Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol 2, No.4, 2011

Malicious Node Detection in MANET

Sima
Department of Computer Science & Engg.
Karnal Institute of Technology & Management Kunjpura Karnal, India
E-mail: simasingh.2009@gmail.com

Ashwani Kush
Department of Computer Science
University College, Kurukshetra University Kurukshetra, India
E-mail: akush20@gmail.com

Abstract

A mobile ad hoc network consists of mobile wireless nodes. MANET is a self organized and self configurable network where the mobile nodes move arbitrarily. The mobile nodes can receive and forward packets as a router. Routing is a critical issue in MANET. In this paper a new scheme has been proposed for security. A comparative study for the performance of the protocols has been done varying in pause time using Network Simulator-2. Performances of the protocols have been compared by taking three metrics as; Packet Delivery Ratio, End to End Delay and Throughput.

Keywords: AODV, Average Delay, Performance Analysis, PDR, Simulation, Ad-hoc Network..

1. Introduction

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand alone infrastructure or centralized administration. Mobile Ad-hoc networks are self –organing and self configuring multihop wireless networks[K. Ramachandran 2003, M Abolhsan 2006] where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. [Mehran Abolhsan 2006, A.Kush et al 2009]. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. Ad-hoc networks are formed in situations where mobile computing devices require networking applications while a fixed network infrastructure is not available or not preferred to be used. In these cases mobile devices could setup a possibly short-lived network for the communication needs of the moment, Ad-hoc Networks are very useful in emergency search-and rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain. Routing is the act of moving information from a source to a destination. During this process, at least one intermediate node within the internet work is encountered. The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets).

1.1 Application of Ad-hoc Networks

Ad-hoc networks are suited for use in situation where an infrastructure is unavailable or to deploy one is not cost effective. One of many possible uses of mobile ad-hoc networks is in some business environments, where the need for collaborative computing might be more important outside the office environment than environment than inside, such as in a business meeting outside the office to brief clients on a given assignment.

A mobile ad-hoc network can also be used to provide crisis management services applications, such as in disaster recovery, where the entire communication infrastructure is destroyed and resorting communication quickly is crucial. By using a mobile ad-hoc network, an infrastructure could be set up in hours instead of

weeks, as is required in the case of wired line communication[H Bakht 2009]. Another application example of a mobile ad-hoc network is Bluetooth, which is designed to support a personal area network by eliminating the need of wires between various devices, such as printers and personal digital assistants.

2. Protocol Description

Whenever a packet wants to move from source to destination then a routing protocol is required that governs the data communication over the network. Two categories of protocols available are

2.1 Table-Driven routing protocols (Proactive)

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing. Some of the existing table driven[A.Kush et al 2005] or proactive protocols are: DSDV [Hogie L et al, 1997] OLSR [S. Demers] and ZRP [Z.Haas 1997].

2.2 On Demand Routing Protocols (Reactive)

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network. popular ones are ; DSR[D. Johnson, 2002], LAR1 [Vaidya, N.H. 1998] and AODV [Perkins C et al. 2003].

The proposed scheme has been incorporated using AODV [Perkins C et al. 2003]. It discovers routes on an as needed basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers. An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves. The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches. [Perkins C et al. 2003, D. Bertsekas 2004].

3. Proposed Plan

A New protocol has been proposed titled MAODV modifying AODV protocol. In this protocol a malicious node at a random location.

Then using NS-2 [available at isi.edu] simulator a comparative study of two protocols AODV and MAODV has been carried out for 10, 25, 35 and 50 nodes. The simulation has been performed using TCL scripts. The simulation results have been obtained with the help of three metrics as Packet delivery ratio, End to End Delay and Throughput. The results of AODV & MAODV are represented in the form of Graph. Using these graphs AODV & MAODV performance comparison has been made. To carry out the analysis a malicious node has been introduced in the script. This node when comes in direct communication contact with the routing nodes, results in hacker attack. This causes fall of packets. This performance has been studied using extensive simulations with varying scripts. The proposed scheme takes care of this node and in next study the authors are expected to remove this node and generate a new path. This new path will be secured and will result in stable and secured routing.

4. Simulation Model and Evaluation Metrics

The simulation experiment has been done using NS-2.34. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver, to create the statistical data track file and so on. Traffic Model Continuous bit rate (CBR) traffic sources are used. The source-destination pairs are spread randomly over the network. Simulation parameters are Shown in Table-1:

Table 1. Simulator Parameters:

Parameter	Value
Number of Nodes	10,25,35,50
Pause Value	500,400,300,200,100
Environment Size	650*650, 750*750 & 1000*1000
Traffic Pattern	CBR(Constant Bit Rate
Packet Size	512 bytes
Queue Length	50
Simulator	NS-2.34
Antenna Type	Omni directional

Performance metrics used are Throughput , End To End Delay and Packet Delivery Ratio which have been extensively discussed in many earlier versions. [P. Kumar et al 2008, L. Layuan et al 2007 and Fang et al 2004]

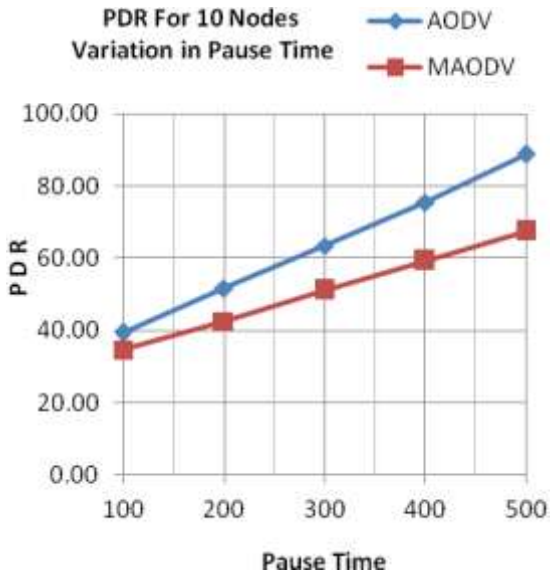
5. Simulation Results:

A comparative analysis of the performance metrics generated from all simulation, over AODV and MAODV routing protocols has been shown in graphs. An Attempt has been made to compare the two protocols under the same simulation environment.

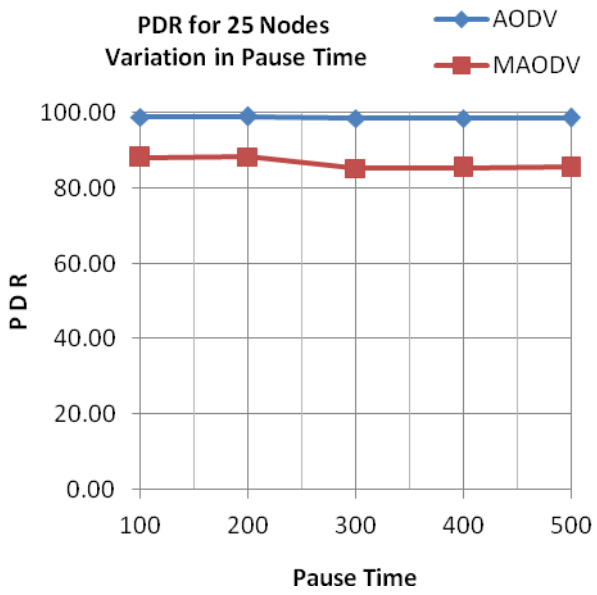
5.1Packet Delivery Ratio

The ratio of delivered packets is an important as it describes the loss rate that will be seen by the transport protocols, which in turn affects the maximum throughput that the network can support. The performance of the protocols decreases as the pause time decreases & the performance of the protocols increases as the pause time increases.

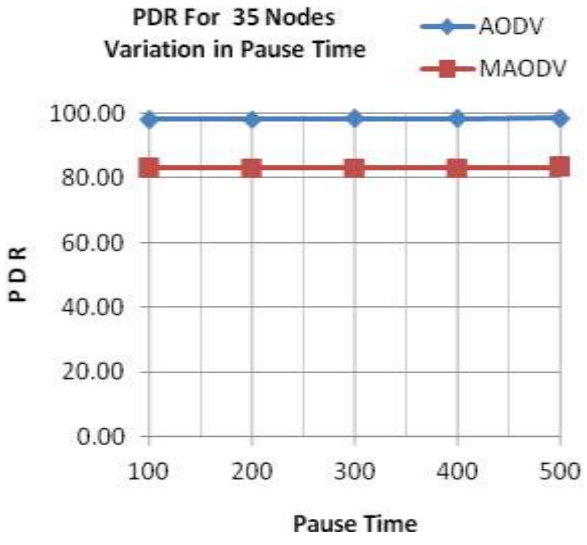
Graph 1-4 shows PDR using 10,25,35,50 nodes. Performance of 10 nodes is shown in Graph-1. It shows that increase in pause time causes increase in PDR in both AODV & MAODV. Performance of 35 nodes has been shown in Graph-3. As predicted the PDR in case of malicious attacks decreases. Though the PDR is consistent but there is fall at all pause times. Graph-4 performance of 50 nodes but the performance difference of AODV and MAODV is high as compare to Graph-3 which is for 35 nodes. It shows that as the no of nodes are increasing hacker affect also increases.



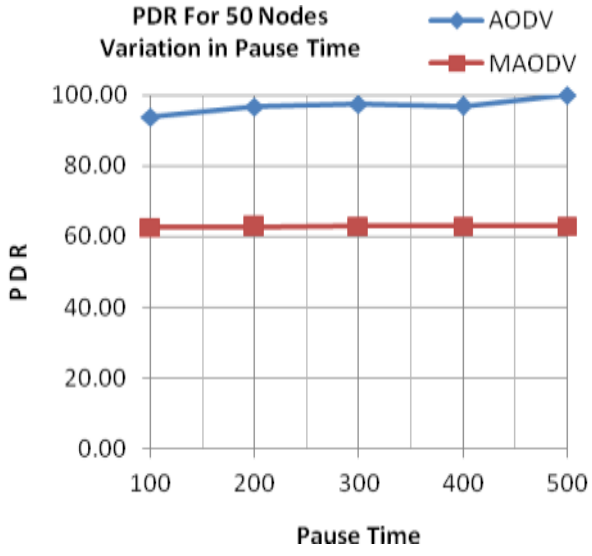
Graph 1: PDR Using Pause Time



Graph 2: PDR Using Pause Time



Graph 3: PDR Using Pause Time



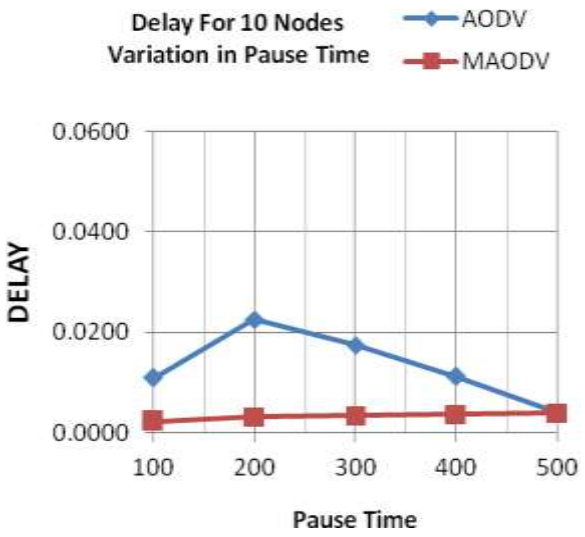
Graph 4: PDR using Pause Time

5.2 Average end to end delay

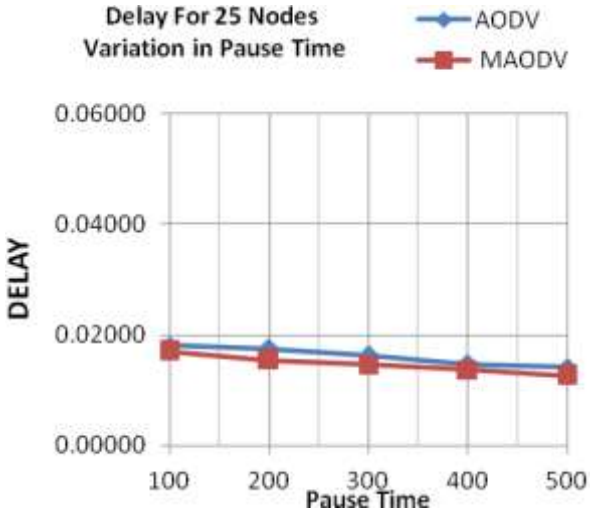
It can be seen that increasing in pause time results in significant change in the average end to end delay The ratio of delivered packets is an important as it describes the loss rate that will be seen by the transport protocols, which in turn affects the maximum throughput that the network can support. The performance of

the protocols decreases as the pause time decreases & the performance of the protocols increases as the pause time increases.

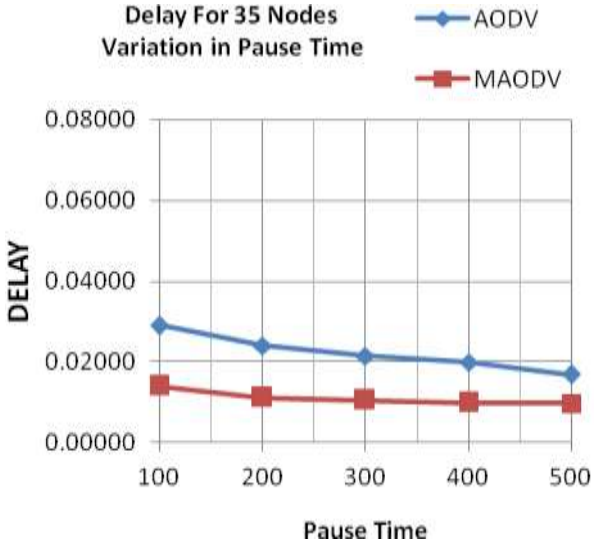
Graph 5-8 shows End To End Delay using 10,25,35,50 nodes. Performance of 10 nodes has been shown in Graph-5. It shows that the difference collapses as the pause time increasing same result for 25 nodes in Graph-6. But Graph-7 shows as the pause time increases MAODV results are improving.



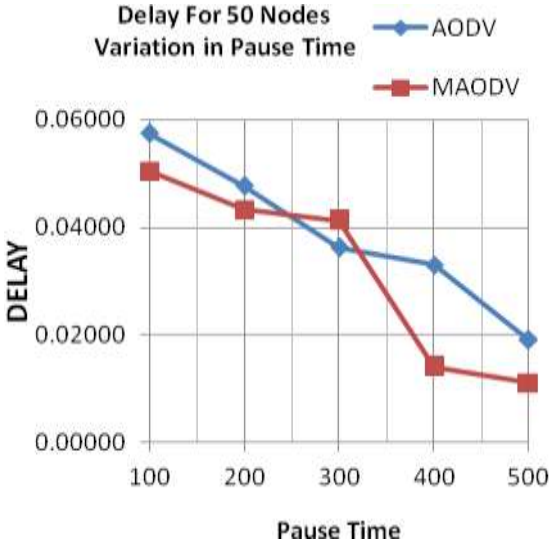
Graph 5: End To End Delay using Pause Time



Graph 6: End To End Delay using Pause Time



Graph 7: End To End Delay using Pause Time

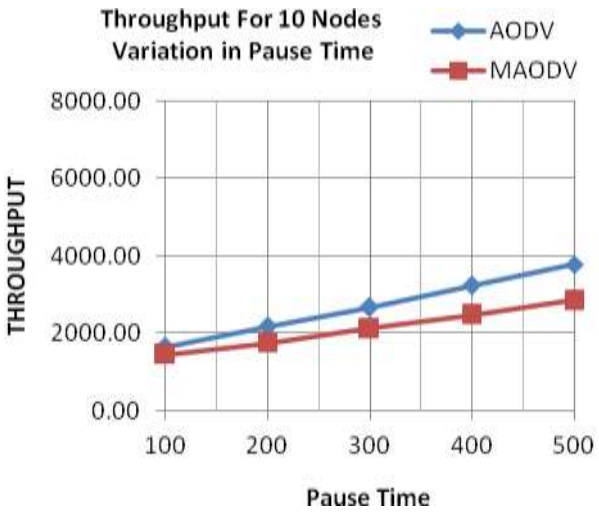


Graph 8: End To End Delay using Pause Time

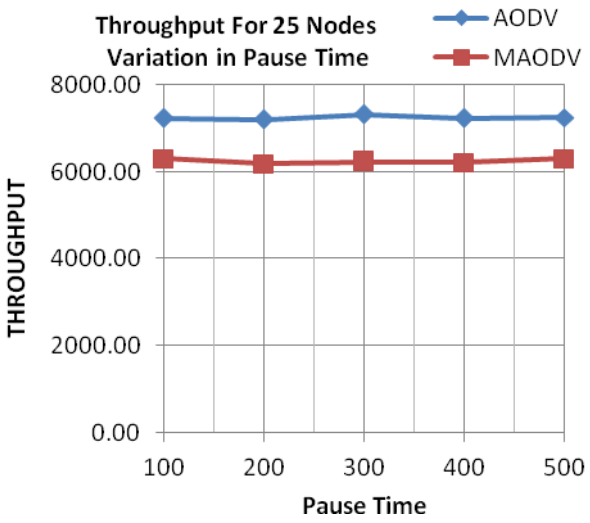
5.3 Throughput

It can be seen that the throughput for 10 ,25,35 & 50 nodes produces almost the same result as the pause time increase performance of protocols also increases for both AODV & MAODV .But AODV results are much better as compare to MAODV in every scenario..

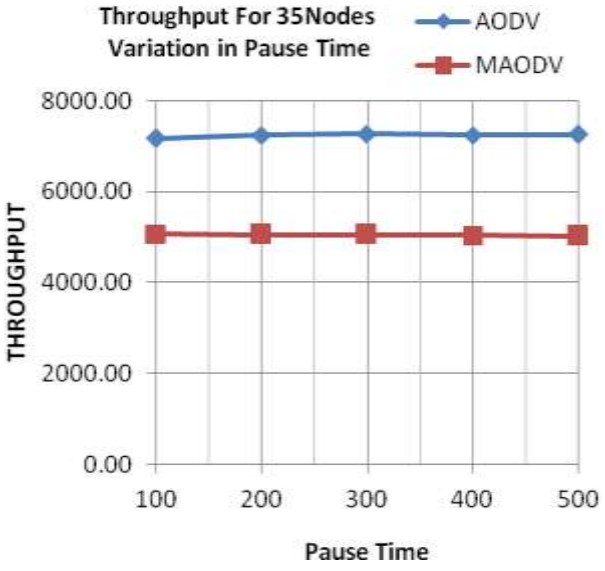
Graph 9-12 shows Throughput using 10,25,35,50 nodes. Performance of 10 nodes has been shown in Graph-9. As predicted the Throughput in case of malicious attacks decreases.



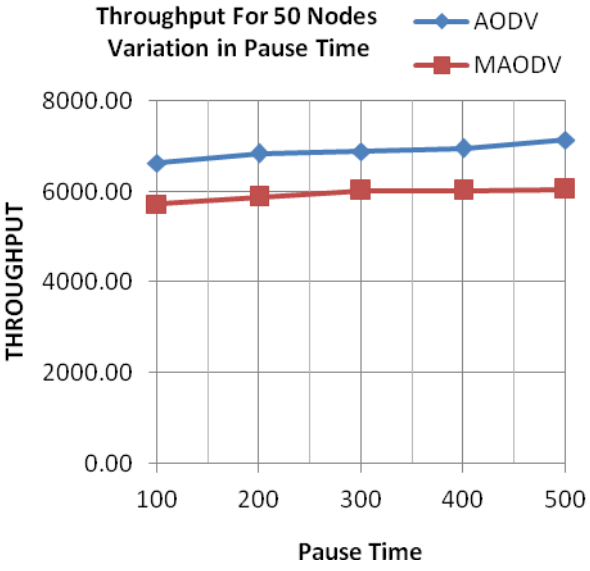
Graph 9: Throughput using Pause Time



Graph 10: Throughput using Pause Time



Graph 11: Throughput using Pause Time



Graph 12: Throughput using Pause Time

6. Conclusion and Future Scope

The area of ad-hoc networking has been receiving increasing attention among researchers in recent years, as the available wireless networking and mobile computing hardware bases are now capable of supporting the promise of this technology. Over the past few years, a variety of new routing protocols targeted

specifically at the ad-hoc networking environment have been proposed. This paper has presented a performance comparison of protocols for adhoc network routing protocol AODV, MAODV using a network simulator NS-2 with scenario consisting of different terrain sizes and pause time .AODV results are much better when nodes are less but as the nodes increased to 35 & 50 the difference in the performance of AODV & MAODV also increased. The routing Throughput of the two protocols are increased as pause time increases. The routing delay of the two protocols is increased as pause time decreases. In future this study can be increased for 75 & 100 nodes. Present study works only with one hacker, this study can be extended using more hackers. In Ad-hoc networks any node can enter in the network at any time but it is very difficult to detect which node is malicious. A new protocol can also be designed for detecting the hackers nodes and providing security to the network.

References

J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, *A performance comparison of multi-hop wireless ad hoc network routing protocols*, Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98), pp. 85-97, Oct. 1998.

Perkins, C.; Belding-Royer, E.; Das, S. *Ad hoc On-Demand Distance Vector (AODV)* Routing, July 2003.

D. Bertsekas and R. Gallager, *Data Networks*, PHI, Prentice Hall Publ., New Jersey, 2004

A. Kush, C.Hwang, *Proposed Protocol For Hash-Secured Routing in Ad hoc Networks*, in Masaum Journal Of Computing (Mjc) Volume: 1 Issue: 2 Month: pp 221-226, September 2009.

Krishna Ramachandran. Aodv-st. Technical report, University of California, Santa Barbara, USA. Krishna/aodv-st/(visited 2006-04-15)

Mehran Abolhsan, Tedeusz wysocki, and Eryk Dutkiewicz; *A review of routing protocols for mobile adhoc networks.* Technical report, Telecommunication and Information Research Institute", University of Wollongong, Australia, 2003.

Ko, Y.B., & Vaidya, N.H. , *Location Aided Routing (LAR) in mobile adhoc network* , in the Proceedings of the 4th annual ACM/IEEE International Conference on Mobile Computing and Networking. (MobiCom) pp.66-75, 1998

Zygmunt J. Haas. *A New Routing Protocol for the Reconfigurable Wireless Networks*, ICUPC'97, October 1997.

A. Kush, P. Gupta, R. Kumar*; Performance Comparison of Wireless Routing Protocols,* Journal of CSI, Vol. 35 No.2, pp 2-6, June 2005.

N.V. Trang, and X. Xing, *Rate-adaptive Multicast in Mobile Adhoc Networks*, WIMOB- 2005 Vol. 3, pp 352-360, 2005.

Humayun Bakht, ZATZ Publications, *Magazine computing unplugged*, available at http://www.computingunplugged.com/issues/issue200409/00001371001.html

P. R. Kumar, C. L. Reddy, and P. S. Hiremath, *A Survey of Mobile Ad hoc Network Routing Protocols*, Journal of Intelligent System Research, vol. 1,pp. 49-64, June 2008.

L. Layuan, Y. Peiyan, and L. Chunlin, *Performance evaluation and simulations of routing protocols in Adhoc networks*, Computer Communications, vol. 30, pp. 1890-1998, 2007.

Gao, Fang, Lu, Yuan, Zhang, Qingshun and Li, Chunli. *Simulation and Analysis for the Performance of the Mobile Ad Hoc Network Routing Protocols* Hebei Univ., Baoding 2007

Hogie L., Bouvry P., *An overview of MANETs Simulation, Electronic notes in theoretical computer science*, in lecture notes of Elsevier, doi:10.1016/j.entcs.2005.12.025. 2006.

David B. Johnson David A. Maltz Josh Broch, D. B. Johnson et al., *The dynamic source routing protocol for mobile ad hoc networks (DSR)*, Internet Draft, MANET working group, Feb 2002.

Stephanie Demers and Latha Kant, *Manets: perfrormance analysis and management*, Telcordia Technologies Inc. , Piscataway, NJ 08854. 2009