A Process to Improve the Throughput and Reduce the Delay and Packet Loss in Ad-Hoc Wireless Network

Kirna Rani
M.Tech CS&E
Punjabi University Regional
Centre, Mohali, Punjab

Kamaljeet Kaur Magnat
Assistant Professor CS&E
Punjabi University Regional
Centre, Mohali, Punjab

ABSTRACT

A network is a collection of two or more computer systems which connected with each other. It is type of replace of information to communicate with one another. It is an association or set up of computer devices which are involved with the communication facilities. When number of computer is connected simultaneously to exchange information they form networks and contribute to resources. Networking is used to distribute information like data communication. Sharing resources can be software type or hardware types. It is central administration system or supports these types of system [1]. The communications protocols used to organize network traffic, with the network's size, its topology and its organizational intent. A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium.

In this paper we will discuss the method to detect and Isolation of Selective Packet Drop Attack in Mobile Ad hoc Networks.

Other aspects of the paper are:-

- To study and evaluate the selective packet drop attack in MANET and its consequences.
- To detect the selective packet drop in MANET using AODV protocol.
- To propose a new scheme to detect malicious node in the network which are responsible for triggering the selective packet drop attack in the network.
- Simulating the detection of selective packet drop attack using AODV protocol in MANET using NS-2 tool.

Keywords

Wireless Sensor Network, MANET, AODV.

1. INTRODUCTION

A network is a group of two or more computer systems which linked together. It is mode of exchange of information to communicate with one another. It is a connection of computer devices which are attached with the communication facilities [1]. When number of computer are joined together to exchange information they form networks and share resources. Networking is used to share information like data communication. Sharing resources can be software type or hardware types. It is central administration system or supports these types of system.

Different types of networks are as following:

- Transmission media based networks like wired network and wireless network.
- Network Size based network like MAN, LAN and WAN.
- Management based networks like peer-to-peer and client/server.
- Topology based networks called connectivity like bus, star, and ring topology.

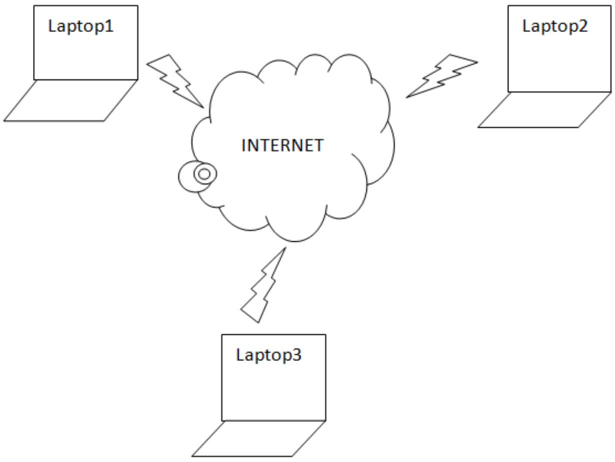

Fig 1: Diagram of Computer Networks

A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium.

2. WORKFLOW OF DESIGN

In this chapter we describe the AODV protocol which is used to establish the best path between the source and destination. The monitor mode algorithm which is used to bring the other nodes in the monitor mode which senses the path which is used for communication. This chapter shows the problem implementation and the solution problem.

3. NETWORK DEPLOYMENT

Firstly we deploy the mobile ad hoc network with infinite number of mobile nodes. All the mobile nodes are randomly deployed into the fixed area. The source and destination are selected for route establishment. For the route establishment source node flood the route request packet in the network and route reply packets are send back to the source by the adjacent nodes. The route is established between source and destination on the basis of hop counts and sequence numbers. The malicious node exists in the route which is selected between source and destination. The malicious node will be responsible for triggering the selective packet drop attack. The proposed mythology will detect the malicious node and isolate, it from the network. In Delay sensitive selective packet drop attack in which either packets drop or transfer to other route to reach to the destination by malicious node. In throughput sensitive packet dropped by the malicious node. In our proposed work we overcome the problem of dropped packet by detecting them and redirect to the source with the help of monitoring nodes.

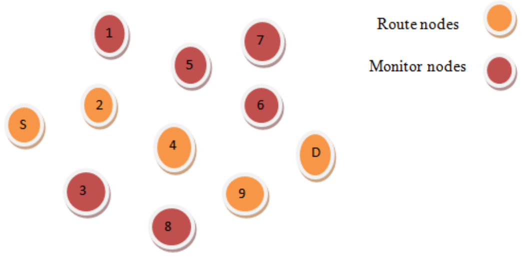

Fig 2: Activation of monitor nodes

In figure 2 The nodes which received the flood messages goes to the monitor mode which is used to detect the malicious node which redirect the path of the node. Other nodes are route nodes are considered in route nodes from source to destination after receiving fake packets.

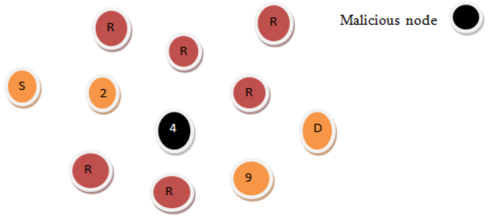

Fig 3: Detect Malicious node

In above figure monitoring node monitor the flood packets. They identified the malicious node which redirects the path from source to destination path to other path. When monitor nodes detect malicious node they all send reply message to the source node to isolate the path.

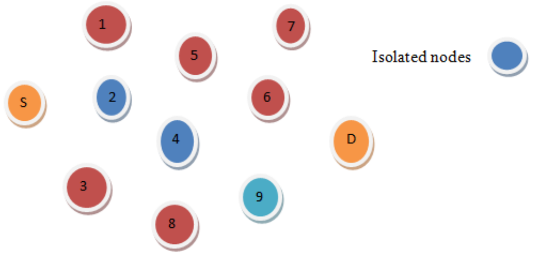

Fig 4: Isolated existing path

In this figure after receiving reply message from the monitor node source node isolated existing path and find out new path for communication from source to the destination.

In our proposed work we deal with the throughput delay sensitive wormhole attack. Suppose we have a network in which number of nodes are present. There are two ways in which packets are transferred from source to destination. First of all source sends fake packets for the route establishment from source to destination. We can also say that source sends fake messages. Secondly source flood the packets in the network as data packets. The node which received data packets goes to the monitor node. In this process source generate ICMP packets that flood in the network. The nodes which receives them as a data packet goes to the premicous node or monitor node. After receiving monitoring packets other nodes than monitor nodes in the network, they start monitoring intermediate nodes from source to destination. Monitor node sends packets on route. It does not send data packets but send random packets in the network. Now the nodes which receive the packets forward it to the destination and consider that path as a route. But the monitor nodes also monitoring those nodes which drop the packet that is malicious node dropped the packets or send it to the destination through other paths. Monitoring nodes detect that node which further does not send it to the destination. So the nodes which detect the malicious node reply to a source node expect route node so that source isolate the path and stop forwarding more packets.

4. ALGORITHM

```
Start ( )
  1.  Deploy the wireless ad hoc network with fixed number
      of mobile nodes and in fixed area
  2.  Select the shortest path between the source and
      destination using AODV routing  protocol
  3.  The source node send fake messages to destination to
      verify the route
To verify the route
{
            4.  Source flood the monitor mode in the network
            5.  The nodes after receiving the monitor mode
                message start monitoring  the route between
                source and destination
If (Malicious node ==exits)
{
            6. A The other nodes in the network send malicious
               node information to source
            7. B The source isolate the selected path
            8. C The source select the other best path
            9. Else
{
The source keeps on communicating with destination
}
End
```

5. TOOLS USED

For the implementation of the protocol NS2 tool has been used. Set the simulation environment various scenarios are used as following below: NS-2 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS-2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms. Queuing algorithm includes fair queuing, deficit round robin and FIFO. NS-2 started as a variant of the REAL network simulator in 1989. REAL is a network simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks. In 1995 ns development was supported by Defense Advanced Research Projects Agency DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. The wireless code from the UCB Daedelus and CMU Monarch projects and Sun Microsystems has added the wireless capabilities to ns-2.

NS2 Overview: The network simulator (NS), which is a discrete event simulator for networks, is a simulated program developed by VINT (Virtual Internetwork Test-bed) project group. It supports simulations of TCP and UDP, some of

MAC layer protocols, various routing and multicast protocols over both wired and wireless network etc.

Depending on user's requirement the simulation are stored in trace files, which can be fed as input for analysis by different component:

- A NAM trace file (.nam) is used for the ns animator to produce the simulated environment.
- A trace file (.tr) is used to generate the graphical results with the help of a component called X Graph.

5.1 Problem Implementation

Network Deployment

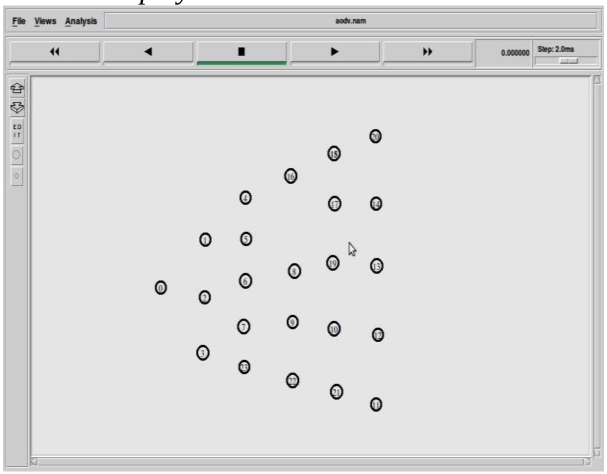

Fig 5: snapshots of initialization of network

The source node is sending the route request packets to its adjacent nodes to establish path to the destination. Every node on the network receive the packets.

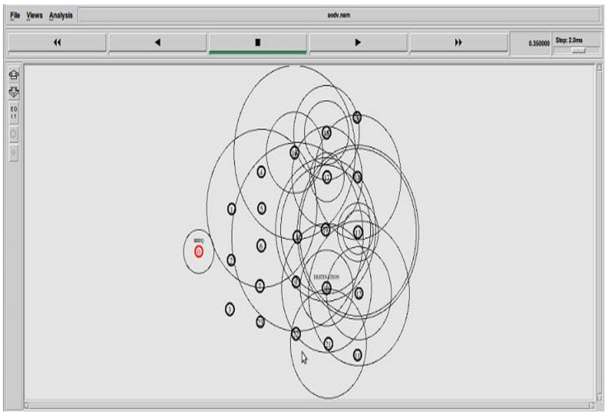

Fig 6: Snapshots of source node sending request packet

The adjacent nodes which is having path to destination will reply back with the route reply packets.

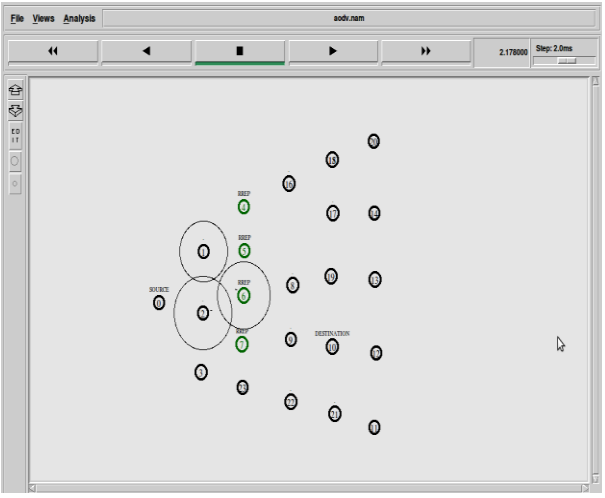

Fig 7: snapshots of sending reply to the source node

The source node selects the best possible path to destination on the basis of hop count and sequence number.

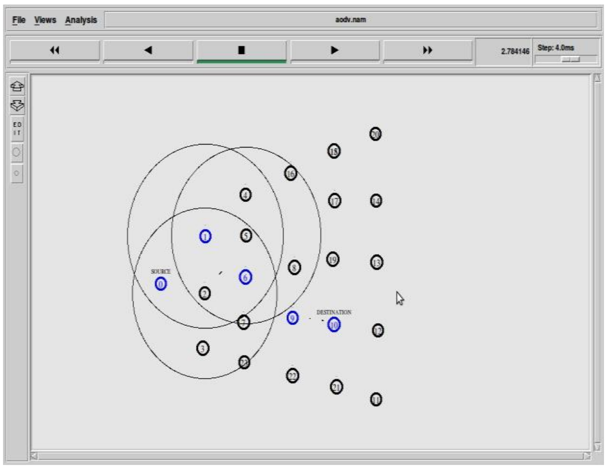

Fig 8: snapshots of best path establish

The path which is selected between source and destination, is the optimized path. In the selected path malicious node exists which is responsible for triggering the selective packet drop attack.

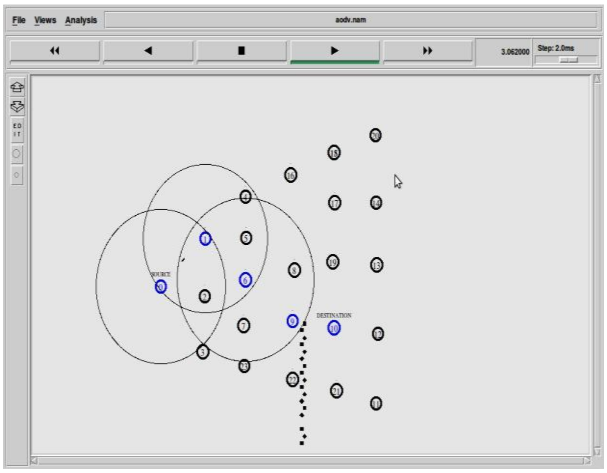

Fig 9: snapshot for find the malicious node

5.2 Solution Implementation

The network is deployed with the fixed number of mobile nodes.

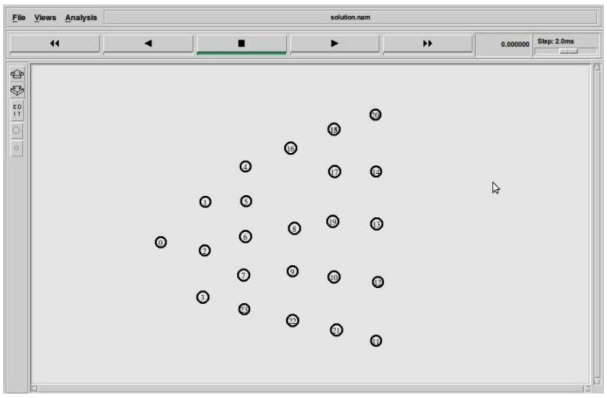

Fig 10: snapshot of network deployment

The source node floods the route request packets in the network. The source wants an optimized path to the destination. The optimized means the path between source and destination which is having minimum hop count and maximum sequence number.

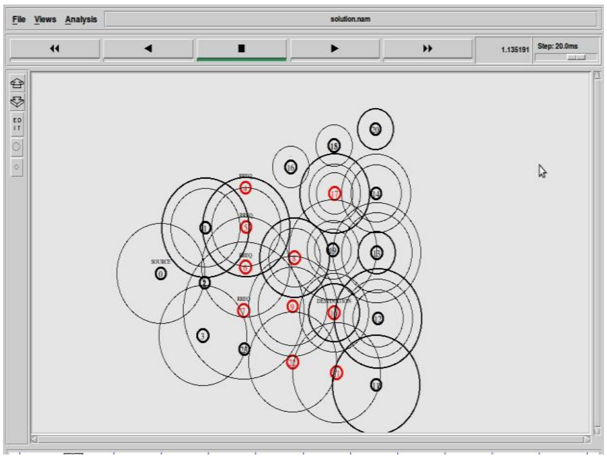

Fig 11: source node floods the route request packets in the network

The adjacent nodes to destination which is having path to destination will reply to source with the route reply packets.

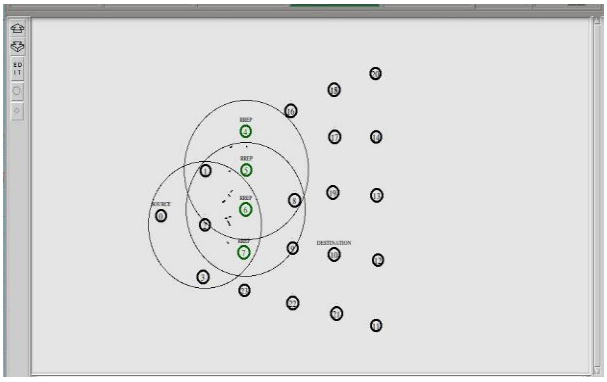

Fig 12: snapshot of path to destination

The best path between source and destination is selected on the basis of hop count and sequence number.

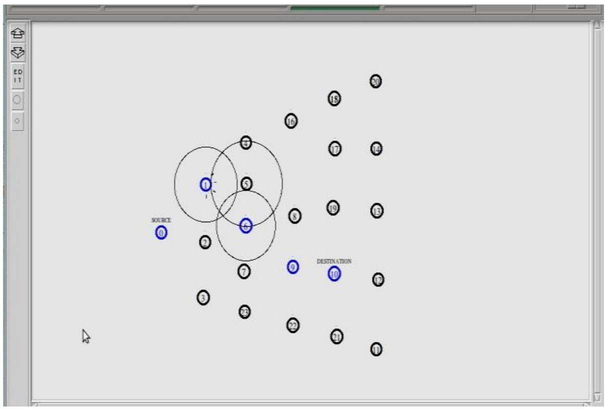

Fig 13: snapshot of best path between source to destination

The source node also floods the moniter mode messages in the network. The nodes when receives moniter mode messages will go in the moniter mode and start monitering the path between source and destination.

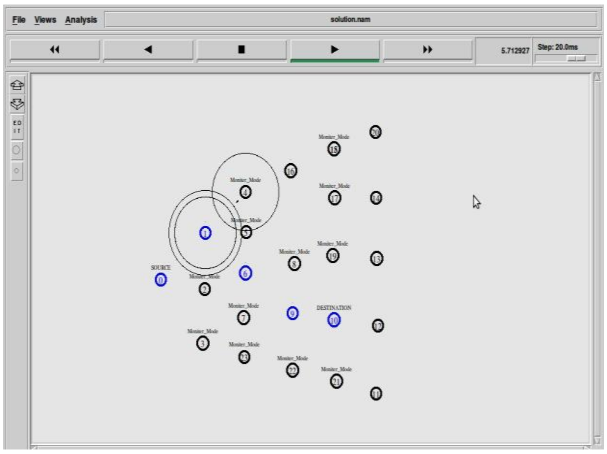

Fig 14: snapshot source node floods the monitor mode messages in the network

The other nodes in the network which receives monitor mode messages will detect the malicious node in the network and isolate the path between the source and destination. The source selects the other best possible path between source and destination

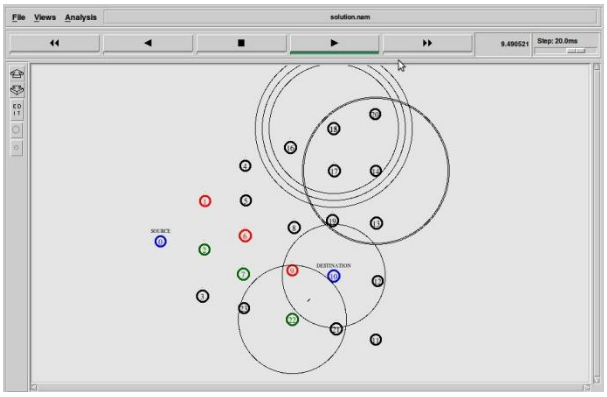

Fig 15: snapshot of sending packet through the other best possible path

6. RESULTS & ANALYSIS

The following three graphs can show the improvement in the performance graphs.

1.) In the figure, it is shown that graph of network delay. The network delay is more in the previous scenarios. The network delay is reduced in the new scenario. (Fig.16)

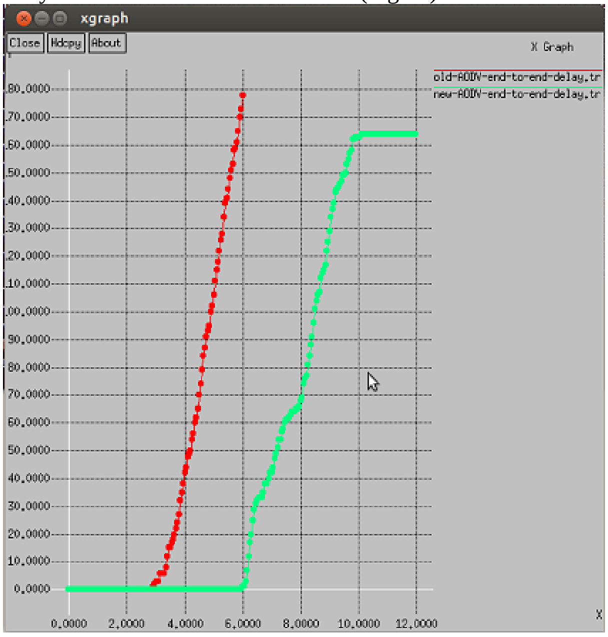

Fig 16: Delay Graph

2.) In the figure, it is shown that graph of packet loss. The packet loss is more in the previous scenarios. The packet loss is reduced in the new scenario. (Fig.17)

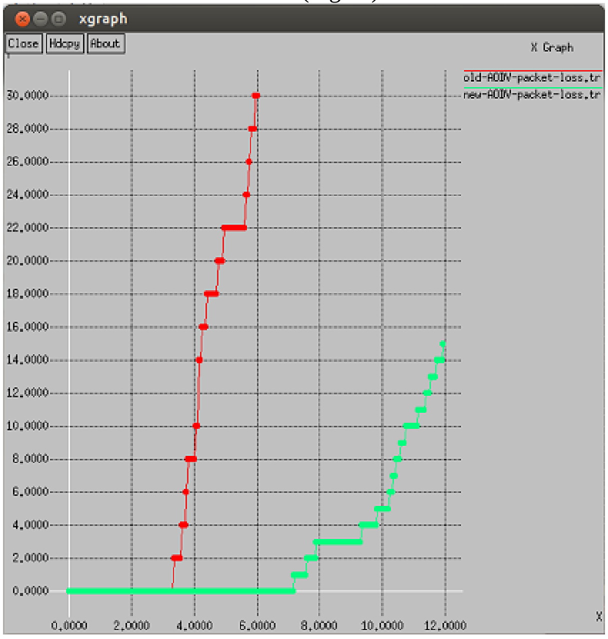

Fig 17: Packet loss Graph

3.) In the figure, it is shown that graph of Throughput. The network throughput is more in the new scenario. In the old scenario it will reduced due to selective packet drop attack in the network which is triggered by the malicious node. (Fig.18)

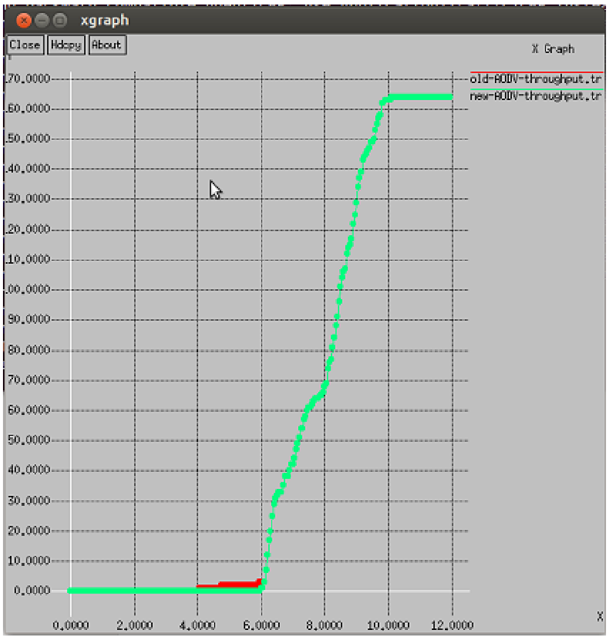

Fig 18: Throughput Graph

7. REFERENCES

[1] Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, “End to End Delay Analysis of Prominent On-demand Routing Protocols”, IJCST Vol. 2, Issue1, March 2011

[2] ABDUL HAIMID BASHIR MOHAMED, thesis, “ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS”2004

[3] Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, “An Intrusion Detection Tool forAODV-based Ad hocWireless Networks”, 2004

[4] Sevil Şen, John A. Clark, Juan E. Tapiador, “Security Threats in Mobile Ad Hoc Networks”, 2010

[5] Rusha Nandy, “Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme” Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)

[6] Wenjia Li and Anupam Joshi , “Security Issues in Mobile Ad Hoc Networks- A Survey”,2005

[7] Gene Tsudik, “Anonymous Location-Aided Routing Protocols for Suspicious MANETs”, 2010

[8] Karim El Defrawy, and Gene Tsudik , “ALARM: Anonymous Location-Aided Routing in Suspicious MANETs” , IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9, SEPTEMBER 2011

[9] Steven M. Bellovin and Michael Merritt “Limitations of the Kerberos Authentication”, USENIX – winter 1991

[10] Seung Yi, Robin Kravets, “Key Management for Heterogeneous Ad Hoc Wireless Networks” , 10 th IEEE International Conference on Network Protocols (ICNP’02) 1092-1648

[11] Pradeep kyasanur “Selfish MAC layer Misbehavior in wireless networks”, IEEE on Mobile Computing, 2005

[12] Yixin Jiang Chuang Lin, Minghui Shi, Xuemin Shen “Multiple Key Sharing and Distribution Scheme With (n;

t) Threshold for NEMO Group Communications”, IEEE 2006

[13] Caimu Tang ,Dapeng Oilver “An Efficient Mobile Authentication Scheme for Wireless Networks”, IEEE

[14] Tien-Ho Chen and Wei-Kuan, Shih, “A Robust Mutual Authentication Protocol for Wireless Sensor Networks ETRI Journal, Volume 32, Number 5, October 2010

[15] Sushma Yalamanchi and K.V. Sambasiva Rao “Two-Stage Authentication For Wireless Networks Using Dual Signature And Symmetric Key Protocol” International Journal of Computer Science and Communication (IJCSC), n Vol. 2, No. 2, July-December 2011, pp. 419-422

[16] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada “On Alarm Protocol in Wireless Sensor Networks”, 2010

[17] S. Sharmila and G. Umamaheswari, “ Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012

[18] Priyanka Goyal, Vintra Parmar and Rahul Rishi , “ MANET: Vulnerabilities, Challenges, Attacks, Application” , IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011

[19] Donatas Sumyla, **“** Mobile Adhoc Networks**” ,** IEEE Personal Communications Magazine, April 2003, pp. 46-55.

[20] Amandeep Singh Bhatia and Rupinder Kaur Cheema ,“Analysing and Implementing the Mobility over MANETS using Random Way Point Model” , International Journal of Computer Applications (0975 – 8887) Volume 68– No.17, April 2013

[21] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester , “ An overview of Mobile Adhoc Networks: Applications and challenges”, Sint Pietersnieuwstraat 41, B-9000 Ghent, Belgium ,2005

[22] Loukas Lazos, and Marwan Krunz, “Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks” Dept. of Electrical and Computer Engineering, University ofArizona, Tucson, Arizona, 2009

[23] Jiazi YI , “ A Survey on the Application of MANET”, 2005

[24] Ian D. Chakeres and Elizabeth M. Belding-Royer , “AODV Routing Protocol Implementation Design”, In C. E. Perkins, editor, Ad hoc Networking, pages 173.219. Addison-Wesley, 2004

[25] Rusha Nandy, “Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme” Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages: 1035-1043 (2011)

[26] Tien-Ho Chen and Wei-Kuan, Shih , “A Robust Mutual Authentication Protocol for Wireless Sensor Networks” ETRI Journal, Volume 32, Number 5, October 2010

[27] Vinit Garg, Manoj Kr.Shukla, Tanupriya Choudhury, Charu Gupta, “Advance Survey of Mobile Ad-Hoc Network,” IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011