Efficient and Secure Protocol for Mobile Ad-hoc Networks

Meeta Singh
Research Scholar
Computer Science & Engineering
Bhagwant University, Ajmer, Rajasthan -305004, India

A.K.Yadav, Ph.D
Professor
Computer Science & Engineering
Bhagwant University, Ajmer, Rajasthan -305004, India

ABSTRACT

Mobile ad hoc networks (MANET) are currently the most evolving research area in wireless networks as well as mobile communications. Discovering a new path upon route failure has become hot research issue. Also current MANET protocols are being designed without security in mind, where it is assumed that all the nodes in the network are friendly. In MANET communications, every node in the network acts as a router and forwards the packet from one node to another. So to meet the growing needs of MANET communications the model should handle link failure efficiently and should also address security issues. New protocol to resolve link failure which is caused due to node mobility and also security issues in the current paper.

General Terms

Computer Network, Wireless Ad-hoc Network, Protocol.

Keywords

AODV, Ad-hoc Network, MANET.

1. INTRODUCTION

MANET is an autonomous and infrastructures less network where a number of wireless mobile nodes are communicate with each other. MANET is a group of mobile wireless nodes, which communicate with each other without any fixed networking infrastructure and without the need of any centralized administration. It was first designed for military purpose and very special areas such as emergency, rescue operation, airports, but later the demand for such wireless communications has increased, thereafter many protocols have been developed for mobile ad- hoc networks. Many routing protocols have been developed Mobile Ad hoc Networks (MANETs), but the most common among them are AODV and Dynamic Source Routing (DSR)[1].

These two protocols are the most widely worked on demand Ad-hoc network routing protocols. Later numerous other proactive and reactive routing protocols are Dynamic Destination-Sequenced Distance-Vector routing (DSDV)[2], Optimized Link State Routing (OLSR)[3], Dynamic MANET On-demand Routing (DYMOR), Signal Stability based Adaptive routing (SSA)[4], and other hybrid routing protocols such as the Zone Routing Protocol (ZRP), Hybrid Wireless Mesh Protocol (HWMP)[5] etc. MANET is having wide range of protocols, which are supporting different level feature and function for communication with security and efficiency.

2. RELATED WORK

There are two reasons of route failure in the MANET namely node mobility and wireless link collisions on routes (i.e., false route failure). If the packet delivery loss is due to the latter,

unnecessary route reestablishment will degrade the network performance[6]. This algorithm proposes a node movement detection scheme that can predict false route failures and prevent unnecessary route reestablishments by referring to changes in its neighborhood. In this mechanism, every node can determine its movement based on its neighbor table and decide whether to retransmit a failed packet or to discover an alternate route. The HELLO message is modified by adding an M flag bit to it. Every node in the network periodically broadcasts modified HELLO messages to its neighbors via 1-hop flooding. If a node receives a HELLO message with the M flag bit set to1, it updates its neighbor table and makes a prediction on its movement by calculating changes in its neighborhood. This algorithm focuses on network parameters like throughput (for the static chain topology) and packet delivery ratio (PDR).

In this section, discuss briefly about AODV[7] and DFRP[8]. Major drawback of most of the protocols is that they do not address the link failure problem. Many routing protocols have been proposed to address link failure problem. Ad-hoc on-demand distance vector (AODV) is one these protocols which has been widely used as it can quickly adapt to dynamic link environments. AODV is a reactive on-demand routing protocol, where information is transmitted only on demand. In AODV when the link between the host node and the destination node fails, route discovery process is initiated to find the destination node. Then a route discovery request (RREQ) packet is forwarded until the destination node is found. Also this method avoids receiving redundant copies of RREQ by recording the address of the neighbor which sends the request. But the major drawback of this protocol is the route discovery process is re-initiated from the source node. Route disconnection and also route discovery from the initial node brings a negative impact on packet delivery. So to improve the overall efficiency of the network, it is very important to predict the link failure. So, in this paper new supported protocol propose to use a link prediction algorithm to resolve this issue. We also propose a secure AODV to resolve the issues of security.

Also, we shall discuss briefly about how the DFRP[9], [10] protocol works upon a link failure. DFRP protocol uses two mechanisms to predict the link breakage and take action before it happens. For prediction, it utilizes the link state prediction method to collect the current link signal strength status to detect link failure. For getting neighbors signal status, it utilizes beacon frames to find the node that has a stronger signal when compared to the current connection signal strength among neighboring nodes. Upon a positive reply, the current-node will divert the route to the stronger node. The major drawback of DFRP[11], [12] protocol is link failure and security, if none of neighbors has stronger signal

strength when compared to current route or it does not have a route to the destination node, then the protocol fails to forward data.

3. PROPOSED MODEL

3.1 Objective

Our proposed model is concerned with efficiency of handling the link failures and security of MANETS. Also our main objective is to reduce flooding of Route re discovery packets. To overcome the drawbacks of DFRP [13], [14] [15], [16] so propose a new supported ADOV-DFRP Broadcasting model

For enhancing the efficiency of the model, where utilize two mechanisms namely:

- Local Route Request (LRREQ)
- Upstream Notification (UN)

3.2 Local Route Request

Unlike AODV – DFRP local route request protocol which utilizes link state prediction method for predicting active links, protocol broadcast the Local Route Request to all the neighboring nodes to detect the signal strength and also if it has a route to destination. If the link state algorithm predicts a failure between two links, then LRREQ is broadcasted to all the neighboring nodes.
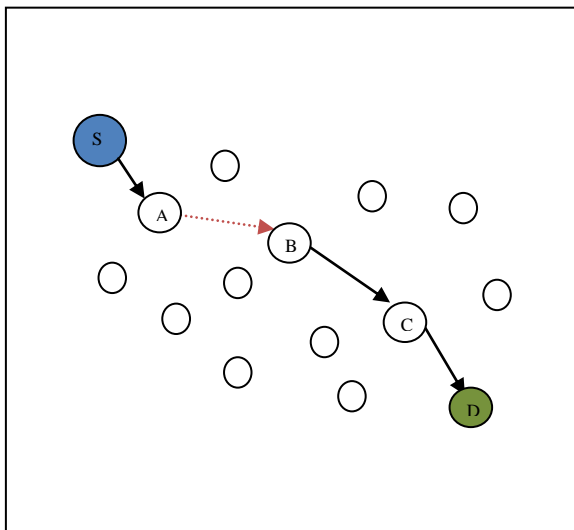

Figure: 1 Link A-B vulnerable to failure

In Figure 1 the link state algorithm predicts a link failure from node B, then node A instead of sending warning messages to the sender as in traditional AODV, it broadcasts LRREQ to all its neighbors except to the node from which it has received request as shown in Fig 2.

As show in Figure 2 'A' broadcasts LRREQ to all the neighboring nodes except to 'S', from which it has received request.
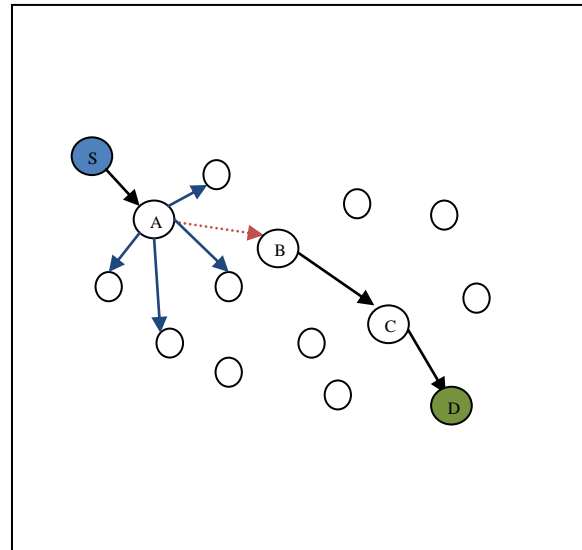

Figure: 2 Node A broadcasting LRREQ to all neighboring nodes

3.3 Up Stream Notification

If node A does not receive a positive response from its neighbors either because they have no route to the destination node or because they do not have a stronger signal when compared to current route, then node A will send a warning message one hop upstream i.e., previous node (node S as in Fig 3) indicating that the link will soon be broken. When the upstream node receives such a warning message from the downstream node, it circulates a Local Route Request (LRREQ) to all its neighbors except the upstream one and the process goes on until a new route is discovered as shown in Fig 3. The warning message includes the current signal strength and the address of the destination node. The warning messages are sent till a stronger node which has route to the destination is discovered.
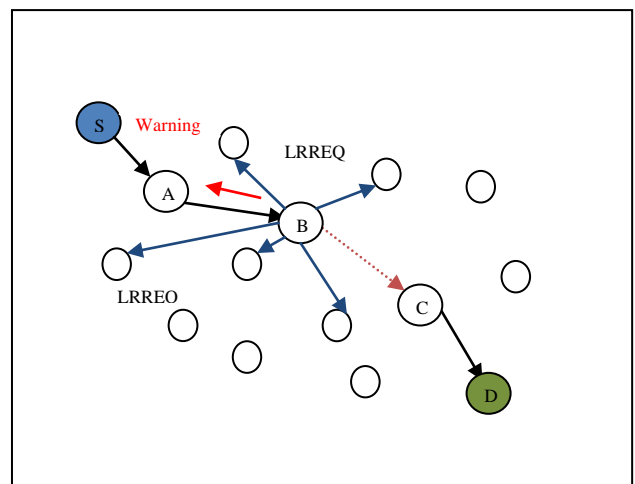

Figure: 3 UpStream Warning Messages

If one of the neighboring node responds with a route reply (RREP) i.e., it has a stronger signal than the current route and also a route to destination as shown in Fig 4. For example in Fig 4, node X has a stronger signal than the route B to C , because the link B to C is vulnerable to be broken, so now the route is redirected via node X as shown in Fig 5.
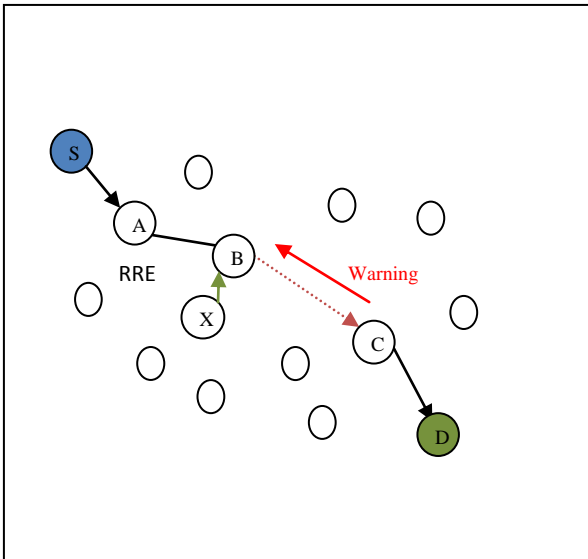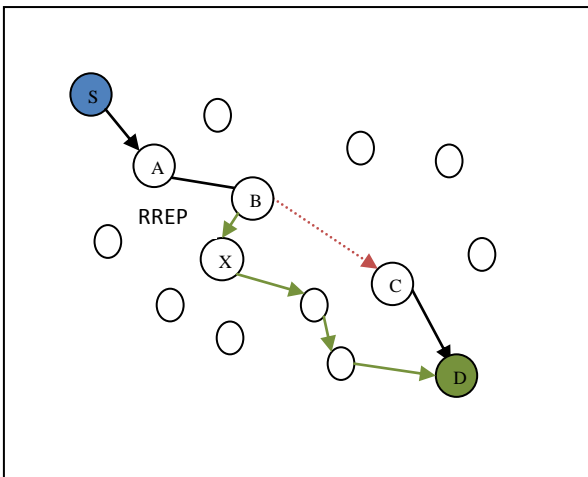
Figure: 4 Route Response

Figure: 5 Route Reconstruction

The entire process of route discovery is given in the form of a flow chart as shown in Fig 6.

4. SECURITY OF AODV

New propose Secure AODV[17], [18], [19] to address the security issues in MANETS like integrity, authentication and non-repudiation. Our secure AODV is a two step authentication process:

- Digital Signatures for authenticating the message
- Hash function to secure hop count information

As shown in Fig 7 the message in the data packet is signed digitally by the sender and hash

$h = H$ (Message+ Next Hop Information) is computed for the message along with the next hop information and sent to the next node in the route. The authenticity of the message is verified at the destination by verifying the digital signature. Also the hop count is protected by the use of hash function.
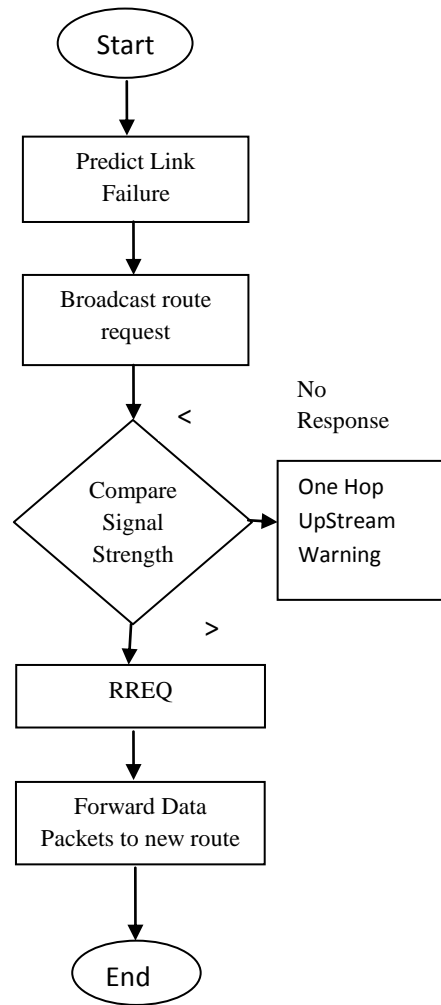

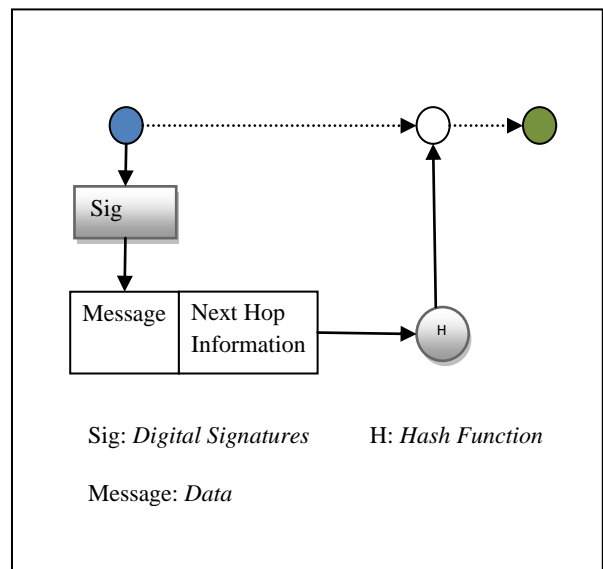**Figure: 6 Flow chart for AODV DFRP Broadcasting Protocol**

Sig: *Digital Signatures*   H: *Hash Function*

Message: *Data*

Figure: 7 Secure AODV

5. SIMULATION AND MODELING OF RESULTS

For simulating[20] the results for the new proposed model have conducted experiments using the ns-2 simulator which is as an open source tool. Where used the mobility and traffic generator tool, "cbrgen.tcl" and "setdest" scripts, to generate the traffic and mobility, which is provided along with the standard ns-2 distribution.

Table 1: Simulation Parameter

Parameters	Values
Simulation	Ns-2
Protocol	AODV
No of node	10, 20, 40 & 80
Movement Model	RPGM
Traffic source	Constant Bit rate (CBR)
Simulation area	1000 m x 1000 m
Simulation Time	200 sec
Max. Pause time'	5 sec
Node speed	5, 10, 20, 30 & 4020 m/s
No of connections	4, 8, 30 & 40
Group Size	5
Max. Distance to group	170
Group change probability	0.03
Group size deviation	1.0

Table 1 shows the results that have been generated for various cases. It has generated 4 scenarios and each scenario is tested various times as in Table 3.5, the speed tests for five times intervals (5, 10, 20, 30 and 40 m/s) are considered in each scenario keeping the rest of parameters constant. For example, for the first case, the number of nodes is 10, source connections are 4 and pause time is 5 but the speed varies from 5 to 40 in first case whereas in the next case the speed varies from 5 to 40 m/s. The rest of cases follow similar method until all five scenarios are tested.
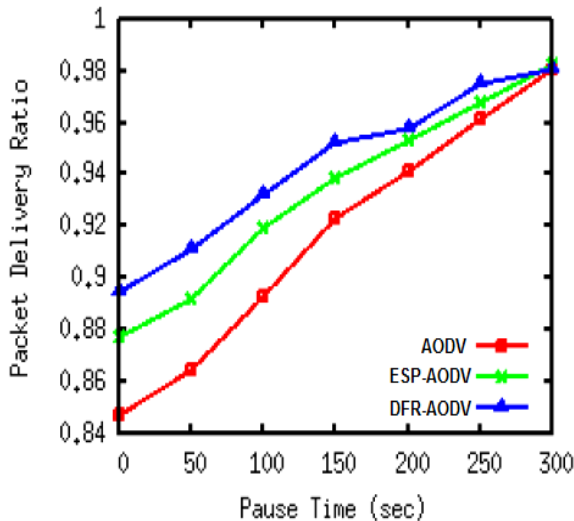

Figure: 8 Packet Delivery Ratio

In this experiment, where utilize CMU's wireless extension which is based on a two-ray ground reflection model and the MAC which used in IEEE 802.11. Random Waypoint mobility (RWP) is used as a mobility model for our experiment.

The simulation result brings out some important characteristic differences between the routing protocols. In all the simulation results AODV[21] outperforms the other protocols. This is because AODV is a proactive protocol and it pre determines the route in well defined manner. It uses destination sequence numbers to ensure loop freedom at all times and it offers quick convergence when the network topology changes.

According to the curves of Figure 8 and Figure 9, shown that ESP-AODV routing protocol over DFR-AODV[22] and AODV routing protocol can be improved, as the AODV routing protocol in this respect a very good performance, so do not leave us much room for improvement.
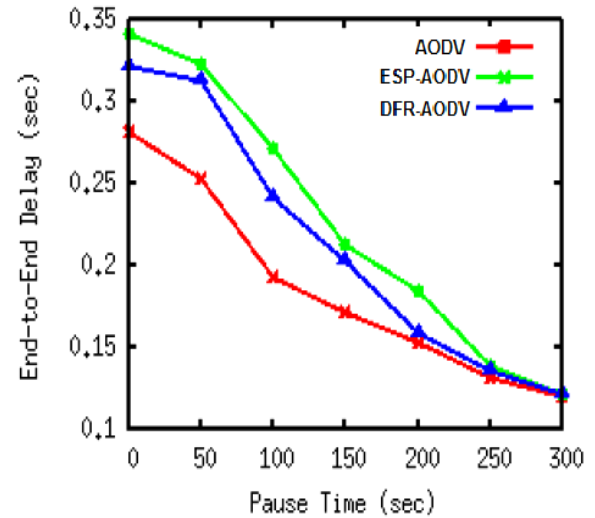

Figure: 9 End-to-End Delay

PDR and end-to-end delay are presented in Fig.8 and Fig.9. Maximum speed of each node is 10m/s. As expected, three improvements significantly enhance the PDR and reduce the end-to-end delay compared with AODV. ESP-AODV is better adapted to frequent topology changes in MANETs, and ensure higher PDR. Although DFR-AODV has longer end-to-end delay than AODV, it delivers more packets through alternate routes. It shows End-to-End delay as function of mobility speed, Node-disjoint ESP-AODV outperforms the rest.
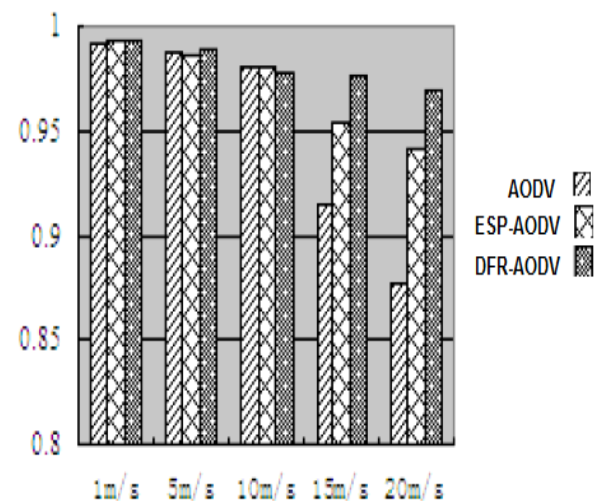

Figure 10. Maximum speed of node vs. PDR

Comparison of packet delivery ratio of each of the three protocols Figure 10, the packet delivery ratio and maximum speed of node simulation results show that, with increase in the number of nodes in the network, the network routing discovery and maintenance of the network becomes congested, AODV and ESP-AODV than DFR-AODV for better control of network congestion.
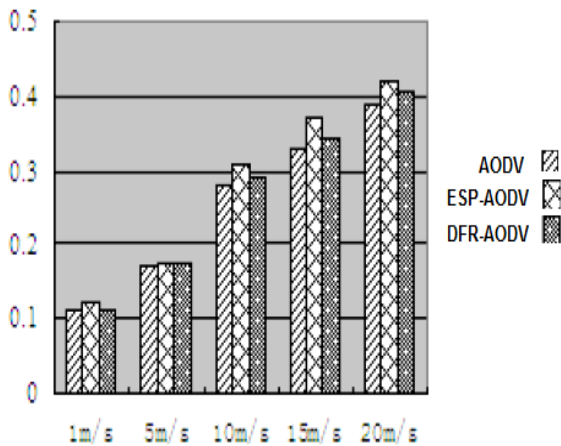

Figure 11. Maximum speed of node vs End-to-End Delay

PDR under different speeds of node are shown in Fig.10. In ESP-AODV, because of link failure prediction mechanism proposed, can always guarantee to have a higher PDR under different speeds of node. End-to-end delays under different speeds of node are shown in Fig.11. That shows ESP-AODV has a shorter delay than DFR-AODV. End-to-end delay differences are not too great between them.

6. CONCLUSION

In this paper, proposed an extension to the Ad-hoc On demand Distance Vector (AODV), namely Efficient and Secure Protocol (ESP). The ESP-AODV protocol will be a reliable solution to a number of current mobile ad hoc network shortcomings. In fact, the ESP-AODV protocol could function as an alternative solution and indeed an acceptable mechanism for the overall wireless link failure enhancement. This protocol is supposed to improve the overall network health. Future work, we are going to implement the proposed protocol to validate the models by an experiment tests using NS-2 simulator and evaluate the Models performance as well. Also, we are going to test suitability of the ESP Protocol to analyze the outcome of the result with different matrix and finally compare with it the AODV standard.

7. REFERENCES

[1] Tony Lasson & Nicklas Hedman (1998)"Routing protocols in wireless Ad hoc network" Lulea university of technology, Stockholm.

[2] Lee Kok Thong (2004) "Performance analysis of mobile ad-hoc routing protocols" thesis Naval post graduate college, Monterey, California.

[3] Bilal Mustafa & Umar Waqas Raja (2010) "Issues of Routing in VANET" School of Computing at Blekinge Institute of Technology.

[4] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications(1997)," IEEE Std. 802.11-1997,.

[5] Behrouz A. Forouzan(2008) Data communications and Networking, Networking series,Tata Mcgraw-Hill publishers.

[6] Imran Khan(2009) "Performance evaluation of Ad hoc routing protocols for Vehicular ad hoc networks" Mohammad Ali Jinnah University

[7] Perkins & E. Royer & S. Das, & K. Marina(2001), "Performance comparison of two on-demand routing protocols for ad hoc networks,'" in IEEE Personal Communications..

[8] Christoph Sommer & FalkoDressler (2009) " The DYMO Routing Protocol in VANET Scenarios" University of Erlangen-Nuremberg, Germany.

[9] T. Jacquet and P. Clausen. (2003, Oct.), "Optimized Link State Routing Protocol (OLSR) ", IETF RFC 3626

[10] Z.J. Hass, R. Pearlman, (1999) Zone routing protocol for ad-hoc networks, Internet Draft, draft ietf-manet-zrp-02.txt,

[11] Sanjeev Dhawan, "Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX", Faculty of Computer Science & Engineering, University Institute of Engineering and Technology (U.I.E.T), Kurukshetra University Kurukshetra (K.U.K)-136118, Haryana, India,The 2nd International Conference on Wireless ,Broadband and Ultra Wideband Communications (AusWireless 2007) IEEE, 2007

[12] Suhua TANG'and Bing ZHANG,(2004),"A Robust AODV Protocol With Local Update", ATR Adaptive Communications Research Laboratories, 2-2-2 Hikaridai, "Keihanna Science City", 6194288, Japan, IEEE, 2004

[13] Ammar Zahary and Aladdin Ayesh , "Analytical Study to Detect Threshold Number of Efficient Routes in Multipath AODV Extensions" Faculty of Computing Sciences and Engineering De Montfort University Leicester, LE1 9BH, UK, 2007

[14] Zheng Kai, Wang Neng LIU Ai-fang, "A new AODV based clustering routing protocol" Dept. of Computer CI Dept. East China Normal University Shanghai HP Shanghai, China, 200062 Shanghai, China, 200002, IEEE, 2005

[15] Rajiv Misra, C.R.Mandal, "Performance Comparison of AODV/DSR On-demand Routing Protocols for Ad hoc Networks in Constrained Situation" School of Infomation Technology Indian Institute of Technology,Kharagpur (India) IEEE, 2005

[16] Pirzada, A.A.; Wishart, R.; Portmann, M., "Multi-Linked AODV Routing Protocol for Wireless Mesh Networks," Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, vol., no., pp.4925-4930, 26-30 Nov. 2007.

[17] McDonald, A. B.; and Znabi, T.; . "A Path Availability Model for Wireless Ad Hoc Networks"., Proceedings of IEEE Wireless Communications and Networking Conference 1999 (WCNC.99), New Orleans, LA, USA, September 1999, pages 35-40.

[18] He, D.; Jiang, S. and Rao, J.; ."A Link Availability Prediction Model for Wireless Ad Hoc Networks"., Proceedings of the International Workshop on Wireless

Networks and Mobile Computing, Taipei, Taiwan, April 2000, pages D7-D11.

[19] Qin, L.; ".Pro-active Route Maintenance in DSR., M. Sc. Thesis, School of Computer Science", Carleton University, August 2001

[20] E. D. Kaplan (Editor). ."Understanding the GPS: Principles and Applications", Artech house, ISBN: 0890067937, 1996.

[21] Lee, S.-J.; Su, W. and Gerla, M.; .Wireless Ad Hoc Multicast Routing with Mobility Prediction., ACM Mobile Networks and Applications Journal (MONET), August 2001, Vol. 6, No. 4, pages 351-360.

[22] Rappaport, T. S.; .Wireless Communications: Principles and Practice (2nd 107 Edition)., Prentice Hall, ISBN: 0130422320, 2002.