

Security Performance Issues on ASRP in MANETS

Dr.Balakrishna R¹, Rajesh K.S.²

¹Professor & HOD, Dept of ISE, ²Asst. Professor,

Dept of CSE, Rajarajeswari College of Engineering, Bangalore

¹ rayankibala@yahoo.com

Abstract: *In this paper, the mobile ad hoc networks are proposed the each node participating in the network acts both host & router must be 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. 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 proposed work on this paper is address the security issue, because MANETs are generally more vulnerable, we proposed a secure routing protocol for MANETs, are named ASRP (Authenticate Secure Routing Protocol) based on DSDV. The new protocol works on 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.*

Keywords: MANETs, Security, Cryptography, ASRP, DSDV

Introduction: MANETS 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.

In ad hoc network nodes are try to disrupt the proper functioning network, modifying packets, injecting packets or creating routing loops. In this case security is an important task. 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.

No secure mechanism has been proposed, that can be addressed to detecting malicious and selfish node collectively. The existing protocol Extended Public key Cryptography (EPKCH) [12, 13] that able to detect the malicious nodes and selfish nodes collectively in order to achieving security has Authentication, Integrity, Confidentiality and Non-Repudiation. The proposed protocol named as Authenticate and Secure Routing protocol for mobile Ad hoc Network (ASRP).

It has been implemented using EPKCH mechanism in monitor mode of ASRP to securing MANETs.

Related work :

Extended Public Key Cryptography

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 its Public key.

1.1 Symmetric key Cryptography

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

1.2 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 secret key (Also known as Asymmetric key cryptography).

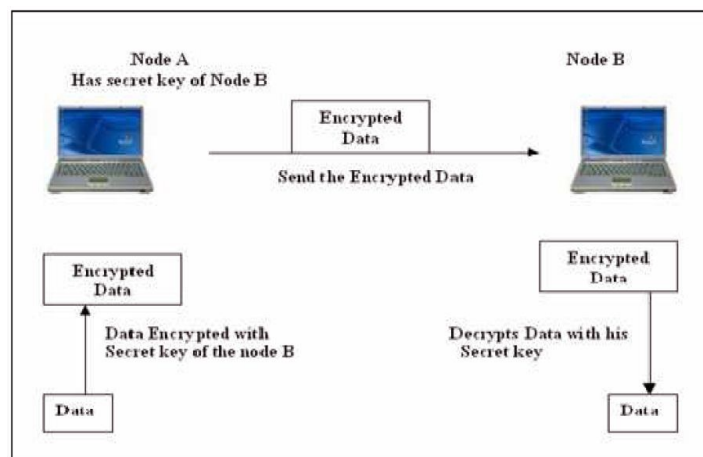


Figure 1.1 Symmetric key Cryptography Each user has two key one public key and other private key. The public key of each user is publically available to all other user in public key database. The public key and private key are mathematically linked. Encryption is performed using public key and decryption is performed using private key.

To generate the two keys, to 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.

$$ed = 1 \pmod{(p-1)(q-1)}$$

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

To encrypt message m , first it divided into numerical block smaller than n with binary data. After encrypting message (plane text) to get cipher text c $c = me \pmod n$ To decrypt message, take encrypted block, $m = cd \pmod n$

1.3 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.

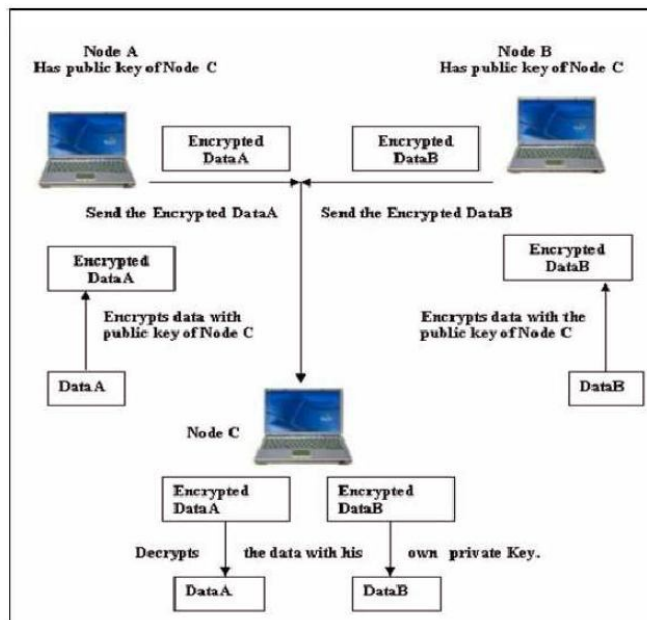


Figure 1.2 Public key Cryptography The symmetric key cryptography and public key cryptography are limited in their operation, they do not possess

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.

2. ASRP :

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.

That is 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 Pack Lazy 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.

2.1 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 neighbor 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. 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).

2.2 Initializing Mode (IM)

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.

2.3 Lazy Mode

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.

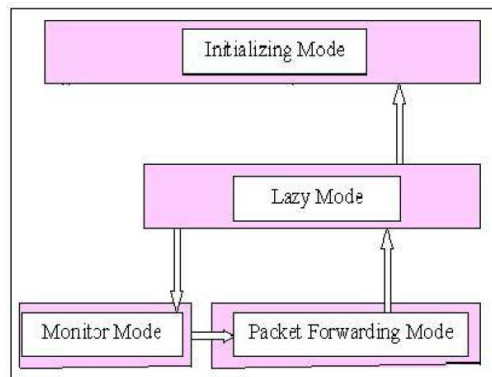


Figure 2.2 Transitions between Modes in LM If the node in LM and detect any neighborhood activity it switch to MM or it has receive any PackForward packet it switch itself to from lazy mode to packet forwarding mode through monitor mode, and after finishing packet forwarding procedure it again back to LM, and forward PackLazy packet to all neighbour nodes.

2.4 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

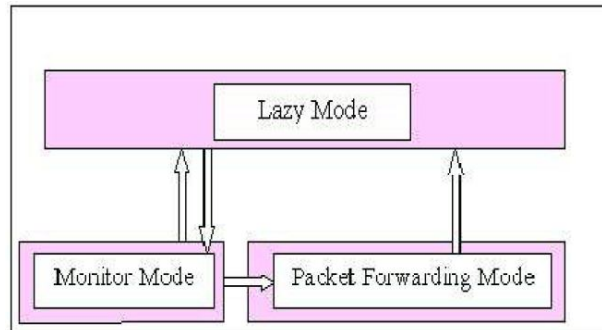


Figure 2.3 Transitions between Modes in MM

General Condition

- I. Procedure for MM when node are in Lazy mode and detect any activity of neighbor nodes
 1. Start
 2. Set Flag = 1 (i.e. If there is any activity of neighbour, 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
- Procedure for MM when nodes are in Lazy mode and receive PackMalicious or PackSelfish or PackForward to neighbour node.

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.

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 ode) 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

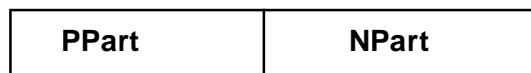
There are two cases possible, first is the network has no node initially and the second case is node A join the network through nodes B1 to Bn. in first case node A enter into network without any condition. In second case if $n=1$, then it join through B1 and if $n=2$, then it join through B1 and B2 etc.

2.5 Packet Forward Mode

The ASRP is proactive secure routing protocol, when MANET is established every source node know to 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 as follows

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



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.

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.

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.

Source A {PPart, NPart}
 PPart =EPA (EPB (EPC (EPDestination (Data, Source, t, n, C), B,) A), Source)
 NPart = EPRSource (A, B, C, (Destination, t, n)
 KSource-
A {PPart, NPart}
 PPart = EPB (EPC (EPDestination (Data, Source, t, n, C), B), A)
 NPart = EPRA (B, C, Destination, t, n) KBB
C {PPart, NPart}
 PPart= EPC (EPDestination (Data, Source, t, n, C), B)
 NPart = EPRB (C, Destination, t, n) KCC
 EPDestination {PPart, NPart}
 PPart= EPDestination (Data, Source, t, n, C)
 NPart = EPRC (Destination, t, n)

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.

3. 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.

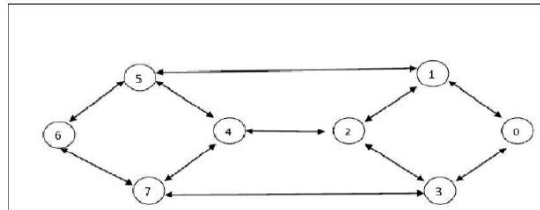


Figure 3.1 Simulated MANET

The simulation results are perform as follows

- Network input by adding the node in form of adjacency list.
- Simulate the packet transfer in the Initializing Mode.
- Simulate the packet transfer in the Lazy Mode.
- 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.

```

Turbo C++ IDE
*****Activate Source Routing Protocol For RHEL*****
*****
Enter the number of nodes in Network # 8
Enter the Name of Nodes # 8
node1
node2
node3
node4
node5
node6
node7
node8

The Enter Nodes are:
0
1
2
3
4
5
6
7
8

== Number of nodes in adjacency list of node 0 # 2
Enter Name of Node # 1 1
Enter Name of Node # 2 3
== Number of nodes in adjacency list of node 1 # 3
Enter Name of Node # 1 0
Enter Name of Node # 2 2
Enter Name of Node # 3 5
== Number of nodes in adjacency list of node 2 # 3
Enter Name of Node # 1 1
Enter Name of Node # 2 2
Enter Name of Node # 3 4
== Number of nodes in adjacency list of node 3 # 3
Enter Name of Node # 1 0
Enter Name of Node # 2 2
Enter Name of Node # 3 7
== Number of nodes in adjacency list of node 4 # 2
Enter Name of Node # 1 2
Enter Name of Node # 2 5
Enter Name of Node # 3 7
== Number of nodes in adjacency list of node 5 # 2
Enter Name of Node # 1 1
Enter Name of Node # 2 4
Enter Name of Node # 3 6
== Number of nodes in adjacency list of node 6 # 2
Enter Name of Node # 1 5
Enter Name of Node # 2 7
== Number of nodes in adjacency list of node 7 # 2
Enter Name of Node # 1 3
Enter Name of Node # 2 4
Enter Name of Node # 3 6

```

Figure 3.2 Network Input

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

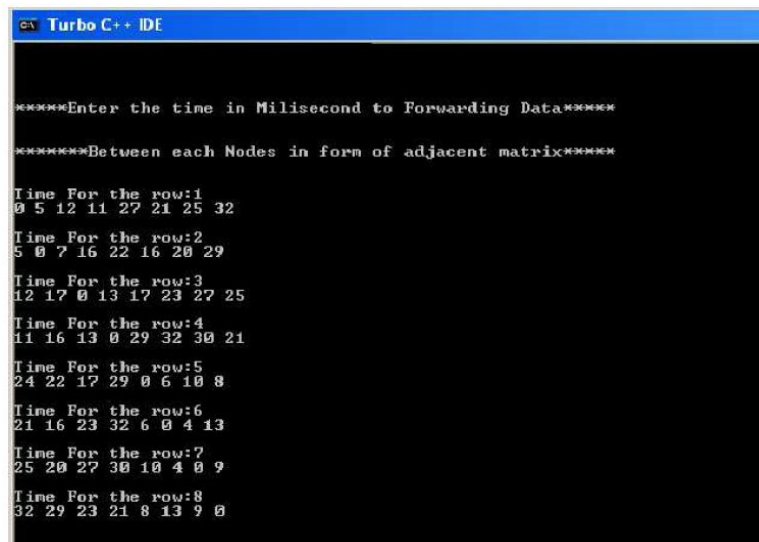
```

Turbo C++ IDE
*****
The Network Entered
****Form of Adjacency List
*****
0->1->3
1->0->2->5
2->1->3->4
3->0->2->7
4->2->5->7
5->1->4->6
6->5->7
7->3->4->6

```

Figure 3.3 Adjacency list of Nodes in the Network

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



```

Turbo C++ IDE

*****Enter the time in Milisecond to Forwarding Data*****

*****Between each Nodes in form of adjacent matrix*****

Time For the row:1
0 5 12 11 27 21 25 32
Time For the row:2
5 0 7 16 22 16 20 29
Time For the row:3
12 17 0 13 17 23 27 25
Time For the row:4
11 16 13 0 29 32 30 21
Time For the row:5
24 22 17 29 0 6 10 8
Time For the row:6
21 16 23 32 6 0 4 13
Time For the row:7
25 20 27 30 10 4 0 9
Time For the row:8
32 29 23 21 8 13 9 0

```

Figure 3.4 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.

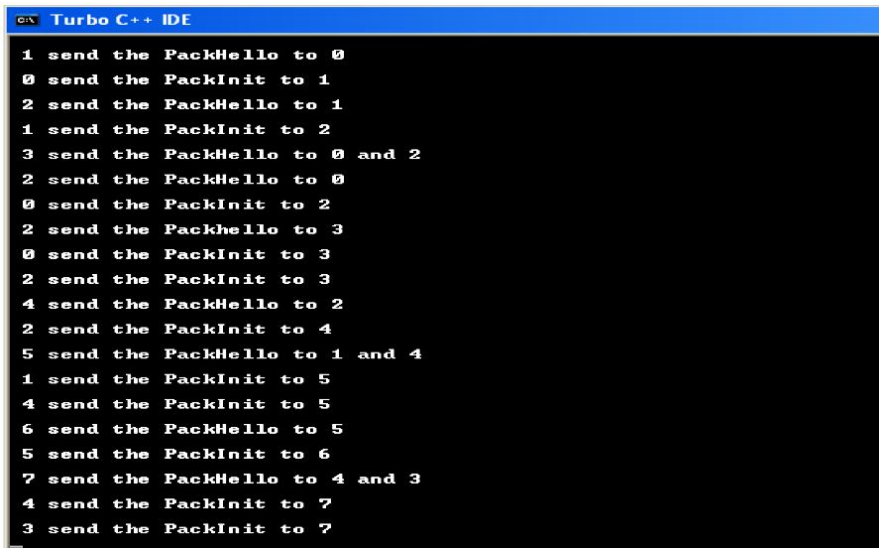
A screenshot of the Turbo C++ IDE window. The title bar reads "Turbo C++ IDE". The main window contains a list of network-related actions in a monospaced font. The actions are numbered 1 through 7 and describe sending PackHello and PackInit packets between nodes 0, 1, 2, 3, 4, 5, and 7. The actions are: 1 send the PackHello to 0; 0 send the PackInit to 1; 2 send the PackHello to 1; 1 send the PackInit to 2; 3 send the PackHello to 0 and 2; 2 send the PackHello to 0; 0 send the PackInit to 2; 2 send the PackHello to 3; 0 send the PackInit to 3; 2 send the PackInit to 3; 4 send the PackHello to 2; 2 send the PackInit to 4; 5 send the PackHello to 1 and 4; 1 send the PackInit to 5; 4 send the PackInit to 5; 6 send the PackHello to 5; 5 send the PackInit to 6; 7 send the PackHello to 4 and 3; 4 send the PackInit to 7; 3 send the PackInit to 7.

Figure 3.5 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.

```

Turbo C++ IDE
Source Node : 0
Source Node -> ..-> destination node** time
0 -> 1 [5]
0 -> 1 -> 2 [12]
0 -> 3 [11]
0 -> 1 -> 5 -> 4 [27]
0 -> 1 -> 5 [21]
0 -> 1 -> 3 -> 6 [25]
0 -> 3 -> 7 [32]

```

```

Turbo C++ IDE
Source Node : 1
Source Node -> ..-> destination node*** time
1 -> 0 [5]
1 -> 2 [7]
1 -> 0 -> 3 [16]
1 -> 5 -> 4 [22]
1 -> 5 [16]
1 -> 5 -> 6 [24]
1 -> 5 -> 6 -> 7 [29]

```

Fig 3. 6 : Information about the route of all destinations from a source

b) Network after (establishing MANET) step II.

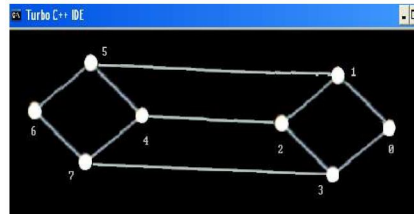


Figure 3.7 MANET after step II

III. Packet Transfer in Lazy Mode

```

Turbo C++ IDE
*****
***** Lazy Mode *****
0 send the PackLazy to 1 and 3
1 send the PackLazy to 0 2 and 5
2 send the PackLazy to 1 3 and 4
3 send the PackLazy to 0 2 and 7
4 send the PackLazy to 2 5 and 7
5 send the PackLazy to 1 4 and 6
6 send the PackLazy to 5 and 7
7 send the PackLazy to 3 4 and 6
    
```

Figure 3.8 Packet transfer during Lazy Mode

IV. Packet Forwarding Procedure

```

Turbo C++ IDE
*****
*****Packet Forwarding Mode*****
*****
Enter the source node
0
Enter the dstination node
4
enter the Packet to be sended
PackData
Destination Node ***** Packet Receives
4                               PackData
    
```

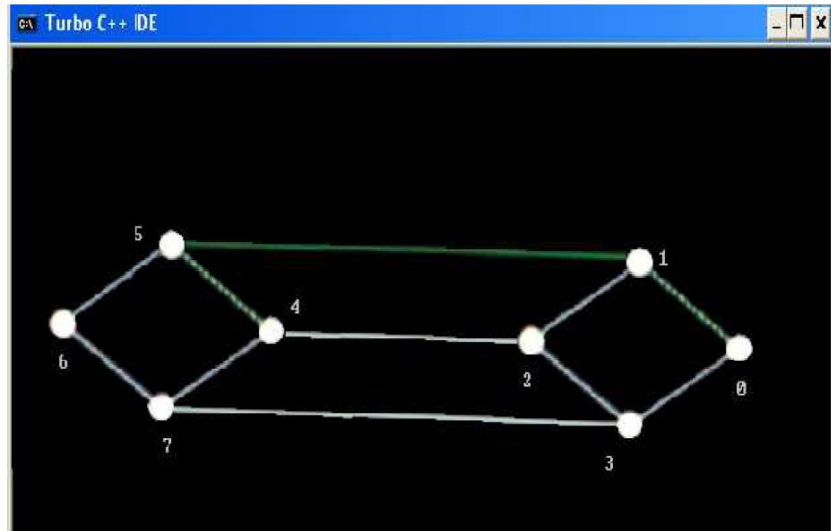


Figure 3.9 Shows the data are going to source to destination via same route

Conclusions

In this work it has been focused on how to detect malicious and selfish node and to design and implement a secure routing protocol. In ASRP protocol discussed various activity of node which they are shown during the MANET operation and these activities are grouped into modes along their working. It also discussed the packets that are going to be exchanged in different mode of nodes.

The conclusion that comes are given below:

The problems of malicious and selfish node are handling simultaneously. It has 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.

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. 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.

Acknowledgements

The authors are thankful for the encouragement and support received throughout this research work to Dr. M.S.Bhaghashekar, Principal & Management, RRCE, Bangalore

References

- [1] C. Perkins, "Ad hoc Networks," Addison-Wesley, 2004.
- [2] M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.
- [3] Chatchik Bisdikian, "An overview of Bluetooth Wireless technology"IEEE Communication Magazine, Vol. 39, No. 12, pp 86-94 December 2007.
- [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, 2006
- [6] C. Murthy and B.Manoj, "Ad hoc Wireless Networks: Architectures and Protocols," Prentic Hall PTR,2010.
- [7] ETF 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,

- 2004 [9] H Deng, W. Li, and D. Agrawal, Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine. Vol. 40, No. 10, 2005
- [10] L. Zhou and Z.Haas. Securing ad hoc networks. IEEE, Networks, 13(6):24–30, 2003.
- [11] A.Shamir. How to share a secret. Communications of the ACM,(11):612–613, Nov.2000
- [12] B. Schneier, Applied Cryptography,Wiley, 1996.
- [13] A. Salomaa, “Public-Key Cryptography,” Springer-Verlag, 2001.
- [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.

Authors Biography Dr. R. Balakrishna, working as a Professor and HOD, Rajarajeswari college of engineering, Bangalore, India. He is completed his Ph.D from Sri Krishnadevaraya University Anantapur. M.Tech Degree from MDU, Rohatak. His research interests are in the field of wireless adhoc network, Sensor Network, Artificial Neural Networks, Data Mining, Operating System and Security.

He has published over 32 National and International journals and Conferences various papers across India and other Countries. He is the Life member of Indian Society for Technical Education and IAENG, CSI, IEEE.

* * * * *