Performance Analysis of DSR and AODV in Manets: Using WLAN Parameters

Devendra Singh
Department of Computer Science,
Amity University, Lucknow, India.

Vandana Dubey
Faculty, Dept. of Computer Science,
Amity University, Lucknow, India.

Shipra Sharma
Faculty, Dept. of Computer Science,
Amity University, Lucknow, India.

ABSTRACT
In these days it is no longer optional to have security solutions predictable for every type of organizations and individuals. Security is one of the main issues in the MANET in particular with respect to size and complexity of the network. The aim of the paper is to discuss special security aspects of MANET and relative study of the routing protocols such as AODV and DSR. The main task of this paper is to perform the experimental study which is based on simulation .This paper also discusses MANET network scenario which we implement in our simulation. In our simulation we use to implement AODV and DSR routing protocols and also did comparative study that which one is better with respect to different aspects.

General Terms
MANETs, AODV, DSR, OPNET.

Keywords
Throughput, Load, Delay, Retransmission Attempts.

1. INTRODUCTION
MANETs are very useful when infrastructure is not available or very expensive [1]. Main challenges in MANET is packet loses due to the transmission errors such as high bit error rate (BER) which causes higher packet loses, hidden terminal problem is also associated with the MANET which creates increased collisions, presence of interference in the surroundings is also a major factor, frequent path breaks also occurs due to the mobility of nodes and wireless channels are more error prone as compared to wired channels [2]. The occurrence of interference is when an intermediate or destination node in a route disappears from the network range. When a path breaks occurs it is important that a routing protocol efficiently seeks to learn new available paths and builds a new topology so that reliable connections are established. If the network load causing overhead is lowered then the overall performance of MANET will be increased. Mobility management is extremely important aspect of MANET it justifies the need for efficiency in any MANET routing protocols [3]. It is correct that the wireless channel is accessible to both network users as well as to attackers. There is no well defined rule or place where traffic from different nodes should be monitored or access control mechanisms can be enforced. Due to this way there is no any defense line that separates inside network from the outside network. Due to this way the existing ad hoc routing protocols, like Dynamic Source Routing (DSR) and Ad Hoc On Demand Distance Vector (AODV are assumed to be trusted. As a result, an attacker can become a router and disrupt network operations).

2. PROTECTING MOBILE ADHOC NETWORKS
MANETs follows open peer-to-peer architecture which has many inbuilt drawbacks. In case of wired networks there are dedicated routers but in case of mobile ad hoc network each mobile node acts as a router in order to forward packets from one node to other node. In mobile ad hoc networks there are no boundaries of wireless channel; it is accessible to both network users as well as to malicious attackers. Due to this there is no well defined infrastructure in order to deploy single security solution over MANET. The network topology in MANETs is highly dynamic due to free movement in the network like nodes can frequently join or leave in the network by their own will. Users need security services at any point due to the dynamic behaviors of mobile whenever they move from one place to another in the network. There are some characteristics of security solutions of MANETs which will clearly provide versatile security solutions with respect to network protection and also provide desirable network performance [4].

1. For securing an entire network security solutions should be implemented in various individual components of the network.

2. In MANETs security solutions should be implemented according to the various layers of the protocols and each layer should also have a defense mechanism to handle that particular situation.

3. Security solutions should also able to avoid threats from outsiders as well as insiders.

4. Security solutions like prevention, detection and reaction should be implemented.

5. Security solutions should be achievable and practical implement able when the networking scenario is highly dynamic.

3. ROUTING SECURITY IN MANET
Challenges associated with the related protocols in the MANET.MANET have become the most common research area in the recent years [5]. An ad hoc routing protocol is a rule that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. In ad hoc networks, nodes are not familiar with the topology of their networks instead they have to discover it. The basic idea is that a new node may broadcast its presence and should pay attention for broadcast by its neighbors. Security always implies the identification of potential attacks, threats and vulnerabilities of a certain system. Vesa Karpijoki [6] and Janne Lundberg [7] discussed some types of attacks that can be performed on MANET. Attacks can be classified into passive and active attacks. A passive attack does not

disturb the operation of a routing protocol, but only attempts to discover valuable information by listening to routing traffic, which makes it very difficult to detect. An active attack is an attempt to improperly modify data, gain authentication by inserting false packets into the data stream or modifying packets transition through the network. MANETS are very popular but they are also exposed to may types of attacks [8, 9]. Various attacks associated in MANET.

3.1 Black hole:
Malicious node advertises itself having the shortest path to the node whose packets it wants to interrupt.

3.2 Wormhole Attack:
In wormhole attack the attacker creates a tunnel. Attacker receives packet at one point and tunnels them to another point and then replies from the other end of the tunnel. Routing can be disrupted when routing control message are tunneled.

3.3 Spoofing Attack:
In spoofing attack, the attacker assumes the identity of another node and receives the messages of that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network.

3.4 Denial of service:
In this attack the network bandwidth is hijacked by a malicious node. For instance, a route request is generated whenever a node has to send data to a particular destination. A malicious node might generate frequently unnecessary route requests to make the network resources unavailable to other nodes.

3.5 Routing table overflow:
In this attack the attacker attempts to create routes to imaginary nodes. The goal is to have enough routes so that creation of new routes is prevented.

3.6 Impersonation:
A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table.

3.7 Energy consummation:
MANET has limited battery backup. Battery-powered devices save energy by transmitting only necessary data. Attacker attempts to consume the power of batteries by requesting routes or forwarding unnecessary packets to a node.

3.8 Information disclosure:
The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route. Several security schemes for MANETs have been proposed.

Table 1. Security Attacks on each layer in MANET[10]

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, black hole, Byzantine, flooding, resource consumption location disclosure attacks
Data link layer	Traffic analysis, monitoring disruption MAC (802.11), WEP weakness
Physical layer	Jamming, eavesdropping interceptions.

4. ROUTING PROTOCOLS IN MANET
Many different routing protocols have been developed for MANETS. They can be classified into two categories [11]:

4.1 Table-driven:
Table driven routing protocols also called proactive routing protocols. They always create up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

4.2 On demand:
Table-driven routing is source-initiated on-demand routing approach different from Table-driven. On demand routing protocols activated when there is a need [12, 13]. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Three main routing protocols for a MANET are destination-sequenced distance-vector routing protocol DSDV [14], AODV [15] and Dynamic Source Routing protocol DSR [16]. Effective operation of a MANET is dependent on maintaining appropriate routing information in a distributed fashion.

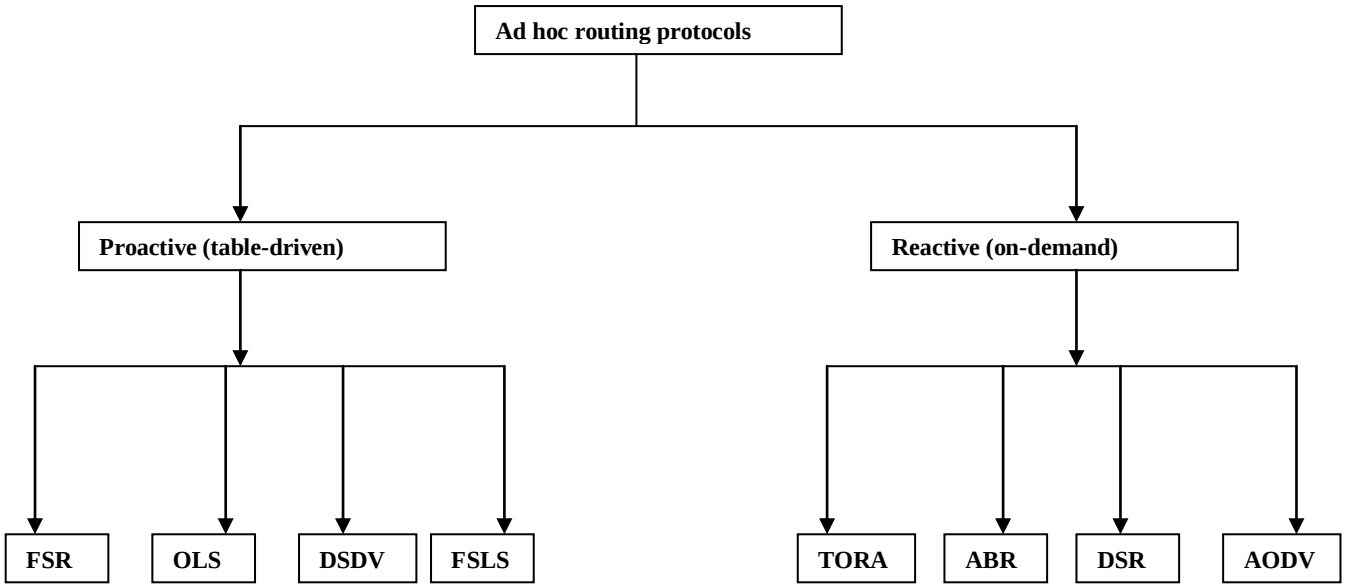

Fig 1: Routing protocols classification [11]

5. OPNET SIMULATION

There are various types of network simulation tools available to perform simulation tasks related to research work. OPNET simulator is one of them [17, 18]. OPNET simulator is one of the most famous GUI tool to perform research work in various types of networking fields and also used to simulate the routing protocols in different types of network scenarios .It is a network simulator which is used for multiple network solutions and applications e.g. research and development (R&D), network operation, network engineering, planning and performance management. It has been developed for modeling of different communication devices, technologies, protocols and in order to simulate performance of these technologies. At present OPNET is one of the most powerful and very useful tool in research field. The main task of this paper is to perform the experimental study which is based on OPNET simulation and we also implement comparative study of routing protocols with respect to different performance metrics parameters which are given below:

1. Delay,
2. Load (bits/s and packets/s), and
3. Throughput (bits/s and packets/s)
4. Retransmission Attempts(packets)

5.1 Network Scenario

In this simulation environment we create a network scenario of 15 and 48 nodes with the comparison of delay, load and throughput with respect to AODV and DSR routing protocols.

5.1.1 Simulation Parameters

Examined protocols	AODV and DSR
Simulation time	15 minutes
Simulation area (m x m)	1500 x 1500
Number of Nodes	15 and 48
Traffic Type	TCP
Performance Parameters	Throughput, delay, Load
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential (1)
Packet size (bits)	exponential (1024)
Transmit Power (W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

6. RESULT & ANALYSIS

We compare two routing protocols of MANET in the basis of various WLAN parameters. The measurement unit for these parameters is bits per second.

6.1 Throughput among AODV and DSR

In communication networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. The simulation graph of our experiment shows that

AODV has high throughput as compare to DSR. Throughput of DSR is high in small size network as compared to large size network.

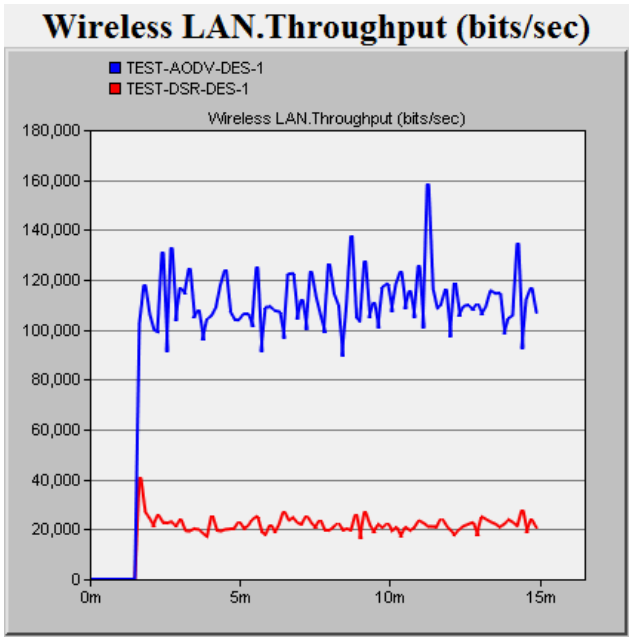

Fig 2: Throughput in 15 nodes environment

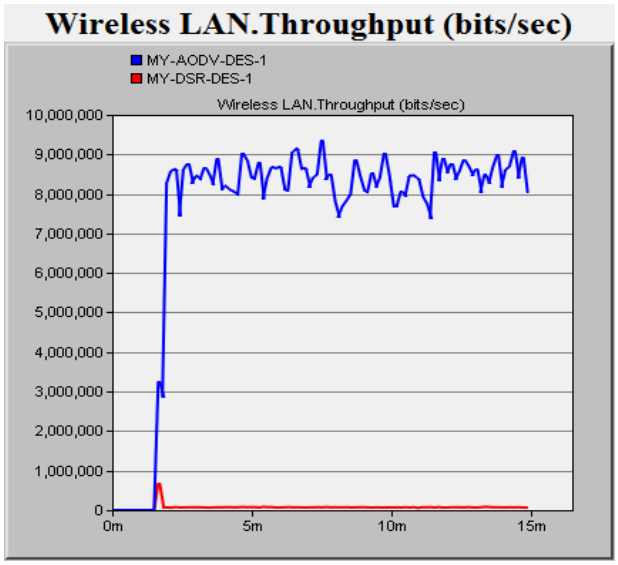

Fig 3: Throughput in 48 nodes environment

6.2 Delay among AODV and DSR

Network delay is an important design and performance characteristic of a computer network or telecommunications network. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another .Our simulation graph shows that AODV has low delay as compared to DSR.

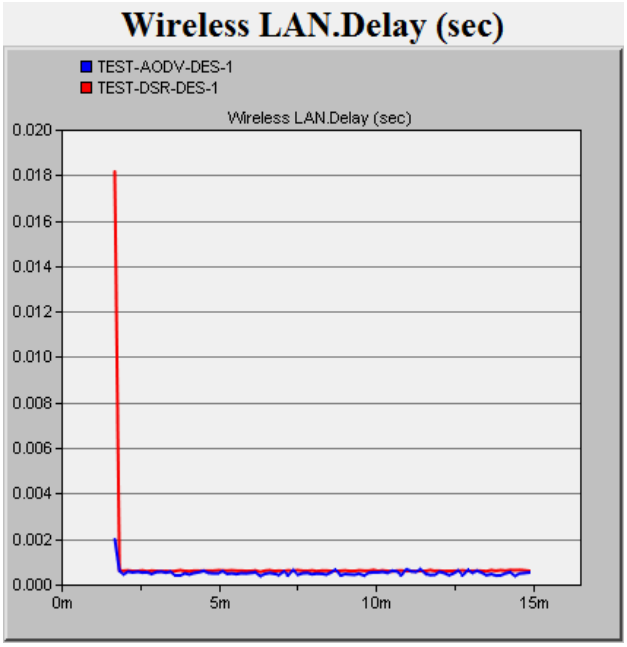

Fig 4: Delay in 15 nodes environment

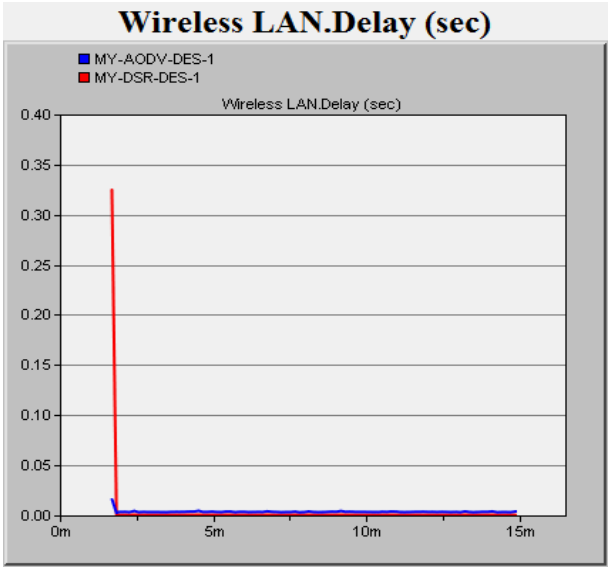

Fig 5: Delay in 48 nodes environment

6.3 Loads among AODV and DSR

Our simulation graph shows that DSR has low traffic load as compared to AODV. AODV also perform well as compare to DSR because byte overhead and packet overhead of AODV are less than DSR overhead. DSR has high load because of high number of its route discoveries and wide flooding network discovery. DSR load in less in small size networks as compared to large size networks.

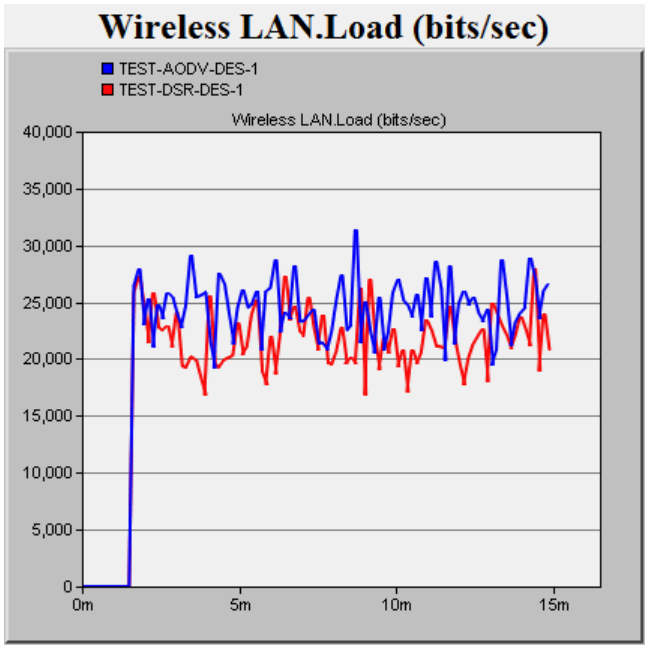

Fig 6: Load in 15 nodes environment

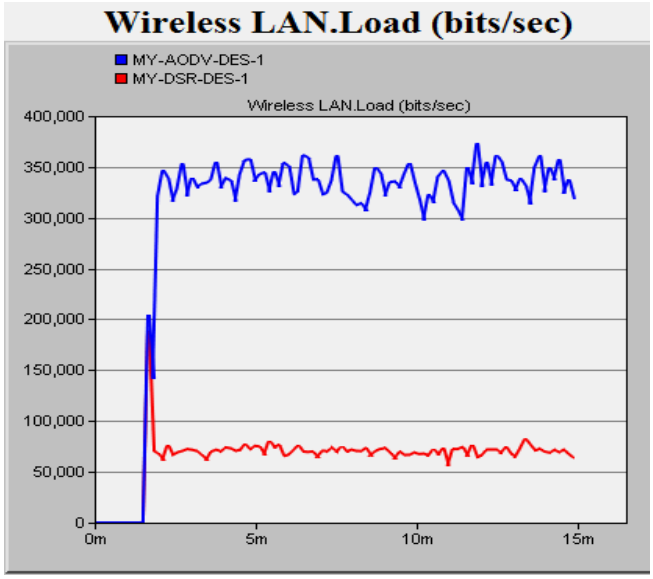

Fig 7: Load in 48 nodes environment

6.4 Retransmission Attempts among AODV and DSR

Retransmission attempt is high in AODV in large network as compared to small network. In case of DSR retransmission attempt is continuously low as compared to small network which is varying in the case of small network.

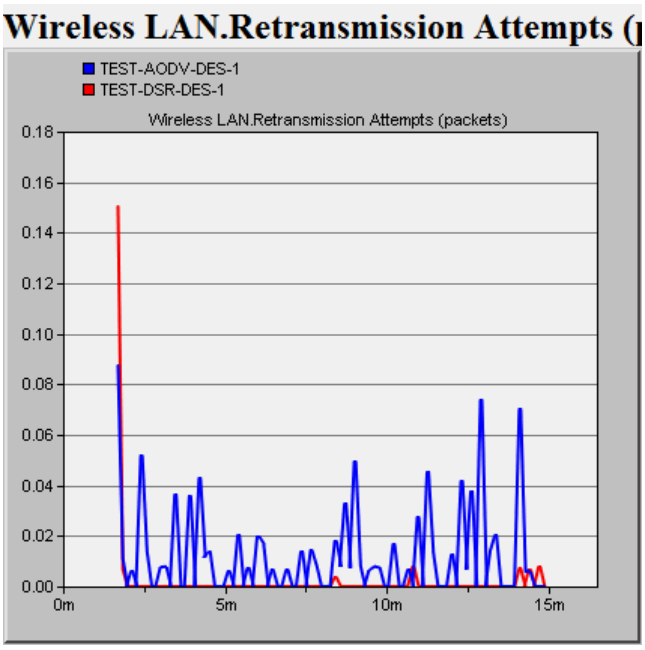

Fig 8: Retransmission Attempts in 15 nodes environment

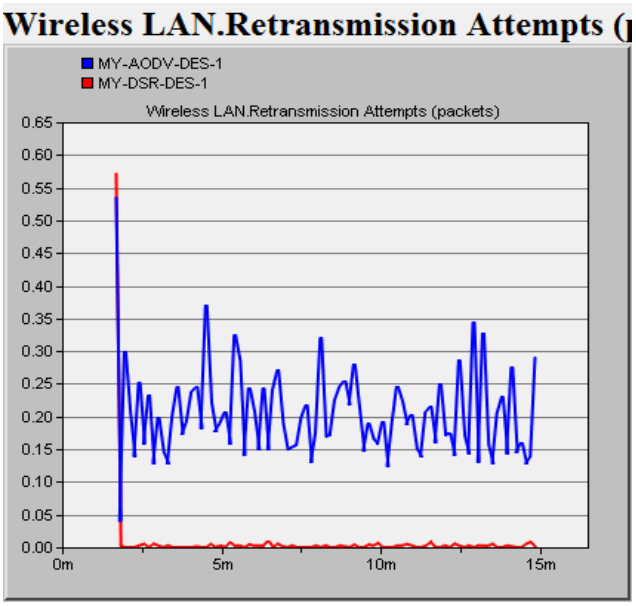

Fig 9: Retransmission Attempts in 48 nodes environment

7. CONCLUSION

This paper shows the impact of routing protocols on a typical MANET performance. The simulation results give a clear view of which routing protocols perform best in a given situation. The simulation results provide a clear view for implementing a MANET routing protocol, for example in particular AODV can perform well in medium size networks. In terms of reactive routing protocols, according to the results, DSR is best recommending for small networks, AODV for Medium networks. Finally we conclude if we have large

network than the better option is to use AODV as compared to DSR.

8. FUTURE WORK

Mobile Ad-Hoc Networks has the ability to deploy networks where the infrastructure in not mentioned or known. The MANET is a rising research area with practical applications. Routing security in wireless networks seems to be a difficult task that cannot easily be solved. It is not possible to find a general idea that can work efficiently against all kinds of attacks because every attack has its own separate characteristics. When deploying a MANET security is one of the important features that should be considered. A wireless MANET involves greater security problem as compared to wired networks because of its characteristics like open medium, dynamic topology, and absence of central authorities, distributed cooperation, and constrained capability. In our paper, we also find some of the points that can be further researched and explored in the future. However, in our paper we recognized that there are some drawbacks which should be improved and some of them are given below: Lacks of effective analytical tools especially in case of large scale wireless network setting.

9. ACKNOWLEDGMENTS

I would like to express my heartiest gratitude to our honorable faculty members for their suggestions, guidance, constant encouragement and enduring patience throughout the progress of the research paper. I would also like to express my sincere thanks for their advices and all-out cooperation.

10. REFERENCES

11. H. Pucha, S. M. Das, Y. C. Hu, "The Performance Impact of Traffic Patterns on Routing Protocols in Mobile Ad Hoc Networks", Journal (COMNET), vol. 51(12), pp. 3595-3616, August 2007.

[2] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Low price Edition, Pearson Education, 2007.

[3] X. Hong, K. Xu, M. Gerla, "Scalable Routing Protocols for Mobile Ad-Hoc Networks" IEEE Network Magazine, Volume-16, Issue-4, pages: 11–21.

[4] B. Schneier, Secret and Lies, Digital Security in a Networked World, Wiley, 2000.

[5] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91.

[6] V. Karpijoki, "Security in Ad Hoc Networks," http://www.hut.fi/~vkarpijo/netsec00/netsec00_manet_sec.ps

[7] J. Lundberg, "Routing Security in Ad Hoc Networks,"Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html

[8] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[9] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

[10] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Department of Computer Science and Engineering, Florida Atlantic University, http: / / students. fau.edu/ jchen8/web/paper s/SurveyBookchapter.pdf.

[11] D. P. Agrawal and Q.-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole Publishing, Aug. 2002.

[12]C.E.Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routinsg," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.

[13]C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[14] Perkins Charles E., Bhagwat Pravin: Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, London England UK, SIGCOMM 94-8/94.

http://www.cise.ufl.edu/~helal/6930F01/papers/DSDV.pdf

[15]C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003..

[16]D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728 (Experimental), February 2007.

[17] M.K. J. Kumar, R.S. Rajesh, "Performance Analysis of MANET Routing Protocols in different Mobility Models" IJCSNS International Journal of Computer Science and Network 22 Security, VOL.9 No.2, February2009.

[18] Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com