10">1</td><td colspan="10">2</td><td colspan="2">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="16">Reserved</td><td colspan="8">Htime</td><td colspan="8">Willigness</td></tr>
<tr><td colspan="8">Link Code</td><td colspan="8">Reserved</td><td colspan="16">Link Message Size</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
<tr><td colspan="32">..</td></tr>
<tr><td colspan="8">Link Code</td><td colspan="8">Reserved</td><td colspan="16">Link Message Size</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
</table>

Figure: 4.1 OLSR HELLO Message Frame Format

4.1.3 TC Message

TC messages are sent periodically just like HELLO messages but the interval is larger than HELLO messages. The purpose of TC messages is to diffuse link state information to the entire network that will be used for routing table calculation. The message contains the list of bi-directional links between a node and some of its neighbors. The novelty of OLSR lies into the broadcast technique of TC messages as it is flooded into the network exploiting the MPR optimization and thus reducing the number of messages flooded into the network. Only the nodes that are selected as MPR generate and broadcast TC messages.

An individual OLSR packet can contain multiple HELLO or TC messages. All messages are uniquely identified by its originator address and message sequence number from the message header. The basic layout of an OLSR packet is shown in Figure 4.2

OLSR Packet Format

Packet Length	Packet Sequence Number

<table>
<tr><td>Message Type</td><td>Vtime</td><td>Message Size</td></tr>
<tr><td colspan="3">Originator Address</td></tr>
<tr><td>Time To Live</td><td>Hop Count</td><td>Message Sequence Number</td></tr>
<tr><td colspan="3">...
MESSAGE
...</td></tr>
<tr><td>Message Type</td><td>Vtime</td><td>Message Size</td></tr>
<tr><td colspan="3">Originator Address</td></tr>
<tr><td>Time To Live</td><td>Hop Count</td><td>Message Sequence Number</td></tr>
<tr><td colspan="3">...
MESSAGE
...</td></tr>
<tr><td colspan="3">....
(etc.)
...</td></tr>
</table>

Figure 4.1: OLSR packet format

4.3 Security and Integrity Protection Extensions

The proposed work correlates to the applied OLSR in a *Secure Conventional Meeting* like business issues discussion, Government issues discussion or some other secret discussion in a meeting room or Assembly Hall etc. As MANET belongs to open medium environment, hence all MANET applications are more prone to errors and attacks. A malicious node can easily intrude to the system for disturbing the communication. In wireless environment we need not only link level security but also require secure routing mechanism. The conventional meeting application in MANET requires strong security, simply over hearing of intruder can destroy the system. The OLSR protocol works very well in an ordinary environment for communication, but here we have to give strong attention so that its vulnerabilities never give a chance to the intruder system accessing. OLSR advertise control messages (Hello messages and TC messages) periodically in MANET. These messages give a chance to malicious user to enter to MANET. The aim of the proposal is to identify that how OLSR should advertise control messages, so that no unauthorized user becomes a part of meeting. A Case study shown in Fig 1, depicts the idea of research problem well. A malicious node is trying to become a part of the meeting members. To get control on this unauthorized action we propose a strong authentication scheme for Hello and TC messages exchange. We take an assumption that meeting team will be trusted, otherwise the system will prone to the following attacks:

- Identity spoofing to HELLO messages
- Link spoofing to HELLO messages
- Identity spoofing to TC messages
- Link spoofing to TC messages

MEETING HALL

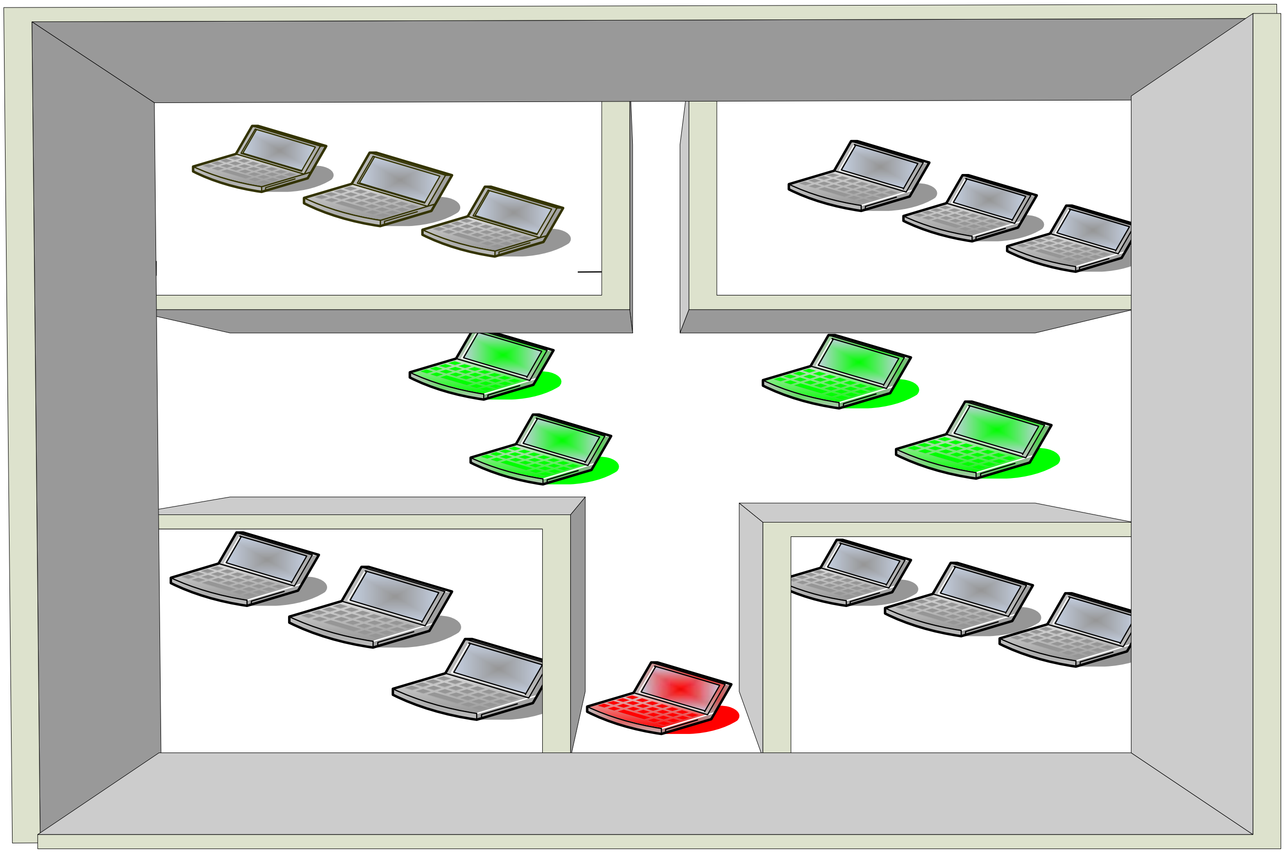


Figure 4.3: Problem description Case study

The main idea is the secure exchange of control messages; the exchange of control messages should follow the mechanism below.

First of all the trusted meeting members will request for unique *Global secret key* for confirmation of their trusted neighbors. After that meeting member should start controls messages like

❖ **HELLO messages include**

- Secure MAC value of HELLO SET (set of 1-hop neighbors). The MAC value should be generated by a secret share Hashing technique. e.g. chaining

- *Global secret key*, in order to sure that incoming HELLO messages is from trusted meeting member.

❖ **TC messages include**

- Secure MAC value of TC SET (set of MPR Selector). The MAC value should be generated by a secret share Hashing technique. e.g. chaining
- *Global secret key*, in order to ensure that incoming HELLO messages are from trusted meeting member.

Following the above mention rules, the communication of nodes in Figure 1 is given below:

HELLO messages of user 1, 2, 3 are shown below

$\mathit{HELLO}_{user\text{-}1}$(h(user-1, HELLO SET), Global Secret key, FF:FF:FF:FF:FF:FF)

h(user-1, HELLO SET) = $h_k(M)$ where k is secret key where h is hashing function

FF:FF:FF:FF:FF:FF = broad cast to 1-hop neighbors

$\mathit{HELLO}_{user\text{-}2}$(h(user-2, HELLO SET), Global Secret key, FF:FF:FF:FF:FF:FF)

$\mathit{HELLO}_{user\text{-}3}$(h(user-3, HELLO SET), Global Secret key, FF:FF:FF:FF:FF:FF)

Each user will define 1-hop neighbors from these HELLO messages and also find out 2-hop neighbors as well by comparing HELLO SET of incoming HELLO message and finally select their MPR also. The malicious node can’t become a trusted meeting member as in advance, it will fail by sharing Global Secret key to its neighbors. But suppose the Malicious node prepares an invalid HELLO packet and sends it to one of meeting member, the packet should be directly discarded and warning alarm will be started node will inform the entire MAMET network about the false hello message , as any incoming HELLO message is first authenticated with Secret key *k*. A MAC, also known as a cryptographic checksum, is generated by a function C. The MAC is appended to the message at the source at a time when the message is assumed or known to be correct. The receiver authenticates that message by re-computing the MAC.

The MAC function is a many-to-one function, since potentially many arbitrarily long messages can be condensed to the same summary value, but don’t want finding them to be easy! The information mechanism will be described during the thesis.

TC messages of MPR

$\mathrm{TC}_{\mathrm{MPR}}$ (h(MPR, TC SET), Global Secret key, MPR) here h(MPR, TC SET) = MAC secret key where h is hashing function. The malicious node will again fail to attack on MPR because of the Global Secret key absence.

Chapter 5

OLSR Vulnerabilities and New Security Extensions to OLSR

MANET application environments such as the battlefield or law enforcement situations are exposed to more threats than other environments such as electronic classrooms. A MANET node may be easily compromised if captured in the battlefield. Due to the open medium environment in a MANET, an intruder can join in the routing process without any attaching point. Dynamic membership and topology due to mobility are also big holes for security. To favor mobility and lower bandwidth, as well as lower computing power in the MANET, the OLSR protocol design achieves optimization, as mentioned in Section 2, over LSR through the use of MPR nodes. However, it also loses a security advantage that LSR has the fight-back feature. This feature makes LSR robust to malicious attacks and more promising for detecting faults; each router floods its local connectivity to every other router, and each router receives the connectivity information from all other nodes and has the complete topology information for the whole network. In OLSR, only the connectivity used as routing computation (the connectivity to those MPR selectors) is flooded in the whole network. The fight-back feature is lost in OLSR because of the optimization required to tailor to a MANET environment. As the existing IETF's RFC on OLSR does not specify validation procedures and security mechanisms, numerous opportunities exist for intruding OLSR nodes to launch attacks. Malicious attacks to routing protocols can be cataloged as invalid update messages and router overload (Denial Of Service). DOS attacks are not strictly a routing protocol issue. This paper focuses on invalid update messages in an OLSR MANET. Neighbor nodes know each other by exchanging HELLO messages, which reflect the local connectivity and are used to select the MPRs for routing connectivity. The TC message is different from the Link-State Advertisements (LSA) message because it propagates only partial local connectivity of MPR selectors instead of complete local connectivity of all neighbors. In order to support routing in MANET, a MANET node normally takes two responsibilities: generating control messages and forwarding control messages. To compromise the integrity of the routing protocol, an active attacker can send incorrect control packets while the MANET node is generating control messages, or alter control packets while the MANET node is forwarding control messages. Furthermore, there are two ways to tamper with a control message: change its identity (identity spoofing) or damage its contents (link spoofing). The following paragraphs catalog various attacks and describe them in detail.

5.1 Change Identity in HELLO Message (identity spoofing)

Some time an intruder spoofs identity of an ordinary MANET's node as its source address and send HELLO messages to its neighbors through that spoof identity. In this way intruder neighbors select wrong decision of being packet transmitting to its MPR. Figure 5.1 shows how the topology's image of a

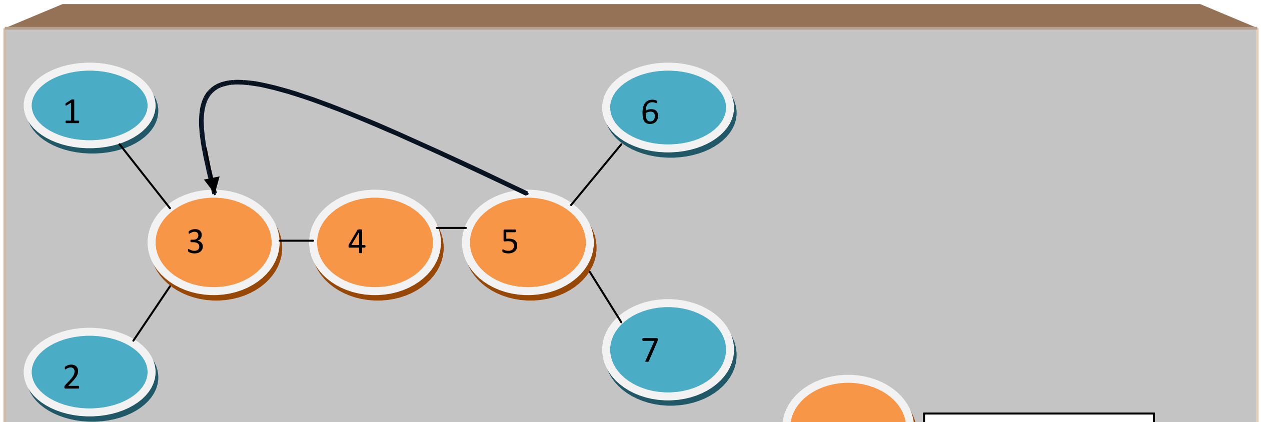


Figure 5.1: Node 5 spoofs identity of Node 3 in its HELLO message

MANET is distorted when Node 5 impersonates Node 4. Node 6 and 7, select Node 3 as their MPR. Traffic to Node 6 or Node 5 will be sent to Node 3, which is believed to be the last hop to Node 6 or Node 7, then lost at Node 3 because Node 3 does not have Node 6 or Node 7 in its neighborhood.

5.2 Change Contact in HELLO Message (link spoofing)

In this situation non existing neighbors masquerades as others existing neighbors or falsifying data of the neighbor's causes to the damage of the HELLO packets. In such situation attacker neighbors can disturb the MPR selection mechanism and increase the possibility of malicious to select as MPR. Once the intruder becomes MPR, then he gets the authority to manipulate the traffic, deleting and disable neighbors which can cause the unreachable to those neighbors.

5.3 Change Identity in TC Message (identity spoofing)

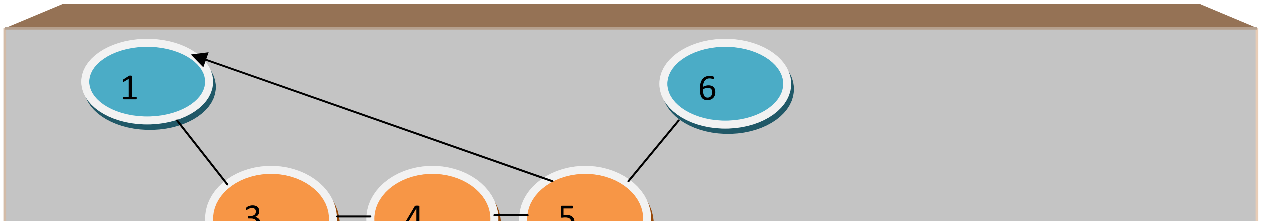


Figure 5.2: Node 5 spoofs identity of Node 1 in its TC message

In this case malicious spoof identities of MANET’s node IP address and propagate TC messages through that address as source node. In this manner, intruder neighbor selects wrong node as its last hop node for packet transmission. As Figure 5.2 shows, Node 5 is selected as the MPR by Node 6 and Node 7, and Node 5 is supposed to send a TC message to propagate that Node 5 is the last hop to Node 6 and 7. Instead of sending a correct TC message, Node 5 spoofs Node A’s IP address in its TC message. The attack results in a distorted topology as shown in Figure 5.2. Traffic to Node 6 or 7 is delivered to Node A.

5.4 Change Contact in TC Message (link spoofing)

Change contact in TC message (link spoofing) refers to injecting fictional MPR selectors or disabling offered MPR selectors. In case of disabling offered MPR selectors some MPRs selectors well come in the state of unreachable in OLSR network as well as the nodes which are connected to those Offered selectors are unable to participate in further communication with other nodes. While in case of Injecting fictional MPR selectors creates unacceptable channels to those MPR selectors from TC message originated node.

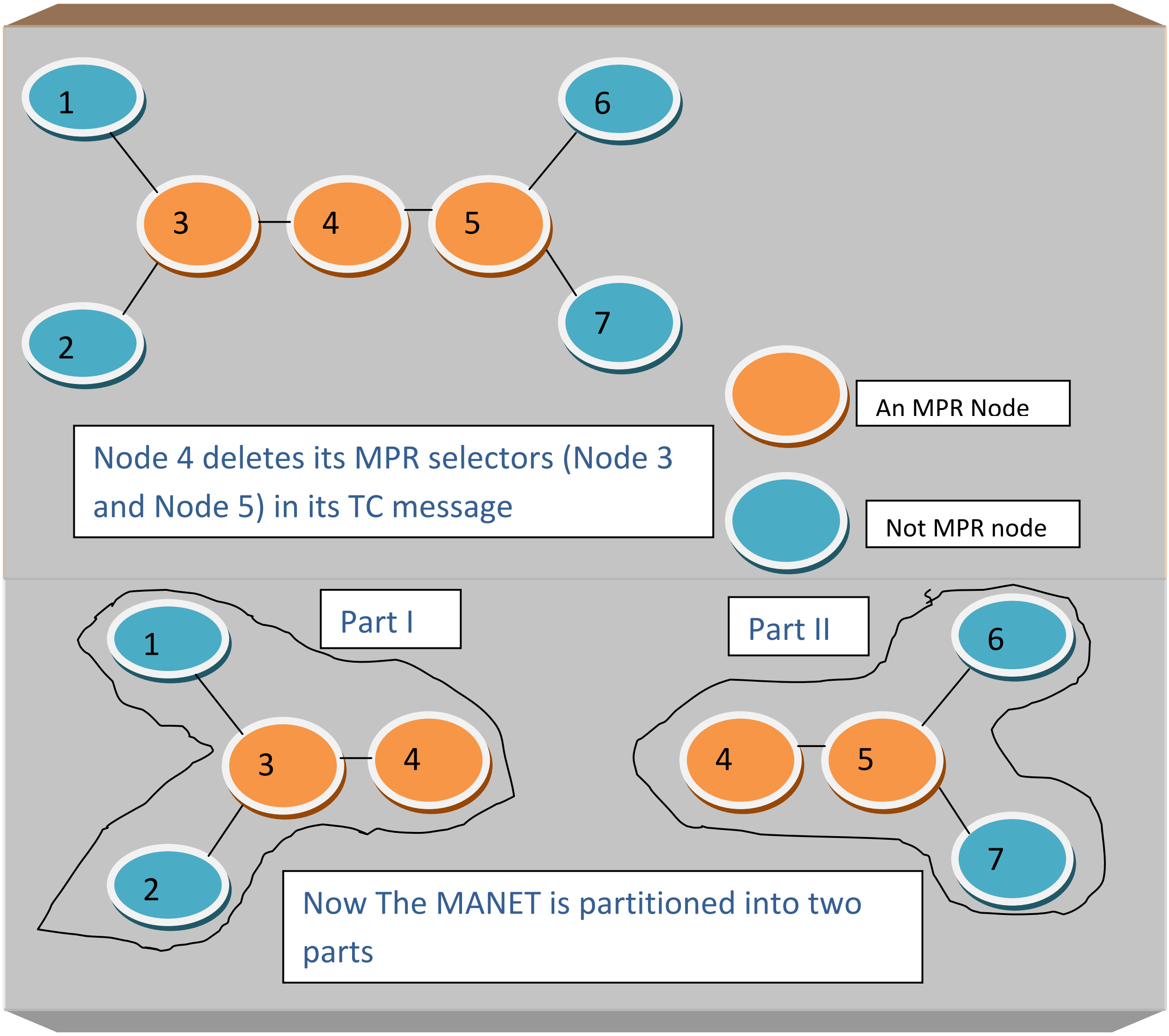

1
6
3
4
5
2
7
An MPR Node
Not MPR node
Node 4 deletes its MPR selectors (Node 3 and Node 5) in its TC message
Part I
Part II
1
3
4
2
4
5
6
7
Now The MANET is partitioned into two parts

Figure 5.3: Node 4 deletes its MPR selectors (Node 3 and Node 5)

5.5 Replay Attacks

One type of attack on MANET is replay attack on network connection to repeat the valid data transmission. In replay attacks basically an attacker copies a specific stream of transmitted messages between two nodes and replays the data stream to one or more of the nodes.

5.5 Secure Optimized Link State Routing Protocol SOLSR

As a countermeasure, to get control on this unauthorized action we propose a strong authentication and encryption scheme for Hello and TC messages exchange. So we employ Global Secret Key Global secret key, in order to sure that incoming HELLO messages and TC messages is from trusted meeting members and MAC algorithm for the authentication of control message follow by encryption for message secrecy. Only the authentication checks on the information message cannot prevent the replay attacks in MANET environment. So we developed a timestamp approach to avoid replay attacks. Hence we have tried to protect the network from the above attacks with the help of these security checks.

5.5.1 Overview of OLSR Secure Routing Checks

In this part, the overview of the security checks for the attacks declared within Section 5.5 is described.

5.5.1.1 Nodes authentication

In the environment of ad hoc Network we employ nodes authentication when nodes try to tie with the Ad hoc network. To execute nodes authentication function, it raises one of key issues which node or nodes authenticate a new connecting device or node. Because MANET is a decentralized style of network, there is no availability of a fixed station for authentication. So we decided that directly connected nodes authenticate each other before the communication. We employ Global secret key for nodes authentication. Neighbor's nodes authenticate each other using global secret key. Global secret key is basically a public key cryptosystem. Furthermore, nodes re-authenticate each other from time to time and confirm the completeness of a node because MANET nodes are movable.

5.5.1.2 Authentication and Encryption of Hello and TC Messages

In MANET security framework it is assumed that the secrecy and integrity (i.e. protection from modification) of a trusted node is not compromised as well as corroborating the identity of the sender. So only the trusted nodes traffic is allowed in Ad hoc Network. The HELLO messages and Topology control messages are cryptographically signed. In this environment MAC provide the authentication while encryption provides secrecy. We can use the combination of MAC with encryption in various ways to provide both authentication & secrecy of message and nodes as well. We use MAC in Such circumstances where just authentication is needed. As we know that

MAC is not a digital signature so both the sender & receiver share key among each other and could create it.

5.5.1.3 Timestamp approach to prevent replay attack

As we already discussed in section IIB that authentication does not prevent replay attacks. So till up to now two methods are use to avoid the replay attacks one is session tokens and the other is timestamping. In session tokens method one-time token is use for the avoiding of replay attacks. This one-time token expires after it has been used. Timestamp method is a different way to avoid replay attacks. In this method synchronization should be attained using a secure protocol. A distributed timestamp approach is used to gain this synchronization.

5.5.2 Implementation of Secure Routing Checks

We identified the secure routing checks declared in section 5.5. This section explains each check in detail and with a practical scenario.

5.5.2.1 System Specification and Configuration

Figure 4.3, figure 5.4 and table 5.1 shows the scenario, secure routing checks and the system specification of OLSR software embedded nodes (laptops) in a Secure Conventional Meeting like business issues discussion, Government issues discussion or some other secret discussion in a meeting room or Assembly Hall etc. over all communication is based on TCP/IP. The conventional meeting application in MANET requires strong security, simply over hearing of intruder can destroy the system. The OLSR protocol works very well in an ordinary environment for communication, but here we have to give strong attention so that its vulnerabilities never give a chance to the intruder system accessing. OLSR advertise control messages (Hello messages and TC messages) periodically in MANET. These messages give a chance to malicious user to enter to MANET. The aim of this research is to identify that how OLSR should advertise control messages, so that no unauthorized user becomes a part of meeting. In figure 4 a malicious node (laptop with red color) is trying to become a part of the meeting members. To get control on this unauthorized action we propose a strong authentication scheme for Hello and TC messages exchange. We take an assumption that meeting team will be trusted, otherwise the system will prone to the vulnerabilities stated within chapter 4 & 5.

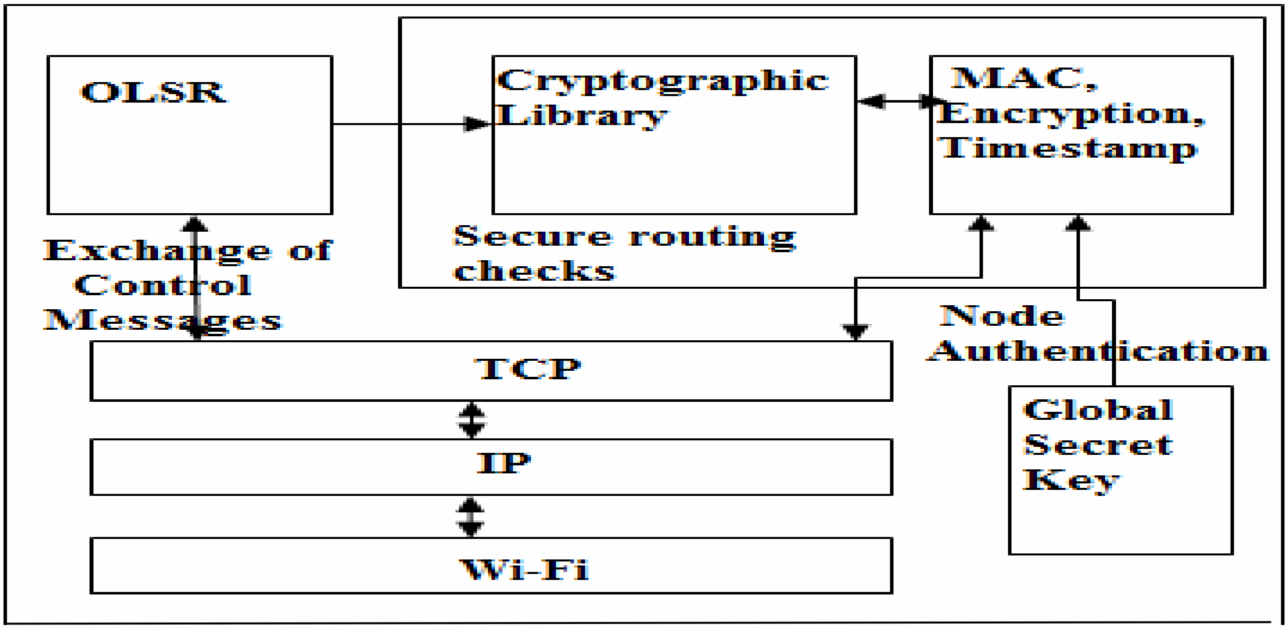


Figure 5.4: OLSR Node Configuration

Table 5.1: Specification of a node

Component	**Name/Version**
Routing Software	OLSR
Operating System	Linux Red Hat 9.0
Wireless I/F	IEEE 802.11b
Cryptographic Library	Botan OpenCL

5.5.2.2 Global Secret Key

In secret conventional meeting authentication process starts when a node receives a HELLO message from another 1-hope neighbor node or receives a TC message from 2-hope neighbor node, at that time the secure routing checks called by the OLSR process and starts mutual authentication process. At the same time if the node gets another Hello message or TC message, just discards the message. If a Hello or TC message from the node which previously failed 3 times in authentication is received, it will also be discarded. Only is that case the completeness of a control message is verified when a control message from trusted or authenticated node is received.

For the secret conventional meeting the authentication process is based on Global secret key. Global secret key is basically a secret text string shared between the trusted members of secure conventional meeting. The length of the key is limited from 8 to 63 characters and can contain any printable ASCII characters but spaces are not allowed. We can configure a global secret key for all MANET devices to use. One node creates a Global secret key, and distributes it to the entire MANET. In key updating process, old Global Secret key is used until a Global secret key is distributed to all trusted neighbor nodes. During the authentication process the key will be transferred in encrypted form, figure 5.5 shows the public key cryptosystem for key exchange during node authentication. Re-authentication process performs after a specific time interval. Global secret key is the best solution for the link spoofing, if an intruder spoofs identity like IP address of a MANET node cannot communicate until the node proves itself a trusted node with the help of global secret key.

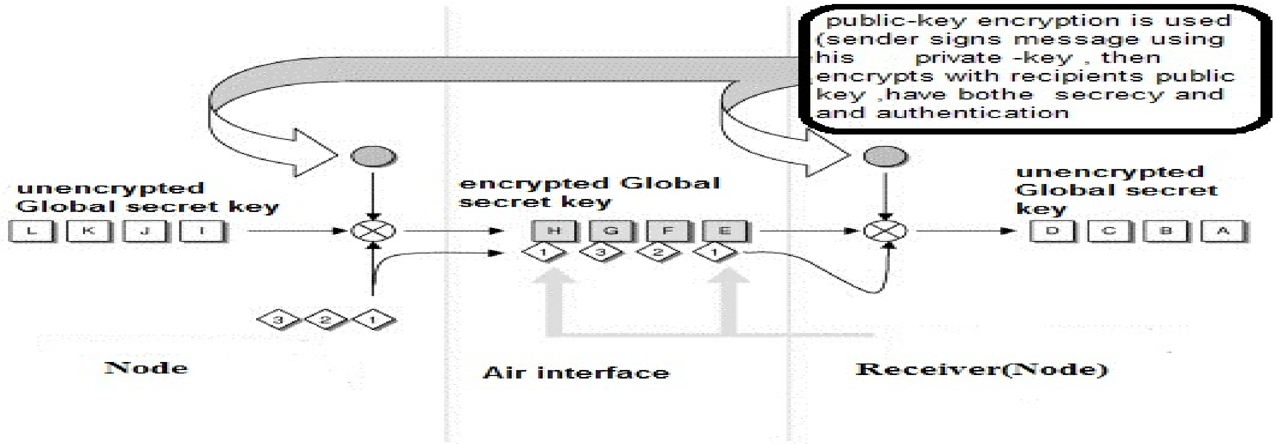

public-key encryption is used (sender signs message using his private -key , then encrypts with recipients public key ,have bothe secrecy and and authentication
unencrypted Global secret key
L
K
J
I
3
2
1
encrypted Global secret key
H
G
F
E
1
3
2
1
unencrypted Global secret key
D
C
B
A
Node
Air interface
Receiver(Node)

Figure 5.5: Secure key transformation during node authentication

5.5.2.3 Control Message Authentication and Encryption

Public key encryption cannot provide confidence of sender and integrity of message. Therefore for secure conventional meeting control message authentication offers the integrity of message. Change contact in HELLO message and TC message are banned by using MAC that is appended to message as a signature and encryption created for secrecy by the originator of each OLSR HELLO and topology control message and transmitted with the HELLO and TC message. MAC can be computed either before or after the control message encryption. Figure 5.6 shows the use of a MAC for authentication.

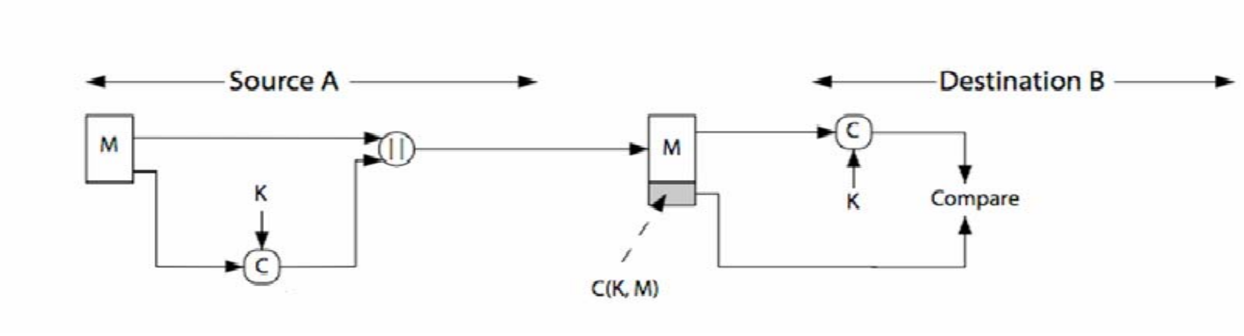


Figure 5.6: Message Authentication

The message prototype which is used to append and encrypt new messages is shown in figure 5.7.

HEADER 4 bytes
Control Message Variable Length
……………………..
MAC 8 bytes
Encryption 8 bytes
Timestamp 4 bytes

Figure 5.7: General secure Message format for OLSR

5.5.2.4 Timestamp

The timestamp is thought to avoid replay attacks, as the Node can authenticate a message is fresh. For example Bob sends periodically broadcasts the timestamp (time on his clock) together with a MAC. On the other hand when Alice desires to send Bob a message, Alice includes her best estimate Timestamp in her message. Bob only acknowledges messages for which the timestamp is within a reasonable acceptance when Alice desires to send Bob a message; actually timestamp approach is used to validate whether a message is old or new to avoid replay attack. The advantage of this scheme over one-time token is that Bob does not call for to generate pseudo-random codes so that why we used timestamp to decrease the working overload at the receiving side. Figure 5.7 shows OLSR control message with timestamp approach.

5.5.3 Summary

This chapter presents a secure design for online secret conventional meeting which consists of Global Secret key, control message authentication and encryption and timestamp approach. These three functions are added for the purpose of forming a SOLSR protocol for MANET application like secure conventional meeting. OLSR is a cluster base routing protocol for information exchange in MANET. This protocol exchange control messages with neighbors frequently, the research has purposed to avail security in exchanging the messages, so that no malicious user could become a part of the meeting session.