SECURITY IN MOBILE AD HOC NETWORKS

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Computer Science & Engineering

By:
Tirthraj Rai
(80732025)

Under the supervision of:
Dr. A. K. Verma
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

MAY 2009

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Security in Mobile Ad Hoc Networks"**, in partial fulfilment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. A. K. Verma.*

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Tirthraj Rai

(Tirthraj Rai)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. A. K. Verma)
Assistant Professor
Computer Science & Engineering Department
Thapar University, Patiala

Countersigned by:

(HEAD) 24/06/09
Computer Science & Engineering Department,
Thapar University,
Patiala.

(R. K. Sharma) 25/6/09
Dean (Academic Affairs)
Thapar University
Patiala.

Acknowledgement

No volume of words is enough to express my gratitude towards my guides, ***Dr. Anil Kumar Verma****, Assistant Professor, Computer Science and Engineering Department, Thapar University, who has been very concerned and has aided for all the material essential for the research work and preparation of this thesis report. He helped me to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research-oriented venture.*

I am also thankful to ***Dr. Rajesh Bhatia,*** *Assistant Professor and Head, CSED,* ***Dr. (Mrs.) Seema Bawa,*** *Professor and* ***Dr. (Mrs.) Inderveer Channa****, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.*

I would also thankful to my brother ***B. R. Rai,*** *and my friends* ***Amit, Arindam*** *and* ***Manoj*** *to help me.*

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my ***Parents*** *and the* ***Almighty*** *for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.*

Tirthraj Rai

Tirthraj Rai

80732025

Abstract

Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. Each node participating in the network acts both as host and a router and must therefore is willing to forward to packets for other nodes. The characteristics of MANETs such as: dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability of that make it completely different from other network. Due to the nature of MANETs, to design and development of secure routing is challenging task for researcher in an open and distributed communication environments.

The main work of this thesis is to address the security issue, because MANETs are generally more vulnerable and we proposed a secure routing protocol for MANETs, are named ASRP (Authenticate Secure Routing Protocol) based on DSDV. This protocol is work on various modes; each mode corresponds to specific state of the node. This protocol is design to protect the network from malicious and selfish nodes. We are implementing Extended Public key Cryptography mechanism in ASRP in order to achieve security goals.

Keywords: - MANETs, Security, Cryptography.

Table of Contents

List of Figures

List of Tables

CHAPTER 1
Introduction

1.1 Motivation

Wireless cellular system has been in use since 1980s. Wireless system operates with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to other. In wireless system the device communicate via radio channel to share resource and information between devices. Due to presence of a fixed supporting structure, limits the adaptability of wireless system, so this generation of wireless system is required easy and quick deployment of wireless network. Recent advancement of wireless technologies like Bluetooth [3], IEEE 802.11 [4] introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) [1, 2, 5, 6], which operate in the absence of central access point. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time.

Mobile ad hoc network consist large number of node, it form temporary network with dynamic topology. In this network each node communicates with each other through radio channel without any central authority. In MANETs each node operates in a distributed peer-to-peer modes [2], serves as an independent router to forward message sent by other nodes. MANETs has shows distinct characteristics, such as:

- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

Apart from these limitation MANETs has many extensive application like: Military application, Natural disaster, Medical service.

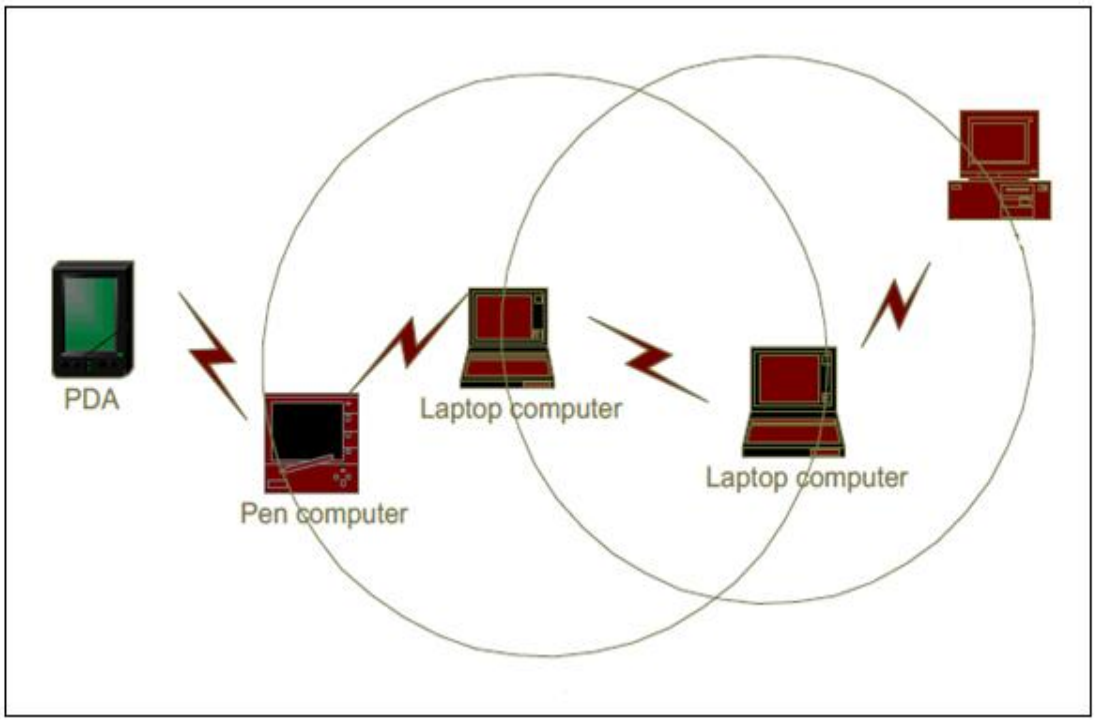


Figure 1.1 Infrastructureless Networks

In ad hoc network there can be node that will try to disrupt the proper functioning network. These nodes can be malicious or selfish [8]. They try to disrupt network function by modifying packets, injecting packets or creating routing loops. So, security is an important task, because MANETs has characteristics such as; dynamic topology, infrastructure less. There are large numbers of secure routing protocols proposed by many researchers they fulfill different security requirements and prevent specific attacks. They are divided into three categories: Reactive routing protocol [5, 6], Proactive routing protocol [5] and hybrid routing protocol [6]. In reactive routing protocol the route is discovered when it required, in proactive each node maintain network information regarding to network connectivity and route information to all others node within the network and proactive is one which is neither reactive nor proactive.

Now, the Most of the solution uses cryptography mechanism to detect selfish, malicious behavior of nodes and securing information from other types of attacks. The mechanisms which are used by different secure routing protocol to detect malicious and selfish node have address separately in different protocol. No secure mechanism has been proposed till date

that can address to detecting malicious and selfish node collectively. We proposed a mechanism, Extended Public key Cryptography (EPKCH) [12, 13] that able to detect the malicious nodes and selfish nodes collectively in order to achieving security goals such as; Authentication, Integrity, Confidentiality and Non-Repudiation. Also, we proposed a routing protocol named Authenticate and Secure Routing protocol for mobile Ad hoc Network (ASRP). We implemented EPKCH mechanism in monitor mode of ASRP to securing MANETs. To design of this protocol follows the table-driven approach, in which each node maintain the information, regarding to network structure and route from a particular source to its all possible destination in its node info table. ASRP is a proactive secure routing protocol.

1.2 Purpose

The secure protocol design and development has become the most challenging task in securing mobile ad hoc network. Most of the existing protocol has been develop based on specific security scenarios. So the main purpose of this research is to understand and evaluate the existing secure protocol and implement a secure protocol which is not address the solution for particular security (attacks) but it is prevent different kind of security scenarios.

1.3 Thesis Outline

We have organized the thesis into 6 chapters. Chapter 2, are the literature review related mobile ad hoc network, security goals, types of attacks on MANETs and some secure solutions based on cryptography schemes. In chapter 3 discuses the problem statement. In chapter 4 we proposed a mechanism for securing MANET and its operation. We present ASRP in chapter 5, description of protocol, activity of nodes, working pattern, structure of various packet forwarding during network initialing mode and packet forward mode of nodes. Chapter 6 summarizes the conclusions drawn in the thesis along with future research.

CHAPTER 2

Literature Review

2.1 Mobile Ad hoc Networks

2.1.1 Introduction

The area of mobile ad hoc networking deals with devices equipped to perform wireless communication and networking, but without any existing infrastructure such as base stations or access points. Wireless devices form a network as they become aware of each other's presence. 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 [1, 2, 5]. Networks are formed on-the-fly, devices can leave and join the network during its lifetime, devices can be mobile within the network, the network as a whole may be mobile and the network can be deformed on-the-fly. Devices in mobile ad hoc networks should be able to detect the presence of other devices and perform the necessary set-up to facilitate communications and the sharing of data and services.

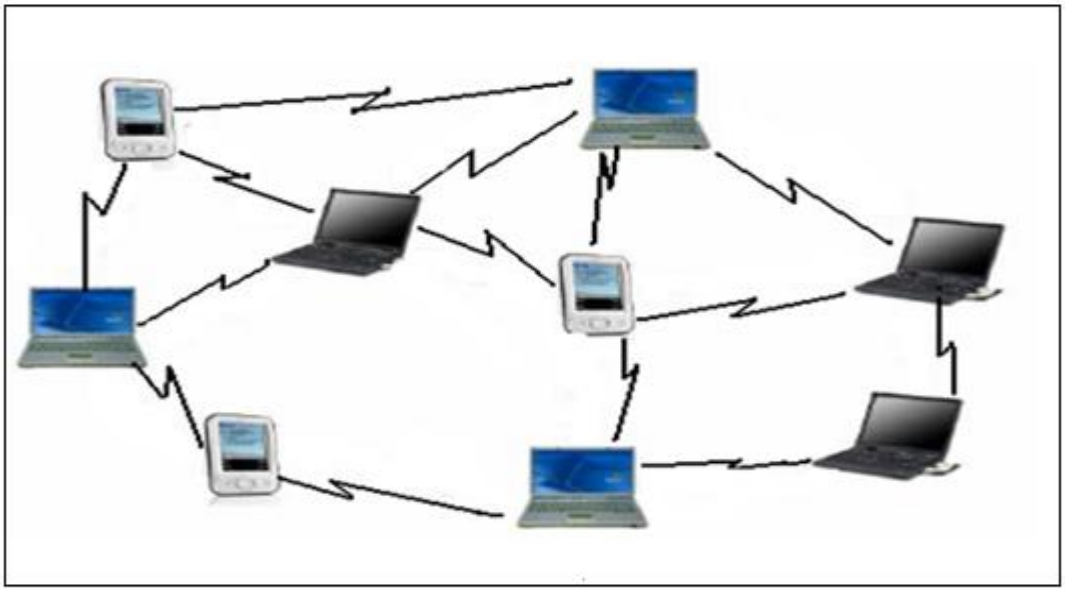


Figure 2.1 MANETs Operation

2.1.2 Features

A mobile ad hoc network has following features:

Autonomous Terminal

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other, since there is no background network words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

Distributed Operation

For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

Multihop Routing

Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes

Dynamic Network Topology

Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly.

Light-weight Terminal

In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

2.1.3 Characteristics

MANETs are new paradigm of networks, offering unrestricted mobility without any underlying infrastructure. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Following are the characteristics of a MANET [2, 7]:

Dynamic Topologies

Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

Energy Constrained Operation

Almost all the nodes in an ad hoc network rely on batteries or other exhaustive means for their energy. The battery depletes due to extra work performed by the node in order to survive the network. Therefore, energy conservation is an important design optimization criterion.

Bandwidth Constraint

Wireless links have significantly lower capacity [47] than infrastructures networks. Throughput of wireless communication is much less because of the effect of the multiple access, fading, noise, interference conditions. As a result of this, congestion becomes a bottleneck in bandwidth utilization

Limited Physical Security

MANETs are generally more prone to physical security threats than wireless networks because the ad hoc network is a distributed system and all the security threats relevant to such a system are pretty much present, as a result, there is an increased possibility of eavesdropping, spoofing, masquerading [30], and denial-of- service type attacks.

2.1.4 Applications [5]

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread applications. Ad

hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. It includes:

- Military Battlefield
- Sensor Networks
- Commercial Sector
- Medical Service
- Personal Area Network

2.2 Routing in MANETs

Routing in mobile ad hoc networks faces additional problems and challenges when compared to routing in traditional wired networks with fixed infrastructure. There are several well-known protocols [31,32] in the literature that have been specifically developed to cope with the limitations imposed by ad hoc networking environments. The problem of routing in such environments is aggravated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth and high error rates [26]. Most of the existing routing protocols follow two different design approaches to confront the inherent characteristics of ad hoc networks, namely the table-driven and the source-initiated on-demand approaches. The following sections analyze in more detail these two design approaches, and briefly present example protocols that are based on them.

2.2.1 Table-driven Ad hoc Routing Protocols

Table-driven ad hoc routing protocols maintain at all times routing information regarding the connectivity of every node to all other nodes that participate in the network. Also known as proactive, these protocols allow every node to have a clear and consistent view of the network topology by propagating periodic updates [26]. Therefore, all nodes are able to make

immediate decisions regarding the forwarding of a specific packet. On the other hand, the use of periodic routing messages has the effect of having a constant amount of signaling traffic in the network, totally independent of the actual data traffic and the topology changes. As an example of two protocols that follow the table-driven design approach we will briefly present the Destination-Sequenced Distance-Vector (DSDV) protocol [19] and the Optimized Link State Routing (OLSR) protocol [27].

2.2.1.1 Destination-Sequenced Distance-Vector Routing (DSDV)

DSDV is a table-driven routing protocol based on the Bellman-Ford algorithm [25]. The DSDV protocol can be used in mobile ad hoc networking environments by assuming that each participating node acts as a router. Each node must maintain a table that consists of all the possible destinations. In more detail, an entry of the table contains the address identifier of a destination, the shortest known distance metric to that destination measured in hop counts and the address identifier of the node that is the first hop on the shortest path to the destination [19]. Furthermore, the DSDV protocol adds a sequence number to each table entry assigned by the destination node, preventing the formation of routing loops caused by stale routes. The routing tables are maintained by periodically transmitted updates by each router to all the neighboring routers.

2.2.1.2 Optimized Link State Routing (OLSR)

The Optimized Link State Routing (OLSR) protocol is a proactive link state routing protocol based on the Open Shortest Path First (OSPF) protocol [28]. OLSR has been specifically developed to support mobile ad hoc networks and the constraints they impose on routing. The OLSR protocol can be conceptually divided into three different operations, namely neighbor sensing, distribution of signaling traffic and distribution of topological information [27]. Neighbor sensing in OLSR is accomplished by transmitting periodic hello messages that contain the generating node's address identifier, a list of its neighboring nodes and the type of the link it has with each neighbor (e.g.: symmetric or asymmetric). For the distribution of signaling traffic OLSR adopts a flooding mechanism where every node forwards a flooded message that it has not forwarded previously. Finally, the distribution of topological information function is realized with the use of periodic topology control

messages that result in each node knowing a partial topology graph of the network which is then used for the computation of optimal routes [24, 26].

The Table 2.1 and Table 2.2 outline the basic characteristics and complexity of two routing protocols discussed above.

Table 2.1 Basic Characteristics of DSDV and OLSR

Protocol	Routing Structure	Number of Table	Critical Nodes	Characteristics Feature
DSDV	Flat	2	No	Loop Free
OLSR	Flat	4	No	Loop Free

Table 2.2 Complexity Comparison of DSDV and OLSR

Protocol	Convergence Time	Memory Overhead	Control Overhead	Advantage/Disadvantage
DSDV	O(Diameter of network-1)	O(Number of node in the network)	O(Number of node in the network)	Loop Free/Higher overhead
OLSR	O(Greater than the diameter of routing tree)	O(Number of node in the network)^2	O(Number of node in the network)	Loop Free/ Low overhead than DSDV

2.2.2 Source-initiated On-demand Ad hoc Routing Protocols

An alternative approach to the one followed by table-driven protocols is the source initiated on-demand routing. According to this approach a route is created only when the source node requires one to a specific destination. A route is acquired by the initiation of a route discovery function by the source node. The data packets transmitted while a route discovery is in process are buffered and are sent when the path is established. An established route is maintained as long as it is required through a route maintenance procedure. The Ad hoc On-demand Distance Vector (AODV) routing protocol [17] and the Dynamic Source Routing protocol [18] are examples of this category of protocols also known as reactive

2.2.2.1 Ad hoc On-demand Distance Vector Routing (AODV)

The AODV protocol uses route request (RREQ) messages flooded through the network in order to discover the paths required by a source node. An intermediate node that receives a

RREQ replies to it using a route reply message only if it has a route to the destination whose corresponding destination sequence number is greater or equal to the one contained in the RREQ [17]. This effectively means that an intermediate node replies to a RREQ only if it has a fresh enough route to the destination. Otherwise, an intermediate node broadcasts the RREQ packet to its neighbors until it reaches the destination. The destination unicast a RREP, back to the node that initiated the route discovery by transmitting it, to the neighbor from which it received the RREQ.

2.2.2.2 Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is based on a method known as source routing [18]. The route discovery process in DSR is similar to the one used by AODV, except that each intermediate node that broadcasts a route request packet adds its own address identifier to a list carried in the packet. The destination node generates a route reply message that includes the list of addresses received in the route request and transmits it back along this path to the source. Route maintenance in DSR is accomplished through the confirmations that nodes generate when they can verify that the next node successfully received a packet. These confirmations can be link-layer acknowledgements, passive acknowledgements or network-layer acknowledgements specified by the DSR protocol. When a node is not able to verify the successful reception of a packet it tries to retransmit it. When a finite number of retransmissions fail, the node generates a route error message that specifies the problematic link, transmitting it to the source node.

Tables 2.3 and 2.4 outline the basic characteristics and complexity of the two routing protocols discussed in this section.

Table 2.3 Basic Characteristics of AODV and DSR

Protocol	**Multiple Route**	**Route Metric Method**	**Route Maintenance In**	**Route Reconfiguration Strategy**
AODV	No	Freshest and shortest path	Route Table	Erase Route then Source Notification or Local
DSR	Yes	Shortest path or next path available	Route Cache	Erase Route then Source Notification.

Table 2.4 Complexity Comparison of AODV and DSR

Protocol	Time Complexity for Route Discovery	Time Complexity for Route Maintenance	Advantage	Disadvantage
AODV	O(2*Diameter of network)	O(2*Diameter of network)	Adaptable to highly dynamic topologies.	Scalability Problems and large Delays
DSR	O(2*Diameter of network)	O(2*Diameter of network)	Multiple Routes, Promiscuous overhearing	Scalability problem due to source routing and flooding.

2.3 Security Problem with Existing Ad hoc Routing Protocols

The main assumption of the previously presented ad hoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the protocol [19, 29]. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. In ad hoc network the routing function can be disrupted by internal or external attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes [14]. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Internal attackers having capability to complete access the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers [23].

2.4 Security Goals

In providing a secure networking environment some or all of the following service may be required [15, 16]

2.4.1 Authentication: This service verifies the identity of node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is

possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANET, and it is much more difficult to authenticate an entity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates.

2.4.2 Confidentially: Keep the information sent unreadable to unauthorized users or nodes. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data, and another technique is to use directional antennas. It also ensures that the transmitted data can only be accessed by the intended receivers.

2.4.3 Integrity: Ensure that the data has been not altered during transmission. The integrity service can be provided using cryptography hash function along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

2.4.4 Availability: Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocol.

2.4.5 Non-repudiation: Ensure that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message.

2.4.6 Access Control: To prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

2.5 Vulnerability in MANETs

Malicious and selfish nodes are the ones that fabricate attacks [70, 14] against physical, link, network, and application-layer functionality. Current routing protocols are exposed to two types of attacks:

- Active attacks
- Passive attacks

Table 2.5 Classification of Security Attacks

Active attacks	Spoofing, Fabrication, Wormhole Attack, Modification, Denial of Service
Passive Attacks	Eavesdropping, traffic analysis, monitoring

2.5.1 Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. These attacks can be classified into further following types.

Spoofing: Occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather [2].

Fabrication: The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [5].

Wormhole Attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols [21].

Modification: The attacker performs such attacks is targeted to integrity of data, by altering packet or modifying packets.

Denial of Service: This active attack [48] aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks.

2.5.2 Passive Attacks

In passive attacks the attacker does not perturb the routing protocol, instead try to extract the valuable information like node hierarchy and network topology from it. Passive attack is in nature of eavesdropping on, or monitoring of, transmission. The goal of opponent is to obtained information that is being transmitted [5]. Passive attacks are very difficult to detect because they do not involve any alteration of data.

2.5.3 Other Advanced Attacks

We will now discuss several specific attacks that can affect the operation of a routing protocol in ad hoc network.

Blackhole attack: In a black hole attack a malicious node advertising itself as having a valid route to the destination. With this intension the attacker consume or intercept the packet without any forwarding [8]. An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped.

Byzantine attack: A compromised with set of intermediate, or intermediate nodes that working alone within the network carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services within the network [9].

Rushing attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack [21]. The rushing attack can act as an effective

denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne [22].

Replay attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [8].

Location disclosure attack: An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques [10], or with simpler probing and monitoring approaches [14]. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.

2.6 Secure Ad hoc Routing

There exist several proposal that attempt to architect a secure routing protocol for mobile ad hoc network [31, 32], in order to offer protection against the attacks mentioned in the previous section. There are several solutions proposed by researcher they are either completely new stand-alone protocol or in some cases incorporation of security mechanism into existing one like DSDV [19] and AODV [17]. Since routing is an essential function for ad hoc networks, the integrated security procedures should not hinder its operation. Another important part of analysis is the examination of assumption and the requirements that each solution depend on. Although a protocol might be able to satisfy certain security constraints, its operational requirements might thwart its successful employment. In order to analyze exiting solution in structure way we have classified them into three categories; Solution based on Symmetric cryptography, solution based on Asymmetric cryptography and Hybrid solution. However, this classification is only indicative since a lot of solution can be classified into more than one category.

2.6.1 Symmetric Cryptography Solutions

2.6.1.1 SEAD [20]

The Secure Efficient Ad hoc Distance Vector (SEAD) is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector (DSDV) [19] algorithms. To developing SEAD, follow the table driven approach. In table driven routing protocol maintain at all times routing information regarding to the network connectivity of every node to all other nodes. It is also known as proactive routing protocol. In order to find shortest path between two nodes, the distance vector routing protocol utilize a distributed version of Bellman Ford Algorithm [19]. The SEAD routing protocol employ the use of hash chains to authenticate hop count and sequence numbers.

Applying repeatedly a one-way hash function to a random value creates hash chain. The element of such hash chain is used to secure the updates of the routing protocol. The SEAD routing protocol proposed two different methods in order to authenticate the source of each routing updates. The first method require clock synchronization between nodes that participate in the network and the second method require the existence of shared secrete between each pair of nodes.

SEAD deals with attacks that modify routing information broadcasted during the updates phase of DSDV protocol: in particular, routing can be disrupted if the attacker modifies the sequence number and the metric field of routing table updates message.

SEAD is prone through wormhole attack. Even if authentication is provided using hash functions, a wormhole attack is possible through tunneling the packets from one location and retransmitting them from other location into the network. All packets in the wormhole attack flow in a circle around instead of reaching the destination. Spoofing attack is possible through compromised node acting like a destination node in the route discovery process by spoofing the identity of the destination node that can cause route destruction. Blackhole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Tunneling and DOS attacks are also possible through compromised nodes. Table driven protocols are much more prone to security threats

2.6.1.2 SRP [23]

Secure Routing Protocol (SRP) [23] was developed based on Destination Source Routing protocol (DSR) [19]. The operation of SRP requires the existence of a Security association (SA) between source node initiating a route query and the destination node. The security association can be utilized in order to establish a shared secret key between the two nodes, which is used by SRP. The SRP protocol appends a header (SRP header) to the packet of the basic routing protocol. The source node sends a route request with a query sequence number (QSEQ) that is used by the destination in order to identify outdated requests, a random query identifier (QID) that is used to identify the specific request. The intermediate nodes broadcast the query to their neighbors, after updating their routing tables.

The entire node maintains their priority ranking of their neighbors according to the rate of generated queries. Nodes that generated a low rate of queries have a higher priority. The destination confirms that the query is not outdated and verifies its integrity and authenticity through the calculation of the keyed hash. So the malicious compromised nodes participating in the network are given least priority to deal with. The security analysis is similar to Ariadne as it is based on DSR protocol.

2.6.1.3 Ariadne

Ariadne is a secure routing protocol [16, 34] developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig based on the Dynamic Source Routing protocol (DSR) [18]. Ariadne is an on-demand routing protocol, which find routes as when it required, dynamically [14]. Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. It contains two phases in its routing mechanism; Route discovery and Route maintenance.

In the route discovery phase the source node establishes a route by flooding route request packets (RREQ). The RREQ contains the source IP address and destination IP address. The neighbor nodes accumulate the traversed path into the RREQ and broadcast to its next neighbor if the current node is not the destination node. Once the destination node receives the RREQ it concatenates the source route in a Route Reply packet (RREP) and replies on the same path as in RREQ. In the RREQ unicast process, intermediate nodes update their routing tables to each of the nodes along the source route.

Route maintenance is carried whenever there is a broken link observed in the specific route to the destination. When the packets are forwarded through a specific route, each node sends the packet to the next node in the route and the next node acknowledges the packet received. When a broken link is observed in the destination path the broken link will not acknowledge to the packet transmitted by the neighbor node, and the node send a route error message (RERR) to the source node. The source then responds to this RERR and stops sending the next packets and will look in its route cache for alternative routes and follow the next available path.

Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps. Wormhole attacks are possible in Ariadne through two compromised nodes.

2.6.2 Asymmetric Cryptography Solutions

2.6.2.1 ARAN [22]

The Authenticate routing for ad hoc network (ARAN) [22] is a secure routing protocol for MANETs, developed by Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz and Elizabeth M. Belding-Royer based on AODV [17].

ARAN utilizes cryptography mechanism in order to achieve security goals such as; authentication, message integrity, and non-repudiation in ad-hoc networks [23]. It uses asymmetric cryptography to securing routing in an ad hoc network and require universal trusted third party (T) [24]. It consist three distinct operational stages: the first stage is the preliminary certification process that requires existence of a trusted certificate authority (CA). Each node before entering the network must contact to certificate authority and request a certificate which contains address and its public key. After getting public key it broadcast its own key to all nodes that participate in the network. The second operational stage of the protocol is the route discovery process that provided end-to-end authentication. This ensures that the intended destination was indeed reached. The route discovery process [17] of ARAN [22] protocol is begins with, a source node broadcast to its entire neighbor a route discovery packet (RDP). The RDP includes the certificate of initiating node, nonce, timestamp and the address of the destination node. Furthermore the initiating node sign the RDP, each node validate the signature with the certificate, updates its routing table and sign on RDP received

by neighbor and forward to its neighbor after removing certificates and signature of the previous node but not the initiator node. The signature prevents malicious nodes form injecting arbitrary route discover packets that alter routes of form loops. The destination node receives the RDP and verify it the replay through route replay packet (REP). The REP contains the address of source node, certificate, nonce and timestamp. The destination sign it REP before transmitting it. The REP is forward back to source node by the process similar to route discovery, except the REP is forward back in unicast along with reverse path.

The third operation stage of ARAN protocol is optional and ensures that the shortest path is discovered. The source node broadcast shortest path discover message (SPM) to its neighbor, which include the address of destination node, nonce, timestamp and its certificate. The message is also encrypted with the destination public key. Route maintenance in the ARAN protocol is achieved with broadcasting error message (ERR) to its neighbor. The ERR include timestamp and a nonce in order to prevent replay attack.

ARAN uses public key cryptography and a central certification authority server for node authentication and neighbour node authentication in route discovery. It prevents spoofing attacks using a timestamp. It prevents many attacks such as replay.

Denial-of-service attacks are possible with compromised nodes. Tunneling attacks are possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Wormhole attack is also possible through two compromised nodes. Table overflow, Blackhole attacks are impossible due to node level authentication with signatures.

2.6.2.2 SAR [21]

SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. As show below the author [Seung, Prasad, Robin] evaluated the security of SAR [21] in terms of trust level and message integrity.

Trust Level: SAR routing mechanism is based on the behavior associated with the trust level of a user. It is a binding between the identity of the user and the associated trust level. To follow the trust-based hierarchy, cryptographic techniques like: encryption, public key

certificates, shared secrets, etc. are employed. Message integrity: The compromised nodes can utilize the information flow in between nodes and reading of packets to launch attacks. It results in corruption of information, confidentiality of the information, and in denial of network services.

The Security analysis on the attack patterns is based on the trust based framework. So the analysis depends on the key management used and the cryptographic systems applied.

2.6.3 Hybrid Solutions

In this category we have included the secure routing protocols that employ both symmetric and asymmetric cryptographic operations. The most common approach is to digitally sign the immutable fields of routing messages in order to provide integrity and authentication, and to use hash chains to protect the hop count metric.

2.6.3.1 SOADV [18]

Secure Ad hoc On-demand Distance Vector (SAODV) is a proposal for security extensions to the AODV protocol [17, 18, 33]. The proposed extensions utilize digital signatures and hash chains in order to secure AODV packets.

In order to facilitate the transmission of the information required for the security mechanisms, SAODV defines extensions to the standard AODV message format. These SAODV extensions consist of the following fields. The hash function field identifies the one-way hash function that is used. The field max hop count is a counter that specifies the maximum number of nodes a packet is allowed to go through. The top hash field is the result of the application of the hash function max hop count times to a randomly generated number, and finally the field hash is this random number. When a node transmits a route request or a route reply AODV packet it sets the max hop count field equal to the time to live (TTL) field from the IP header, generates a random number and sets the hash field equal to it, and applies the hash function specified by the corresponding field max hop count times to the random number, storing the calculated result to the top hash field.

An intermediate node that receives a route request or a route reply must verify the integrity of the message and the hop count AODV field. The integrity requirement is accomplished by verifying the digital signature. Before the packet is re-broadcasted by the intermediate node

the value of the hash field is replaced by the result of the calculation of the one way hash of the field itself in order to account for the new hop.

SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts.

Tunneling attacks are possible through two compromised nodes. Wormhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible reply attacks.

Table 2.6 Shows mapping between the attack patterns and protocols

Protocols → / Attack Patterns ↓	SEAD	Ariadne	SRP	ARAN	SAR	SOADV
DoS	Yes	Yes	Yes	Yes	Yes	Yes
Tunneling	Yes	Yes	Yes	Yes	Yes	Yes
Spoofing	Yes	No	No	No	No	No
Blackhole	Yes	No	No	No	No	No
Wormhole	Yes	Yes	Yes	Yes	Yes	Yes
Routing table overflows	Yes	No	No	No	No	No

Yes = Attack Possible

No = Attack not Possible

CHAPTER 3
Problem Statement

3.1 Problem Statement

The participating nodes of a MANET are independent, mobile and don't have a centralized and organized network infrastructure. All these characteristics of MANETs allow the attackers to easily intrude into the network and have exceptional chances of disturbing and possibly jamming the communication. Any malicious or misbehaving nodes can generate hostile attacks. These attacks can seriously damage basic aspects of security, such as integrity, confidentiality and privacy of the node.

How we can secure our network and its operation during network initializing, packet forwarding and route maintenance process and how we can detect the malicious and selfish node. The above discussion needs the secure mechanism for secure routing in MANET and make sure that it can adapt the situation regarding to detection of malicious and selfish node and node mobility, while node leaving the network and joining the network.

3.2 Explanation

The characteristic of MANETs, such as dynamic topology, node mobility etc. due to this the detection of malicious and selfish node are very difficult. The detection part of problem basically consists of two questions, how to detect malicious and selfish nodes and how to handle the condition of the node mobility while node leaving the network and node joining the network. The EPKCH mechanism is implemented in ASRP to detect malicious and selfish node during network initialization, packet forwarding and route maintenance operation in MANETs. This protocol provides all the features to achieving security goals such as; privacy, authentication, integrity and non-repudiation and that reduced the chance of the attacks to bare minimum. In MANETs every node is mobile; due to the mobility of node many attacks can possible. At the time of attacks the node may leave or join the network so. In ASRP we discuss the different mode of nodes, that is responsible for detecting malicious and selfish node and make network operation secure.

3.3 Justification

The secure protocol discussed in previous chapter have limited with the respects to the detection of the malicious and selfish nodes. ARAIDNE does not take into account the case of the selfish node. SRP suffers for the lack of the validation mechanism. SEAD suffer the problem of spoofing and wormhole. In ARAN DoS and wormhole attacks are possible. So we cannot say that any one protocol is secure in all the security aspects.

EPKCH is implemented in ASRP to securing MANETs operation. EPKCH mechanism detect malicious and selfish node during different operation of nodes. It provides authentication and non-repudiation to each node to verify signature, nonce and timestamp for preventing Blackhole and wormhole attacks. It also provides integrity and privacy by using public key and private key of nodes. So, our protocol provides all the security features. It also prevents MANETS from many types of attacks.

CHAPTER 4

Extended Public Key Cryptography

Introduction

The word “Cryptography” [12, 13] is derived from Greek word means “secrete writing.” It provides set of mathematical tools and for securing information. Cryptography can be used to protect sensitive and valuable information from malicious hackers. The fundamental goals of cryptography is; confidentiality data integrity, authentication and non-repudiation.

There are mainly two categories of cryptography mechanism that are used for designing security based system. One is Symmetric key Cryptography and other is Public key Cryptography.

4.1 Symmetric key Cryptography

This crypto-system used same key for both encryption and decryption. It is also known as Secrete key Cryptography [12]. Both sender and receiver have the same key, when they communicate to each other.

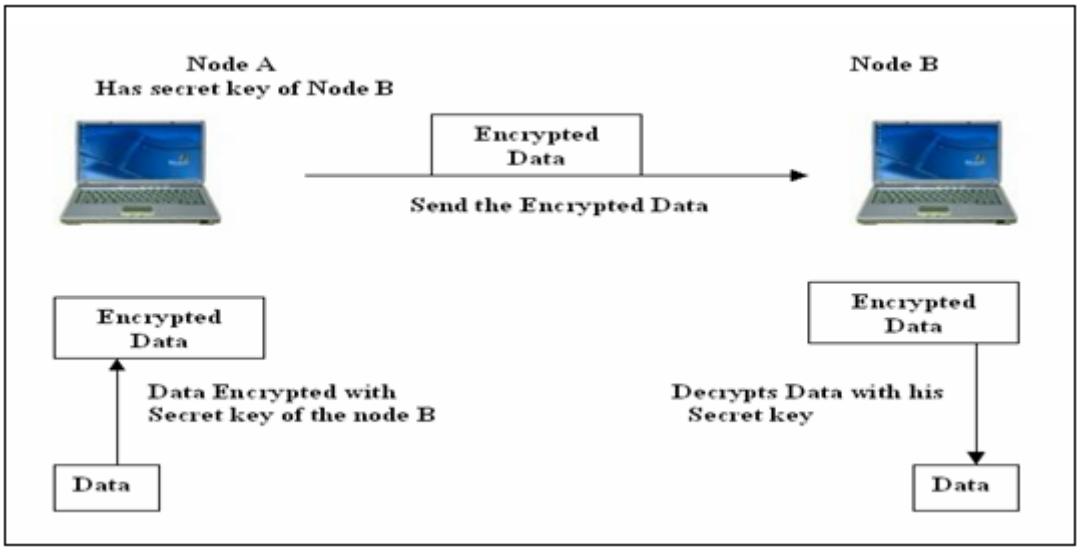


Figure 4.1 Symmetric key Cryptography

The Advantage of Symmetric key Cryptography are:

- Widely used and very popular,
- Very fast relative to other crypto-system, and
- Cipher text is compact.

The Disadvantage of Symmetric key Cryptography are:

- Non-repudiation is not possible,
- There need large number of keys to communicate large number of people in a group, and
- Key length is small compare to public key cryptography.

4.2 Public key Cryptography

This crypto-system [13] uses two key, one key for encryption called public key and other key for decryption called private key or secrete key (Also known as Asymmetric key cryptography). Each user has two key one public key and other private key. The public key of each user is publically available to all other user in public key database. The public key and private key are mathematically linked. Encryption is performed using public key and decryption is performed using private key.

Example: RSA, which is first practically, implemented public key cryptography.
To generate the two keys, we choose two large random number p and q they are relative prime to each other. Compute product of two numbers i.e. n=p*q.
Then randomly choose encryption key e, which is relative prime to (p-1)(q-1).
To compute decryption key d we uses Extended Euclidian Algorithms i.e.

$$ed = 1 \bmod (p-1)*(q-1)$$

$$d = e^{-1} \bmod (p-1)*(q-1)$$

To encrypt message m, first it divided into numerical block smaller than n with binary data.
After encrypting message (plane text) we get cipher text c

$$c= m^e \bmod n$$

To decrypt message, take encrypted block,

$$m= c^d \bmod n$$

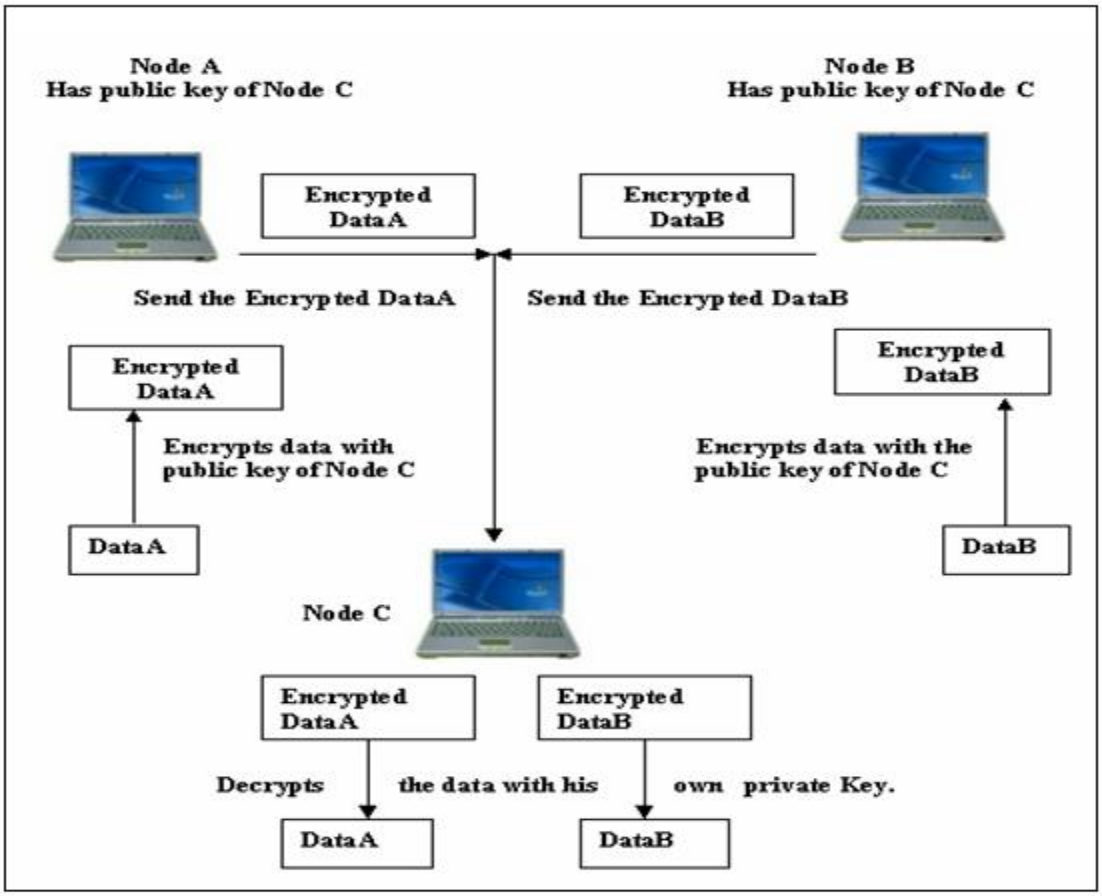


Figure 4.2 Public key Cryptography

The Advantage of Public key Cryptography are:

- Support Non-repudiation,
- Consider very secure, and
- The number of key managed by each user is much less than symmetric key cryptography.

The Disadvantage of Public key Cryptography are:

- Much slower than Secrete key cryptography,
- Key length is large, and
- Cipher text is much larger than plain text.

4.3 Extended Public key Cryptography (EPKCH)

The extended Public key Cryptography is a mechanism that is modify form of public key cryptography. To generates public key and private key each node utilized RSA [14] algorithms. This cryptosystem is mainly design for the securing data during packet forwarding operation and also to detect malicious and selfish node during network initialing and packet forward operation. As the reason discussed above the symmetric key cryptography and public key cryptography are limited in their operation, they do not possess the requisite feature to secure the MANETs operation. So, existing public key cryptography mechanism has been extended to securing the MANETs operation.

The extended public key cryptography mechanism is basically suited for MANET environment but apart from MANET, it is suited well for other environment also. Confidentiality is the basic features provided by the public key cryptography but extended public key cryptography also provide authentication, non-repudiation and integrity.

4.3.1 Operation and Key Management in EPKCH

The extended public key cryptography employs the mechanism that involves the information being encrypted/decrypted or modified by the attacker during the packet forwarding operation. The detail structure is given in the following section.

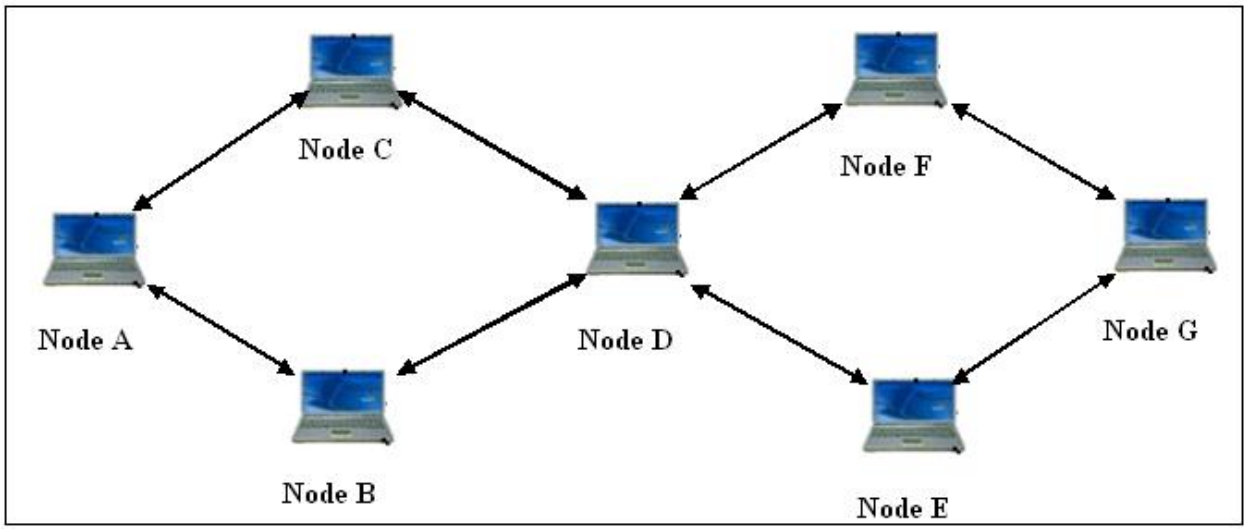


Figure 4.3 Nodes Participating in EPKCH Mechanism

If any node want to join the network, it first it send the PackHello message to all its neighbour to getting certificate, and public key of all other node that participate in the network. We assume that the new node have knowledge about the public key of neighbour node. The PackHello contain its public key and signature of the node. After receiving PackHello, the neighbour sends the certificates, and public key of all the nodes which are available in their NodeInfo table that are signed by its own private key. Certificate contains the IP address of the nodes signature of each node, a timestamp t when node is created, timestamp e, when certificates are expired and a nonce (A random number uses once). After receiving certificate, it joins the network and broadcast its own public key, signature, timestamp, and nonce to all other node within the network. Each nodes after receiving public key, a nonce, a timestamp t, timestamp e and signature of new node, updates its own NodeInfo table.

If a node A want to send the packet to node G, it go to its own NodeInfo table, and search the route information from the source node A to the destination node G. If route information is available to the destination node then packet is send via same route. Sine to design ASRP we follows the table driven approach, so each node must maintain at all times a table that consist the route information about all the possible destination reachable from source node and also maintain the information regarding to network connectivity of every node participate in the network. In this way every node has complete knowledge about the route of each node reachable from a particular source node.

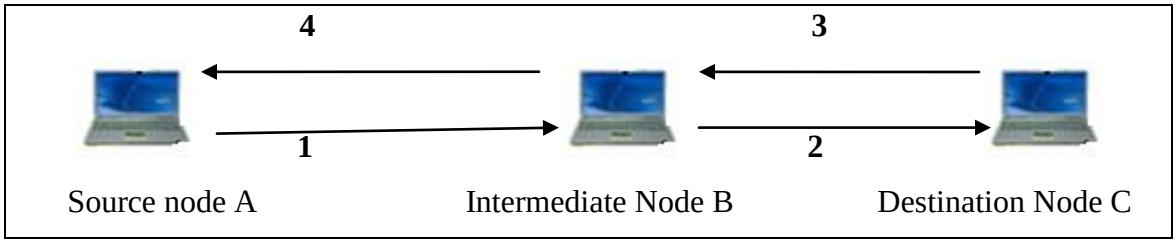


Figure 4.4 EPKCH Mechanism Implemented by Nodes

When the source node has got the complete route information the destination node it sends the packets to destination node. Packet's first part (PackPPart) send the data by encrypting

first part using public key of destination node and the second part (PackNPart) is route guider that guide the nodes on the way to which node they should route the packet. Again each intermediate add his information by signing packets using its own private key and also check the signature of source node by decrypting second part of packet using public key of source node. If any change found it inform all the node within the network, there is malicious or selfish node in a network. This means our mechanism detects malicious or selfish node collectively during network initializing mode and packet forward mode.

4.4 Comparison

The following is the comparison of the

Table 4.1 EPKCH Compared to other cryptography schemes

Support for	Symmetric key Cryptography	Public key Cryptography	Extended Public key Cryptography
Non-repudiation features	No	No	Yes
Message Authentication features	No	Yes	Yes
Packet modification features	No	No	Yes
Number of key required for the n node	n*(n-1)/2	2*n i.e. n private key and n public key	2*n i.e. n private key and n public key

CHAPTER 5

Design, Development and Simulation of ASRP

5.1 Introduction

The ASRP is a proactive secure routing protocol. The design of ASRP follows the table-driven approach, each node maintain a node info table regarding to network structure, route information from a particular source to its all possible destination and information about others node. When a new node enters into network all the node updates its own info table. This means that every node have complete knowledge about the network structure.

The ASRP, protocol works on the terminology of the modes of node, in which each mode define the working pattern of node. The different modes correspond to the activity of node and each mode defines particular state of the node in ASRP. When MANETs is established then every node in the Initialization Mode (IM: it is the network initialization mode) which enables every node setup the network infrastructure and store initial information in its own NodeInfo table and also the information regarding to network structure. When nodes are finish initialization they switch themselves to Lazy mode (LM), where they are waiting for forwarding the packet. Lazy mode is the default mode of the each node when they do not do anything. If any node wants to forward the PackFoward packet they switch from lazy mode to monitor mode (MM), then packet forwarding mode (PFM). As soon as they finished the packet forwarding they switch to lazy mode. In lazy mode the lazy node forward the PackLazy packet to its neighbor node.

So, there are four mode correspond to different activity of node. The IM responsible for the establishment of MANET, LM is the default mode of the node where they do not do anything. MM mode is responsible monitoring the network and node, while node leaving the network and joining the network. The IM also detect the malicious and selfish node within the network. The PFM is also detects the malicious and selfish node during packet forward operation.

5.2 Assumptions

Our proposed secure protocols aim to protect the network from attackers. Our proposed schemes work under several assumptions as follows:

- The network link is bidirectional. That is, if node A is able to transmit to node B, then B is also able to transmit to A.
- The wireless interface supports promiscuous mode operations. That is, each node can receive a copy of the messages being transmitted by other nodes within its receiving range.
- A public key infrastructure exists in the MANET under consideration. Each mobile node stores the public key of all other nodes.
- The trust relation could be instantiated. For example: by knowing public key of other nodes.
- There is a security association between source node and destination node.
- The existence of security association is justified because, host chose to employ a secure communication schemes and consequently, should be able to authenticate each other.

5.3 Packet types and their Structure

There are two types of packet being transmitted by the various nodes; conditional packet and unconditional packet.

5.3.1 Unconditional Packets

The unconditional packets are those packets that a node sends to neighbour which have fixed size and irrespective of the condition.

a) PackHello

This packet is send by node to all its neighbour when the node is in IM.

Table 5.1 PackHello Packet and Structure

Packet_Id	
NodeNameA_1	Signatur_of_A_1
PublicKey	K_{A1+}

b) PackLazy

This packet is send by the node to all its neighbour when the node is in LM.

Table 5.2 PackLazy Packet and structure

Packet_Id	
NodeName	……
PacketType	PackLazy

5.3.2 Conditional Packet

The conditional packets are those packets that a node sends after detecting the particular condition has been satisfied. Some of the conditional packets are fixed size and some are variable size.

I. Conditional Fixed Size Packet

a) PackUpdate

This packet is send by various nodes to their neighbour when they detect that there is any change in their neighbour position of the nodes.

Table 5.3 PackUpdate Packet and Structure

Packet_Id	
NodeName	……
PacketType	Conditional
$NodeNome_{other}$	Info_about_other_node

b) PackError

This packet is send by the node to the source node to indicate that the destination does not exists

Table 5.4 PackError Packet and Structure

Packet_Id	
NodeName	……
PacketType	Conditional
$NodeNome_{other}$	PackError

.

c) PackMalicious

This packet is send by the node to its neighbour when it finds any malicious activity by some node.

Table 5.5 PackMalicious Packet and Structure

Packet_Id	
NodeName	……
PacketType	Conditional
$NodeNome_{other}$	Info_about_other_node or PackMalicious

d) PackSelfish

This packet is send by the node to its neighbour when it finds any selfish activity by some other node

Table 5.6 PackSelfish Packet and Structure

Packet_Id	
NodeName	……
PacketType	Conditional
$NodeNome_{other}$	Info_about_other_node or PackSelfish

II. Conditional Variable size packet

The variable size packets are.

a) PackInitialized

This packet is send by node to neighbour when neighbour node sends PackHello to him.

Table 5.7 PackInitialized Packet and Structure

Packet_Id	
$NodeName_{A1}$	$PublicKey(K_{A1+})$
$NodeName_{A2}$	$PublicKey(K_{A2+})$
----------	---------
$Nonce\_of\_A_1$	$TimeStamp\_of\_A_t$
Number_of_node	No_of_Hopes
PacketType	PackInitialized

b) PackForward

This is the packet which is prepared by the source node first then it is modifying by the all node which are on the route to destination, by adding its own information. All the intermediate node encrypt the NPart of packet by the public key of source node and verify it and then sign on it by using its own private key.

Table 5.8 PackForward Packet and Structure

Packet_Id	
NodeName	……
PacketType	PackForward
PrivacyPart(PPart)	Non-repudiation part(NPart)

5.3.3 General Structure of Packet

I. Fixed Size Packets

The general structure of fixe size packets for ASRP is

Table 5.9 Fixed Size Packets Structure

Packet_Id
MAC_{Sender}
Cond_control_bits
MAC_{other}
Info_control_bits

Table 5.10 Cond_control_bits meaning

Bits	**Meaning**
00	Unconditional PackHello Packet
01	Unconditional PackLazy Packet
11	Conditional Packet

The Info_control_bits are meaningful only if the Cond_control_bits are 11. The 3 bit for the Info_control_bits stand for whether the packet has left neighbour of the sender node has just joined the network or sender node detect the MAC_{other} to be the malicious node or the selfish node. These 3 bit stand for the conditional packets so for the Cond_control_bits are 11.

II. Variable Size Packets

The variable size packet structure for the ASRP is

Table 5.11 Variable Size Packets Structure

Packet_Id
MAC_{Sender}
Info_control_bits
MAC_{other}
Info_variable_size

The Info_control_bits identifies whether the packet is PackForward or PackInitialized Packet.

Table 5.12 Info_control_bits Meaning

Bits	**Meaning**
00	PackForward Packet
01	PackInitialized Packet

5.4 Activities of Nodes

There are various activities of node in mobile ad hoc network:

I. The node is sending HelloPacket packet to it all neighbour node to getting the certificate and public key of all other nodes that participate in the network.

II. The neighbour node sends the public key and certificate signed by its own private key, to the node by sending PackCert packet.

III. The node will forward the PackFoward packet that will receive from its neighbour if it is not destination node.

IV. The node will monitor any topology change in its neighborhood that is if any node is leaving the network, joining the network or changing its position with respect to neighborhood.

All these activities correspond to the specific state of node in mobile ad hoc network. And the group of activities represents the mode of nodes. The first and second activity grouped into IM (network initialized mode), the third activity will come under the PFM (packet forward mode) and the fourth activities come under MM (monitor mode). We discussed every mode of the node detailed in next section.

Figure 5.1 Transitions between Modes

5.4.1 Initializing Mode (IM)

I. Description

This mode is responsible for the establishment of MANETs. It can be established MANET in two ways. One way can be that all the nodes get on at the same time and second way can be that the node get added to the network with the posses of the time. For the first way all the

node are in the IM simultaneously and for latter situation the node added to the network is in IM. After initialization mode node switches to lazy mode. In IM mode, each node got the public key of all other nodes participating in the network before joining the network. In this mode a trust relationship exists between each node that participates in the network by sharing public key and other information.

II. Procedure

- In this mode during the initialization of the network the node, say A, send the PackHello packet to its neighbour to get the PackInitialized packet. If other node send the PackHello packet to the node, say B, it send the PackInitialized to the node.
- When node receives the PackInitialized packet it updates its NodeInfo table, and broadcast PackInfo to all node that participate in the network which contains its public key, timestamp t, timestamp e, address and signature and then switch to lazy mode.
- When the others node receive the information about new node updated its NodeInfo table and also check there is any change in the table or not. If there is no change in the table then it switches to LM.
- If the node not receives the PackInitialized to any its neighbour it again sends the PackHello packet.
- This mode is can also help to find the malicious nodes as they may change the public key of node intentionally. The node can compare the public key send by particular node with the public key send by others nodes and if the find any deviation it send the PackMalicious packet to other neighbour nodes.
- It the node find that a particular node is not responding with the PackInitialized packet corresponding to its PackHello it send the PackSelfish to its neighbour nodes.
- All the nodes switch to IM from the LM if all the node going to change their keys. Then they perform the process of Initializing with neighbors.

The node can change their mode according to their activity, if a node finish the Initialization process it switch to lazy mode and if they want to be forward a PackForward to any node then it switch lazy mode to packet forward mode through monitor mode. Transition between modes depends upon the activity of nodes.

Table 5.13 Packet exchanged and Transition in IM

Mode	Packet exchanged	Transition to Mode
IM	PackHello, PackInitialized	MM, LM

In the Network Initialization procedure, if a node is in IM and send the PackHello Packet.

1. Start
2. Send the PackHello packet to all node which are at the distance i=0.
3. Stop.

A. In the Network Initialized procedure, if a node is in IM and get the PackHello packet.

1. Start
2. Update its NodeInfo table.
3. Send the PackInitialized packets which contain the public key all other node and other information regarding to network structure which are available in its own NodeInfo. It send to that node which are at the distance of i=0.
4. Stop.

B. In the Network Initialized procedure, if a node is in IM and get the PackInitialized Packet.

1. Start
2. Set change = false
3. Updates its NodeInfo table
4. Check for any change in its NodeInfo table, if there is any change

   Then

   Change = True
5. If change = true

   Send the PackHello again

   Go to step 2.
6. Stop

III. Structure of the NodeInfo table

The node stores the information regarding the network structure and information about other nodes (such as public key, address, timestamp t, timestamp e, nonce and signature to all others node that participate in the network)

Table 5.14 Structure of NodeInfo Table

NodeName	**Public key**	**Nonce**	**Timestamp**	**NextNodeName**	**NumberofHops**
-----	-----	-----	----	----	----
----	----	----	----	----	----

IV. Main Goals

The main goals of Network Initialized mode are listed below

- All the nodes can get the public key of all other nodes that participate in the network.
- After IM procedure ever node updates its NodeInfo table and gets complete knowledge about the route of all other nodes that are reachable to source node and also get the information regarding to the network topology.
- All the node have get approximate idea about how much distance and time (millisecond) taken to sending a data to the particular node.
- This mode can help us to detect malicious and selfish node within the network, by comparing the same node public key send by the different nodes.
- This mode is responsible for the establishment of mobile ad hoc network, by adding node in the network.
- The transition from IM to either lazy mode or MM or packet forwarding mode via monitor mode.

5.4.2 Lazy Mode

I. Description

The LM is the default mode of the node. The node switches this mode either from IM, or from MM, or from PFM. When MANET is established every node are in the network initializing mode, as soon as they finished the network initialization process it switch form IM to LM. The node is in PFM, and if there is no packet to be forwarded they switch LM. In this mode, if all the nodes want to change their public keys it switch from lazy mode to initializing mode. If the node in LM and detect any neighborhood activity it switch to MM or it has receive any PackForward packet it switch itself to from lazy mode to packet forwarding mode through monitor mode, and after finishing packet forwarding procedure it again back to LM, and forward PackLazy packet to all neighbour nodes.

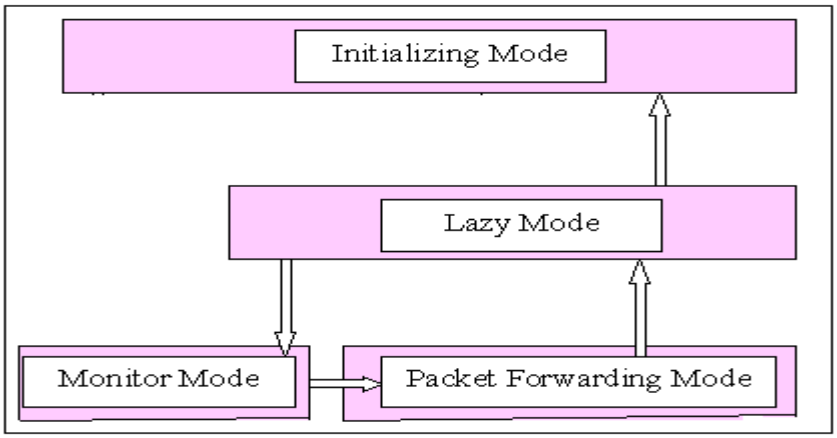


Figure 5.2 Transitions between Modes in LM

II. Procedure

- The Lazy mode is called the default mode of the node.
- As soon as the node finished the network initialization they switch from IM to LM.
- If there is no PackForward packet to be forwarded they switch from PFM to LM.
- When the node in LM detect that there is activity of neighbour node it switch itself to MM
- If the PackForward packet comes from the neighbour node then it switch themselves to PFM through MM and after finishing packet forwarding procedure it comeback to LM.
- If all the nodes want to change their public key then they are also switch LM to IM.
- In the nodes comes in the Lazy mode it send the PackLazy packet to all the neighbour node.

5.4.3 Monitor Mode

This mode is basically for monitoring the network topology when nodes leaving the network, joining the network or changing its position with respect to neighborhood. This mode also detect malicious and selfish node. If the node in mode found any activity of neighbour node or receives any PackMalicious Packet or PackSelfish Packet or PackForward Packet it switches itself to MM. This is the main mode for ASRP, it provide high level of security. This mode is also called the protector mode. These above condition can divided into two part; general condition and special condition

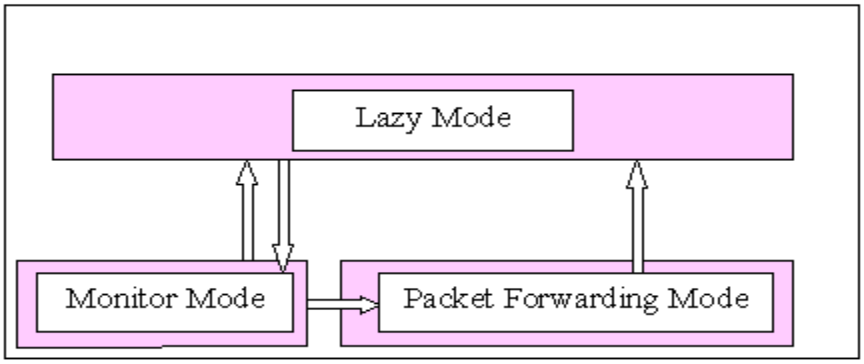


Figure 5.3 Transitions between Modes in MM

A. General Condition

I. Procedure for MM when node are in Lazy mode and detect any activity of neighbour nodes

1. Start
2. Set Flag = 1 (i.e. If there is any activity of nieghbour, then)
   Switch to MM
   Else flag = 0
   End loop
3. It check the neighbour node, for malicious or selfish , if yes then send PackSelfish to all neighbour node
4. If not then return to LM
5. Stop.

II. Procedure for MM when nodes are in Lazy mode and receive PackMalicious or PackSelfish or PackForward to neighbour node.

1. Start
2. If (Flag = True)
   Node receive any packet switch to MM if any PackMalicious or PackSelfish or PackForward packet receive from its any neighbour\
   Else (Flag = False)
   Exit
3. Encrypt the NPart of Packet using public key of neighbour and Compare (by matching signature, nonce, and address of node) the capture packet with the information available in its NodeInfo table.
4. If found any alteration it confirms nodes are malicious.
5. To check selfish node it send ChechPack to all its neighbour for any alteration in network if found then confirms there is a selfish node
6. Else not malicious and selfish node
7. Stop

B. Special Condition

Nodes joining the network, nodes leaving the network and nodes are changing its position within the network. These three special conditions are also handling in monitor mode by sending or receiving PackUpdate packet. These three conditions are explained below. In the case of new node joining the network, say node A want to join the network. There are two cases possible, first is the network has no any node initially and the second case is node A join the network through nodes B_1 to B_n. in first case node A enter into network without any

condition. In second case if n=1, then it join through B_1 and if n=2, then it join through B_1 and B_2.

a. The Procedure for node joining the network is given below

1. Start
2. Flag Join = False
3. While (Join = False)
   The node A checks that if at least one node out of all the node through which it is going to join the network. if there is one node, then
   Join = True
   Else Join = False
   End Loop
4. The node A switch to IM and send the PackHello packet to nodes out of B_1 to B_n which are in LM.
5. The node which are in LM, out of B1 to Bn switch themselves to IM, when it receive the PackHello packet from node A, then updates it NodeInfo table and then it send the PackInitialized Packet to A.
6. Node A match all the PackInitialized packet send by B1 to Bn if there is no change, then

   Node A Update its NodeInfo table and send its own information to all node within the network
   All node in MANET Updates its own NodeInfo table
   Else send PackMalicious to all neighbours.
7. After finishing IM procedure they switch to LM
8. The resident nodes again switch to LM.
9. Stop.

b. Procedure when the node, say D changes its position or detects the change in its neighborhood or node D leaving the network.

1. Start
2. Check any change in its neighbors, if node D leave the network, then
3. The neighbor node E of D send the PackUpdate to all its neighbor
4. If node D change its position, then D send the PackUpdate to its neighbors
5. The neighbor node after receiving it switch to MM, and updates their NodeInfo table and send PackUpdate to all its own neighbors
6. Stop.

5.4.4 Packet Forward Mode

The ASRP is proactive secure routing protocol, so when MANET is established every source node know the route to the all its possible destination node which are reachable from it. The source node then prepare the packet and send it to first node which are on the route of destination node, then first node send to next in this way the data is reaches to the destination node. Now the packet that is sent, consist two parts

PPart	**NPart**

The first part i.e. Privacy part contain the data which is to be transmitted is encrypted by source node by using public key of destination node. The NPart i.e. non-repudiation part contains the address of destination node, a nonce of destination node and timestamp, and the address of all the node along they transmitted. It also contains the address of source and signature of source node which is encrypted by private key of source node. Every intermediate node along the decrypt the NPart of Packet and verify its addresses, if itself

destination node or not then forwards the packet to the next node in the path. This way packet reached to destination node. The NPart contains only the information related to route.

This mode detect malicious and selfish node by verifying NPart of packet. It also detect if link is broken to destination node or if destination not exists by generating PackError packet. If any node behaves as a selfish it detect by resending packet again. If packet send by source node to particular destination and the intermediate node not find the particular destination it send PackError packet to source node.

The data forwarding process is better understood by using an example. Let us suppose the source node want to send the data in PackForward packet has to destination node along the way to destination through the source A ⟶ B ⟶ C ⟶ D destination.

Source ⟶ A {PPart, NPart}

PPart = EP_A (EP_B (EP_C ($EP_{Destination}$ (Data, Source, t, n, C), B,) A), Source)

NPart = EPR_{Source} (A, B, C, (Destination, t, n) $K_{Source-}$

A ⟶ B{PPart, NPart}

PPart = EP_B (EP_C (EPDestination (Data, Source, t, n, C), B), A)

NPart = EP_{RA} (B, C, Destination, t , n) K_{B-}

B ⟶ C {PPart, NPart}

PPart= EP_C ($EP_{Destination}$ (Data, Source, t, n, C), B)

NPart = EP_{RB} (C, Destination, t, n) K_{C-}

C ⟶ $EP_{Destination}$ {PPart, NPart}

PPart= $EP_{Destination}$ (Data, Source, t, n, C)

NPart = EP_{RC} (Destination, t, n)

5.5 Additional Security Features

The others security features enhanced the security of MANET, are given below.

I. The key of the nodes have to be change regularly after some specific time interval, so as keep the MANET secure all time.

II. The dummy packet forwarding operation can be implemented by the intermediate node to detect the node who misbehaves.

III. To detect malicious and selfish during the network initializing process by verifying public key and signature send by all neighbour node to new node.

IV. In case of special scenario of military operation, like some nodes are to join the network latter on, only those nodes join which has the MAC address that has been already verify

5.6 Inbuilt Defense

The various inbuilt defense are in ASRP, to securing MANET, these are:

I. Cooperation Enforcement

The ASRP is the protocol that works by enforcing the cooperation between the nodes. That makes the nodes are more responsible for their action and the probability of the non-intentional behavior of the node also become less. The MANET does not pass the any infrastructure so the nodes have to cooperate fully in order to enforce the operation on the nodes in the correct way.

II. Robust Modular Implementation

There are four modes of the ASRP each mode has its own modular implementation and independent working. That paves the way for the modification of the working of the modes in the future as the need arises without modifying the working of the other modes. Moreover the modular approach is best for the debugging also.

5.7 Simulation

We are using turbo C, for the simulation, has been performed to simulate the transfer of data between various nodes in initializing mode, lazy mode, packet forward mode and monitor mode. The simulation has been performing on eight nodes.

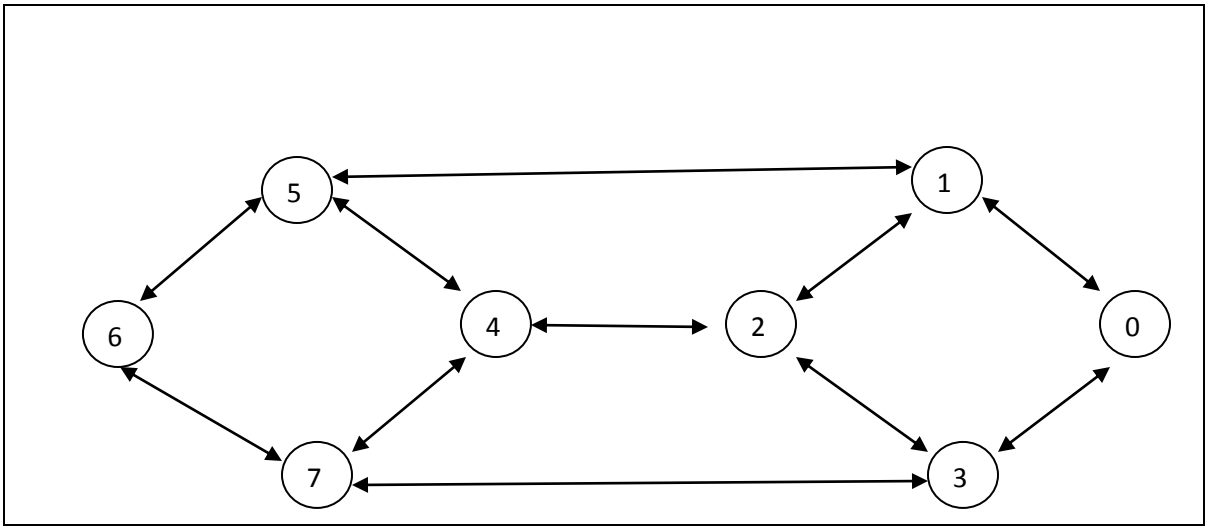


Figure 5.4 Simulated MANET

The simulation program after taking the input performs the simulation as mention below.

I. Network input by adding the node in form of adjacency list

II. Simulate the packet transfer in the Initializing Mode

III. Simulate the packet transfer in the Lazy Mode

IV. Simulate the packet transfer in the Packet Forwarding Mode

Since the ASRP is a proactive secure routing protocol, so in every step it displays the status of tables of all the nodes. The simulation step along with screenshot has been given below.

I. Firstly the simulation program takes the input, in terms of asking for the number, name and name of neighbour of nodes.

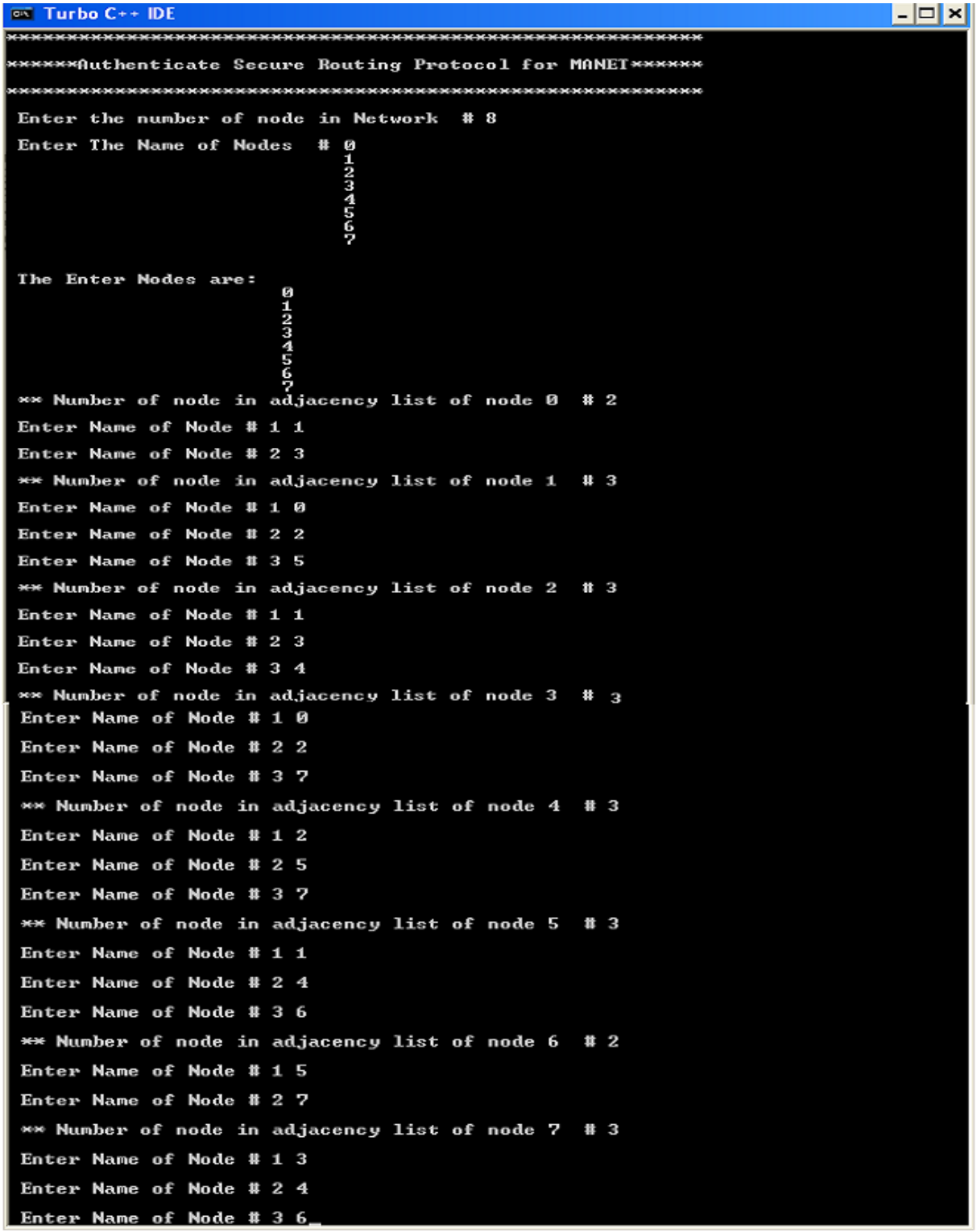


Figure 5.5 Network Input

a) The simulation program displays the network enters in terms of adjacency list.

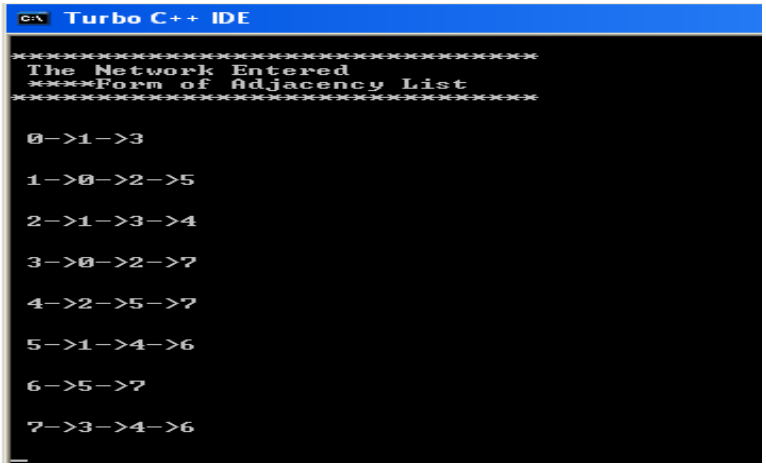


Figure 5.6 Adjacency list of Nodes in the Network

b) The simulation program input the time (in millisecond) to sending the data between each nodes.

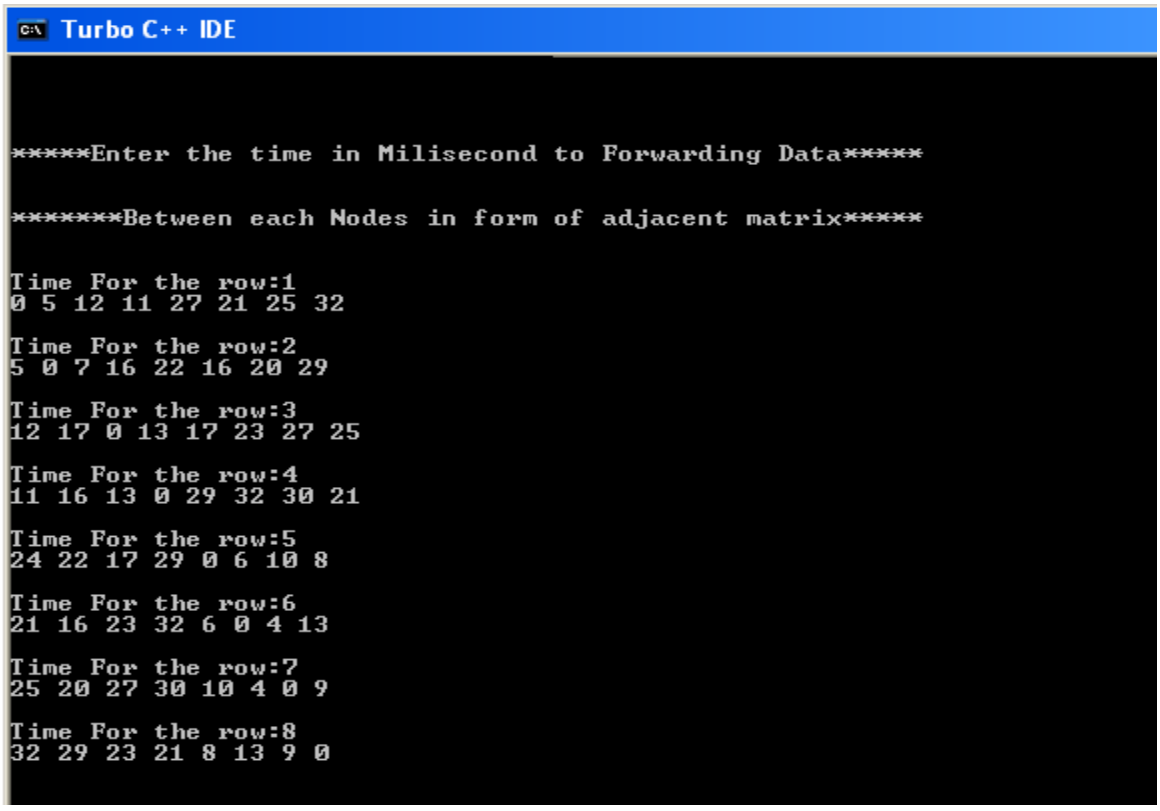


Figure 5.7 Input Times in Millisecond

II. Program to display the packet during the IM, i.e. one node sends the PackHello packet to other and it sends the PackInitialized to previous node.

Initially we assume that node 0 is only single node in MANET, and then enter node 1, and then 2, and so on.

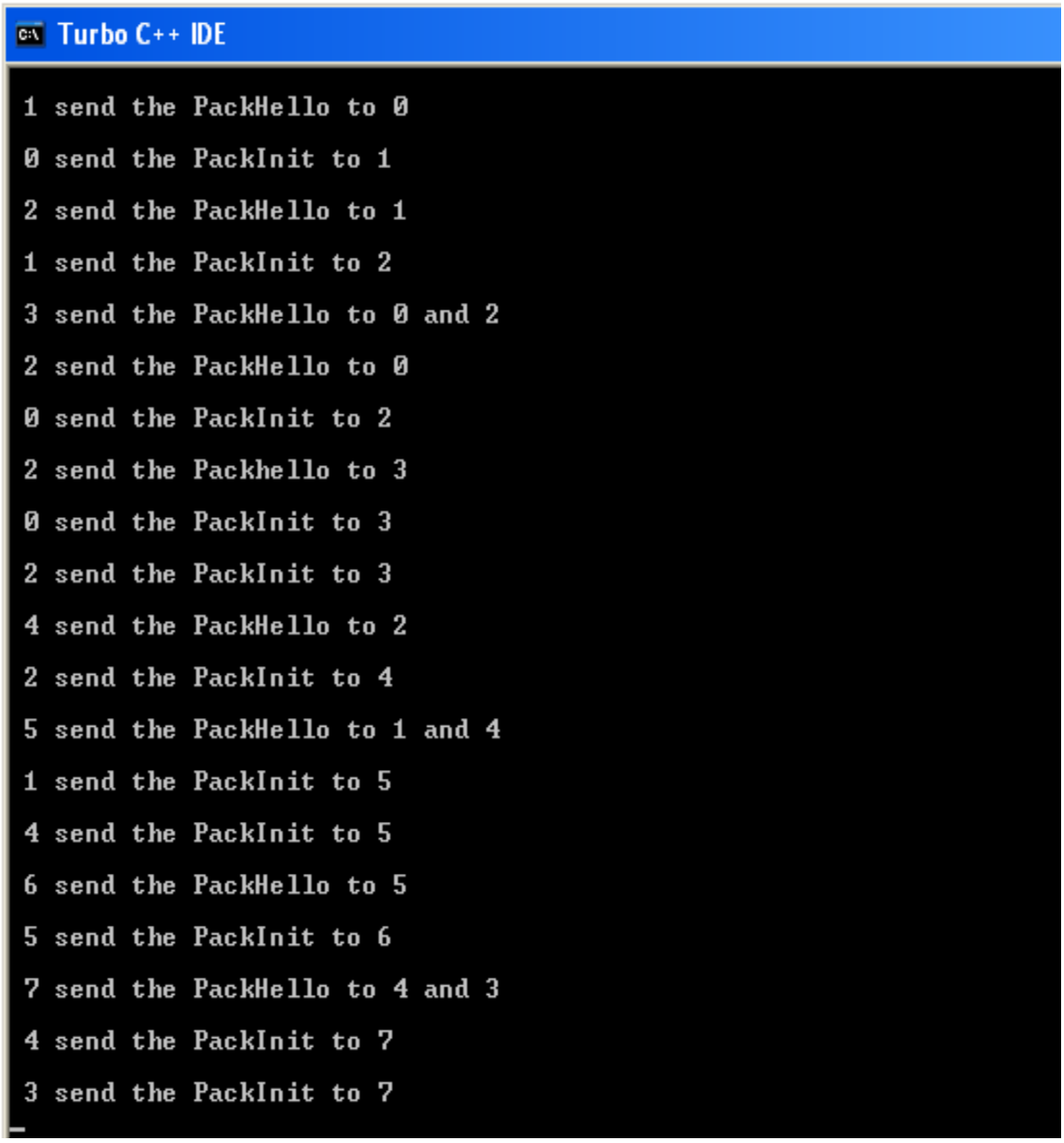
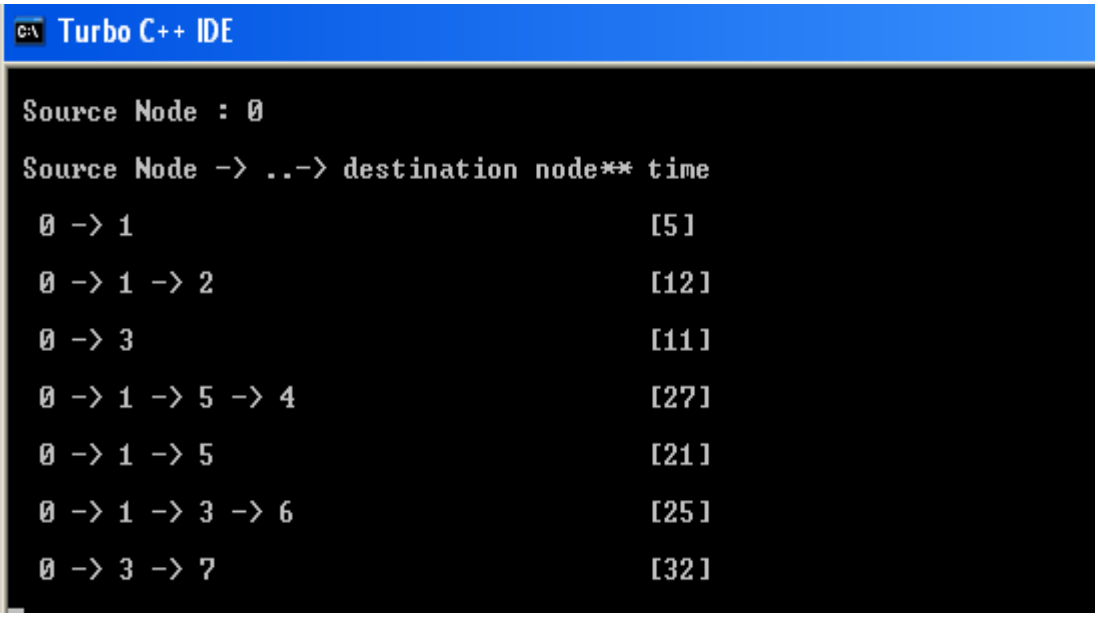


Figure 5.8 Step II Network Initialization Mode

IV. Packet Transfer in Monitor Mode

In this mode if a node detect any activity of neighbour node it goes to MM and send a PackCheck to all its neighbour for detecting Malicious node.

a) After step II every source node shows the route information to its all destination, and time in millisecond.



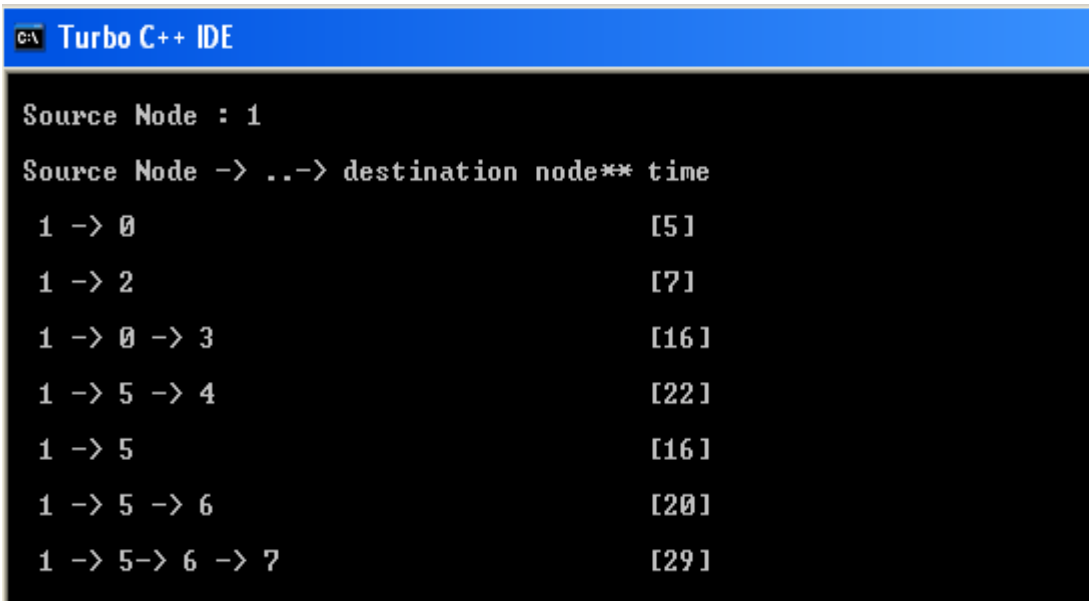


Figure 5.9 Information about the route of all destinations from a source

b) Network after (establishing MANET) step II.

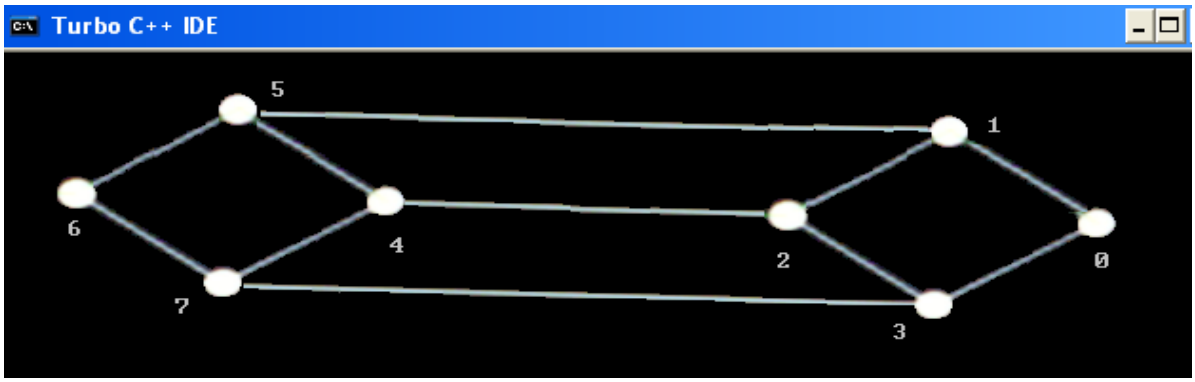


Figure 5.10 MANET after step II

III. Packet Transfer in Lazy Mode

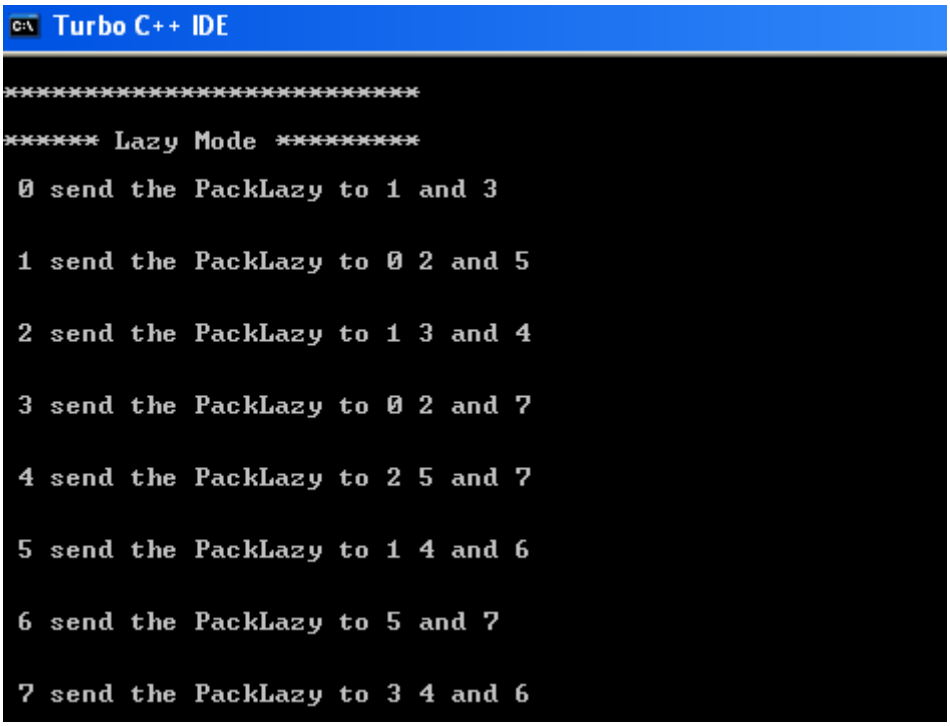
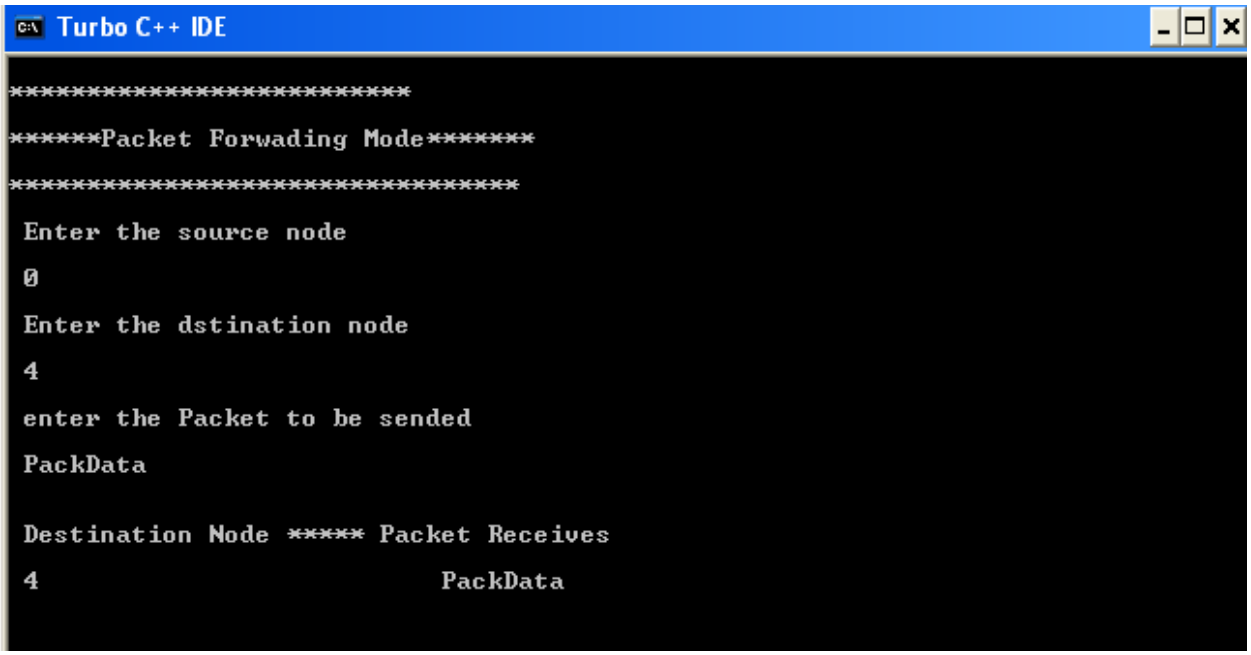


Figure 5.11 Packet transfer during Lazy Mode

IV. Packet Forwarding Procedure



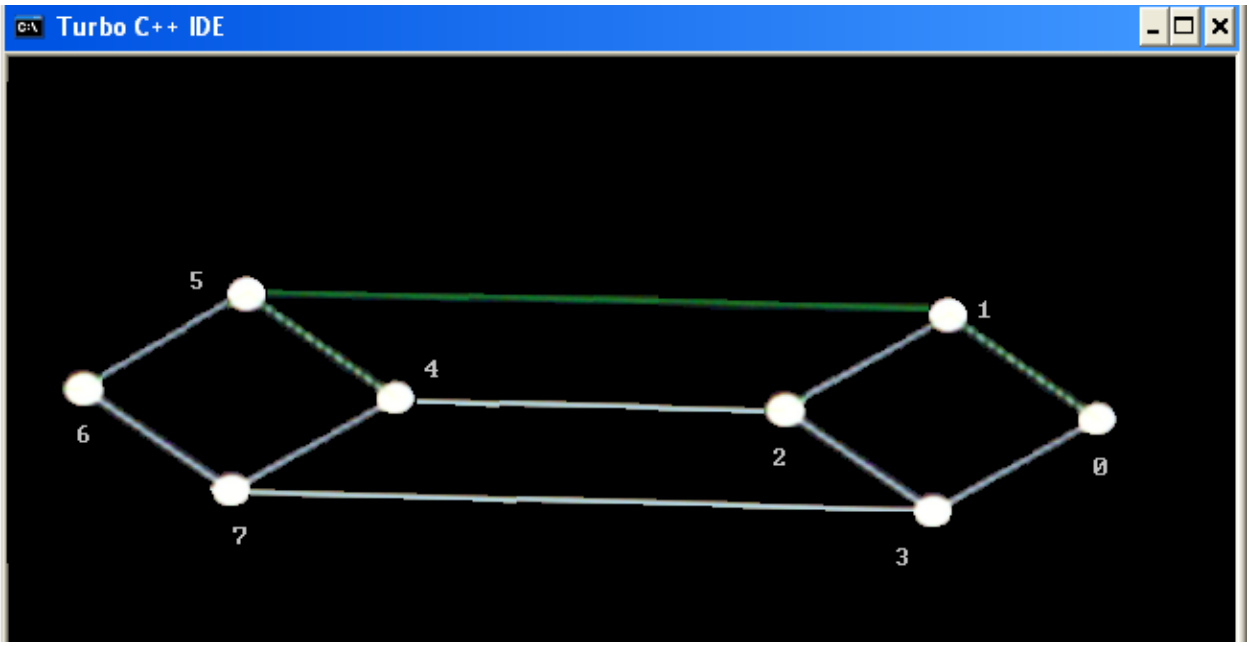


Figure 5.12 Shows the data are going to source to destination via same route.

CHAPTER 6

Conclusion and Future Scope

6.1 Conclusions

Wireless mobile ad hoc networks present difficult challenges to routing protocol designers. Mobility, constrained bandwidth, and limited power cause frequent topology changes. The very basic nature of the mode of communication is the main concern because anything that moves over the open air medium is susceptible to be picked up by unauthorized access. For any mission critical or organizationally sensitive information, ad hoc networks add an element of insecurity. In the existing secure routing protocols most of the security attacks are possible with a compromised node. In this work we focus on how to detect malicious and selfish node and to design and implement a secure routing protocol.

In ASRP protocol we discuss various activity of node which they are shown during the MANET operation and these activities are grouped into modes along their working. We also discussed the packets that are going to be exchanged in different mode of nodes. The conclusion that comes are given below.

I. The problems of malicious and selfish node are handling simultaneously. We discussed Extended Public key cryptography mechanism to handle the malicious and selfish node during network operation. As the selfish node cannot malicious at same time, but if nodes are not malicious then they may be malicious.

II. The protocol is handling the some special situation like nodes joining the network, node leaving the network and nodes are changing its position within the network. The monitor mode of ASRP handles all three situations.

III. In ASRP, there are four modes, the IM corresponds to network initialization phase, the LM corresponds to default phase, PFM responsible for forwarding the packet form source to destination and MM is the protector mode of the network.

IV. The protocol has to develop in the way so that the future modifications are possible without changing overall protocol.

6.2 Future Scope

The proposed secure routing protocol, ASRP, is a proactive routing protocol based on table driven approach. For the future work we can use the hybrid approach or reactive approach in ASRP to implement a new secure routing protocol. We can also add another mode or existing one can be extended to handle some exceptional conditions. The public key cryptography algorithm can also be extended to securing MANET.

Annex- I

References

[1] C. Perkins, “Ad hoc Networks,” Addison-Wesley, 2001.

[2] M. Ilyas, “The Handbook of Ad Hoc Wireless Networks,” CRC Press, 2003.

[3] Chatchik Bisdkian, “An overview of Bluetooth Wireless technology”IEEE Communication Magazine, Vol. 39, No. 12, pp 86-94 December 2001.

[4] Brian P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, “ IEEE 802.11 Wireless Local Area Network,” IEEE Communication Magazine, Vol. 35, No. 9, pp 116-126, September 1997.

[5] C.K.Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems,” Prentice Hall Englewood Cliff, NJ 07632, 2002

[6] C. Murthy and B.Manoj, “Ad hoc Wireless Networks: Architectures and Protocols,” Prentic Hall PTR,2005.

[7] IETF MANET Working Group. Mobile Ad Hoc Networks (MANET). Working Group, Charter available at http://www.ietf.org/html.charters/manet-charter.html.

[8] Sonja Buchegger and Jean-Yves Le Buddec, “Increasing Routing Security in Mobile ad hoc Network,” IBM Research Report: RR 3354, 2001

[9] H Deng, W. Li, and D. Agrawal, Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine. Vol. 40, No. 10, 2002

[10] L. Zhou and Z.Haas. Securing ad hoc networks. IEEE, Networks, 13(6):24–30, 1999.

[11] A.Shamir. How to share a secret. Communications of the ACM,(11):612–613, Nov.1979

[12] B. Schneier, Applied Cryptography,Wiley, 1996.

[13] A. Salomaa, “Public-Key Cryptography,” Springer-Verlag, 1996.

[14] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. Security in mobile ad hoc networks Challenge and solution. IEEE wireless communication, 11, 1, (2004), 38-47.

[15] M. G. Zapata and N. Asokan, " Secure Ad hoc Routing Protocols," in Proceeding of the ACM Workshop on Wireless Security, Atlanta, GA September, 2002.

[16] Y. C. Hu, A. Perrig, and D. B. Johnson, " Ariadne: A Secure On Demand Routing Protocol for Ad hoc Network," in Proceeding of 8th ACM Int'l, Conf. on Mobile Comp, Georgia, September 2003.

[17] C. E. Perkin and E. M. Royer, " The Ad hoc On-Demand Distance Vector Routing Protocol," in C. E. Perkin (ed.), Ad hoc Networking, pp 173-219, Addison-2000.

[18] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad hoc Wireless Network," Mobile Computing, T. Imielinski and H. Korth, Ed. Kluwer, 1996.

[19] C. Perkin and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," ACM SIGCOMM, 1994.

[20] Y-C Hu, D. B. Jhonson, and A. Perrig, " SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Network," in Poceeding of 4th IEEE workshop on Mobile Computing System and Applications.

[21] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002

[22] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "ARAN: A secure Routing Protocol for Ad hoc Network," UMass Tech Report 02-32, 2002.

[23] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Network," in Proc. of CNDS 2002.

[24] Rai Tirthraj, Verma A K, " Survey and Analysis of Secure Routing Protocols for MANETs," in the proceeding of National Conference on Cutting Edge Computer and Electronics Technology (CECT 2009), Pantnager, February 14-16, pages 501-06,

[25] Dimitri P. Bertsekas and Robert G. Gallager , "Distributed Asynchronous Bellman-Ford Algorithm," Data Networks, pp. 325 -333, Prentice Hall, Enlgewood Cliffs, 1987, ISBN 0-13-196825-4.

[26] E. M Royer, C. K Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, vol-2, no.6, 6 April 2007, pp 46-55

[27] T. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The Optimized Link State Routing Protocol," ulation," Proc. 4th Int'l. Symp. Wireless Personal Multimedia Comm. Aalborg, Denmark, September 2001, 6 pp.

[28] J. Moy, "Open Shortest Path First (OSPF) Version 2," RFC 2328, April 1998.

[29] C.E Perkins, E.M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2005.

[30] A Verma, "Mobile Ad hoc Networks (MANETs): An Introduction", in TTC Newscaster (a quarterly newsletter of Thapar Technology Campus), pp. 13-14, April 2004.

[31] A K Verma, Mayank Dave and R C Joshi, "Classification of Routing Protocols in MANET", at National Symposium on Emerging Trends in Networking & Mobile Communication (NSNM-2003), pp. 132-139, Sept 5 – 6, 2003.

[32] A K Verma, Mayank Dave and R C Joshi, "Secure Routing in Mobile Networks: A Review," International J. of Systemics, Cybernetics and Informatics (IJSCI), ISSN 0973-4864 (Peer reviewed and accepted).

[33] Zapata, M. G., "Secure ad-hoc on-demand distance vector (SAODV) routing," IETF MANET, internet draft (Work in progress), draft-guerreromanet- saodv-00.txt, 2001.-accessed 10/10/2006.

[34] YC. Hu, A. Perrig , and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," In Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, pages 12-23.

Annex-II

Publications

1. Tirthraj Rai, A K Verma, " Survey and Analysis of Secure Routing Protocols for MANETs," in the proceeding of National Conference on Cutting Edge Computer and Electronics Technology (CECT 2009), Pantnager, February 14-16, pages 501-06,

Annex-III

List of Abbreviations

AODV	Ad hoc On-demand Distance vector
DSDV	Destination-Sequence Distance Vector
ARAN	Authenticated Routing for Ad hoc Networks
DSR	Dynamic Source Routing
EPKCH	Extended Public key Cryptography
SEAD	Secure Efficient Ad hoc Distance Vector
SRP	Secure Routing Protocol
IM	Initialization Mode
LM	Lazy Mode
MM	Monitor Mode
PFM	Packet Forward Mode
MAC	Media Access Control