Performance Evaluation of Routing Protocol for Mobile Ad-Hoc Network

[1] Chaitali Uikey

[1] School of Computer Science & IT, Devi Ahilya Vishwavidyalaya, Indore, M.P. 452017, India

Abstract

MANET is the compilation of wireless portable nodes which dynamically arranges a short term network without the use of any centralized administration or network infrastructure. Routing protocols used in mobile ad hoc networks must mechanically change to environments that can vary between the extremes of low mobility with high bandwidth, high mobility with low bandwidth. Various secure routing protocols are proposed for mobile ad hoc networks. In this paper, a performance analysis of three MANET routing protocols- AODV, DSR and Sec-AODV are performed. AODV routing protocols was selected on the basis of the intact simulations. Due to the needs of securing the routing in the wireless ad hoc networks, Sec-AODV protocol is proposed and is developed to add security to original AOD. It includes cryptographic operations based on private key cryptography for packet authentication that can have an imperative impact on the routing performance.

Keywords: *AODV, DSR, MANET.*

1. Introduction

Since their appearance in 1970's, wireless networks have become increasingly popular in the computing industry. In wireless networks, devices are connected and communicate with each other not by a clear medium, but by emissions of electromagnetic energy in the air. The most widely used transmission media support is radio waves. The IEEE 802.11 standards specify two operating modes in wireless network: infrastructure network mode and infrastructure less network mode. The infrastructure networks also known as Cellular network, have fixed and wired gateways they have fixed base stations which are connected to other base stations through wires. The transmission range of a base station constitutes a cell. Infrastructure less network is known as Mobile Ad hoc NETwork (MANET). These networks have no fixed routers. All nodes are accomplished of movement and can be connected dynamically in arbitrary manner. An ad hoc network, or MANET (Mobile Ad hoc Network), is a network composed only of nodes, with no Access Point. Here, messages are exchanged and dispatched between nodes [1]. In fact, an ad hoc network has the capability of making communications possible even between two nodes that are not in direct range with each other: packets to be exchanged between these two nodes are forwarded by intermediate nodes, using a routing algorithm. Various secure routing protocols are proposed for mobile ad hoc networks. Most of these protocols are analyzed by three usual techniques : security investigation, real network test and simulation. For the behaviour simulation and evaluation of these protocols we used the NS2 simulation tool. This paper is focused on the MANET routing protocols. In Section 2 provides brief explanations of related research works in this area. Section 3 provides explanations of the Mobile Ad Hoc routing protocols evaluated here while in Section 4 discuss details of the simulation with section 5 obtained results and Section 6 provides conclusions drawn from the obtained results.

2. Literature Review

Various methodologies employed in routing protocol involve the performance comparison of existing MANET protocols which are Ad-hoc On-Demand Distance Vector (AODV) [2] and Dynamic Source Routing (DSR) [3].

Perlman proposed a link state routing protocol that achieves Byzantine Robustness [4]. Although her protocol is robust but it requires a very high overhead associated with public key encryption. Zhou and Hass primarily discussed key management to facilitate efficient secure routing and they devoted a section to secure routing, but conclude that "node can protect routing information in the same way they protect data traffics"[5]. Dahill et. al. proposed ARAN a routing protocol for Ad-hoc Network that uses authentication and requires the use of a trusted certificate server. In ARAN, every node that forwards a route discovery or a route reply message must also sign it, which is very power consuming and cause the size of the routing messages to increase at each hop[6].

Zapata and Asokan proposed a secure version of AODV named SAODV to be appropriate secure solution for Ad-hoc networks [7]. They used signatures for authentication and hash chain for integrity of the routing message. The main disadvantage with the protocol is the use of Public key cryptography that requires a considerable amount of processing power and slows down the process to some extent. In SEAD hash chains are used in combination with DSDV-SQ. to authenticate hop counts and sequence numbers. At every given time each node has its chain [8].
The hash chain dived in to segments; elements in a segment are used to secure hop counts in a similar way in SAODV.

A performance comparison of AODV, DSR and DSDV is undertaken using the NS2 platform and it is concluded that AODV generally outperforms DSR and TORA [9]. Another study was conducted on the performance of a simple link state protocol, AODV and DSR; the authors conclude that AODV and DSR perform well when the network load is moderate while link state outperforms the reactive protocols when traffic load is heavy [10]. Also provide an analysis of DSR and DSDV is performed to study the effect of a real simulation environment on their performance [11].

3. Overview of MANET Routing Protocols

In the recent years, research efforts have been focusing on improving the performance of routing protocols in MANET. The Internet Engineering Task Force (IETF) created a MANET working group (WG) to deal with issues related to the complexity of constructing MANET routing protocols. The MANET WG coordinates the development of several candidates among the protocols including TORA, DSR and AODV. These protocols are classified into two classes based on the time when routing information is updated, the Proactive Routing Protocols (PRP) and Reactive Routing Protocols (RRP). The WG may also consider a converged approach such as hybrid routing protocols. Thus, the paper focuses on AODV and DSR (reactive) protocols.

3.1 Reactive Routing Protocol (RRP)

The reactive (on-demand) routing protocols represent the true nature of ad hoc network, which is much more active than infrastructure networks. Instead of periodically updating the routing information, the reactive routing protocols update routing information when a routing require is presented, consequently reducing the control overhead, especially in high mobility networks where the periodical update will lead to significant useless overhead.

3.1.1 Ad-hoc On Demand Distance Vector (AODV)

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. AODV is an improvement of the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. The on-demand routing protocols suffer more from frequent broken source-to-destination links than table driven routing due to the delay caused by on-demand route recalculation. AODV avoids such additional delay by using distance vector routing. There are some improved versions of AODV [12,13].

Interesting concepts of AODV:

The concepts of AODV that make it desirable for MANETs with limited bandwidth include the following: Minimal space complexity, Maximum utilization of the bandwidth, Simple, Most effective routing info, Most current routing info, Loop-free routes, Coping up with dynamic topology and broken links, Highly Scalable. Limitations/Disadvantages of AODV: Requirement on broadcast medium, overhead on the bandwidth, no reuse of routing info, it is vulnerable to misuse, AODV lacks support for high throughput routing metrics, high route discovery latency.

3.1.2 Dynamic Source Routing (DSR)

DSR is a reactive routing protocol for ad hoc wireless networks. It also has on-demand characteristics like AODV but it's not table-driven. It is based on source routing. The node wishing to send a packet specifies the route for that packet. The whole path information for the packet traversing the network from its source to the destination is set in the packet by the sender [14]. This type of routing is different from table-driven and link-state routing by the way routing decisions are made. In source routing, routing decisions are made by the source node.

4. Performance Evaluation, Simulation Environment

4.1 Performance Metrics

RFC 2501 describes the number of quantitative metrics that can be used for evaluating the performance of routing protocol for mobile wireless ad-hoc networks. In this paper, the general ideas described in RFC 2501 are followed [15]. The packet delivery fractions are most important for best-effort traffic. The normalized routing load will be evaluating the efficiency of the routing protocol. Finally, the normalized MAC load is a measure of the effective utilization of the wireless medium or data traffics. The next sections, defined the three quantitative metrics.

4.1.1 Packet Delivery Ratio

The packet delivery ratio is defined as the fraction of all the received data packets at the destination over the number of data packets sent by the sources'. This is an important metric in networks. If the application uses TCP as the layer2 protocol, high packet loss at the intermediate nodes will result in retransmissions by the sources which will result in network congestion.

Packet_Delivery_Ratio = Total_Data_packets_recvd / Total_Data_packets_sent

4.1.2 Normalized MAC Load

The number of routing, Address resolution protocol (ARP), and control (e.g., RTS, CTS, ACK) packets transmitted by the MAC layer for each delivered data packet. Essentially, it considers both routing overhead and the MAC control overhead. Like normalized routing load, this metric also accounts for transmission at every hop. The first metrics are the most important for best

effort traffic. The routing load metric evaluates the efficiency of the routing protocol. Finally the MAC load is a measure of effective utilization of the wireless medium by data traffic.

4.1.3 Normalized Routing Load

The normalized routing load is defined as the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes. This metrics disclose how efficient the routing protocol is. Proactive protocols are expected to have a higher normalized routing load than reactive ones. The bigger this fraction is the less efficient the protocol.

Normalised_Routing_Load = Total_Data_packets_sent/ Total_Data_packets_recvd

4.2 Simulation Environment

The simulator used to simulate the ad-hoc routing protocols in is the Network Simulator 2 (NS2) from Berkeley.

Simulation Framework Platform Used

Hardware: Pentium Core 2 Duo, 2.1 GHz, 3 GB RAM and 320 GB Hard Disk

Software: Gnorm compiler for C++

Operating System: Open Suse Linux 11.0 Version

Critical Simulation parameter: Other critical simulation parameters are simulation area, number of nodes, node pause time, payload sizes, and data rates.

- **Simulation area:** simulation area is 1000 meter.
- **Number of nodes:** The numbers of nodes used in this are 25, 50, 75, and 100.
- **Pause Time:** node pause time was also used by the node movement model to determine how long a node would wait prior to starting movement to a particular destination. Pause times were varied for all implementation to include 0,10,20,30,40,50,60,70,80,90, and 100 sec. the pause time of zero means that the node is in constant movement.
- **Payload Size:** packet sizes are used in this is 180 bytes.
- **Data rate:** the last critical simulation parameter to be discussed is the data rate. The data rate that has been used is 3 Mbps.

5. Result

5.1 Normalized Routing Load Vs Pause Time

The results from Figure 1, 2, 3 and 4 show that the routing overhead (by collecting the normalized routing load produced) decreased when reaching towards the end of the simulation. We could see that as the longer pause time taken in the simulations; the more stable the routings could be, either to or from all nodes involved. Hence, AODV still outperform the other two routing protocols. On the other hand, in lower pause time, AODV perform better than DSR and proposed Secure AODV but when moving to larger pause time (starting from 60 seconds), proposed Secure AODV gives better outputs towards the end; compared with AODV and DSR.

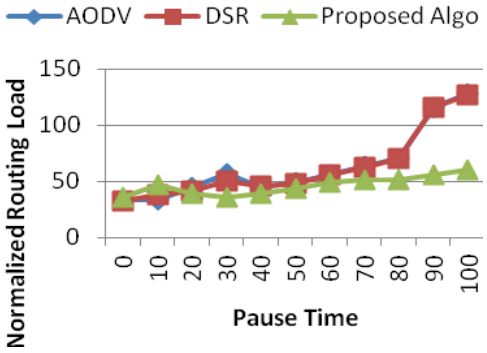

Fig.1 Normalized Routing Load for 25 Nodes

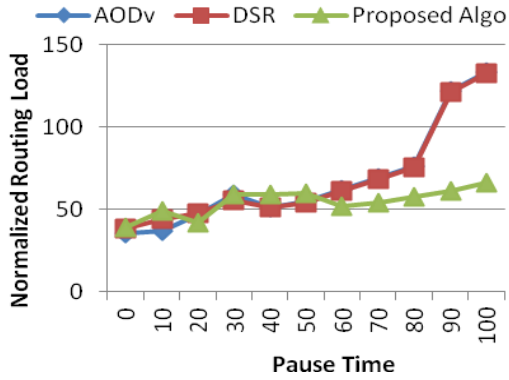

Fig.2 Normalized Routing Load for 50 Nodes

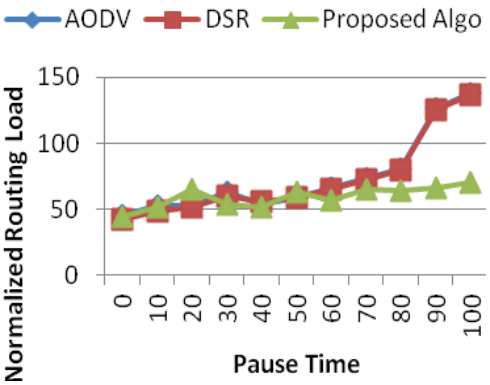

Fig. **3** Normalized Routing Load for 75 Nodes

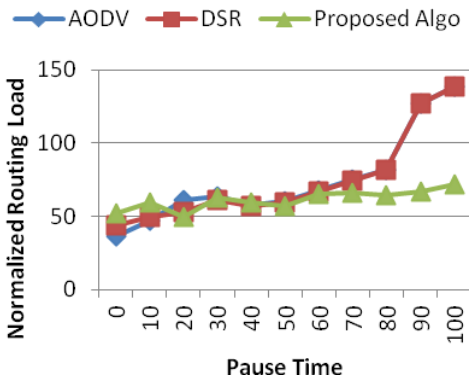

Fig.4 Normalized Routing Load for 100 Nodes

5.2 Normalized MAC Load Vs Pause Time

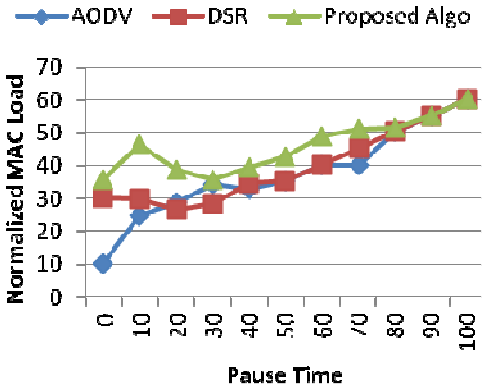

Fig. **5** Normalized MAC Load for 25 nodes

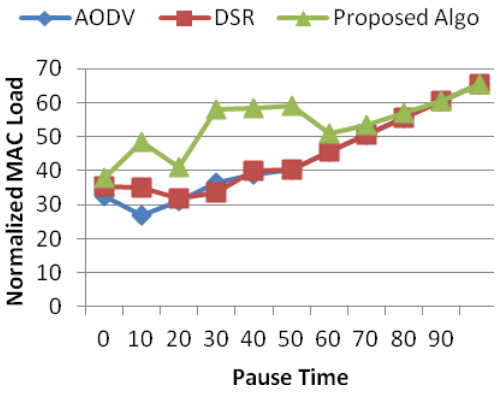

Fig. **6** Normalized MAC Load for 50 nodes

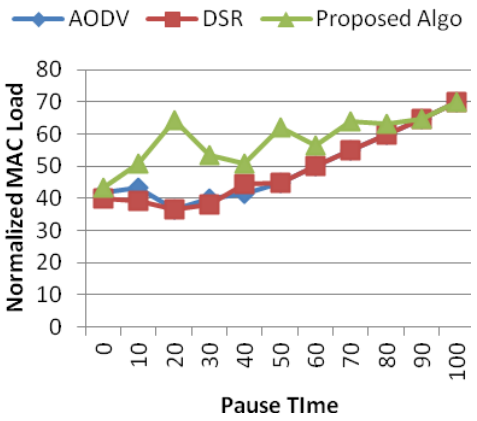

Fig.7 Normalized MAC Load for 75 nodes

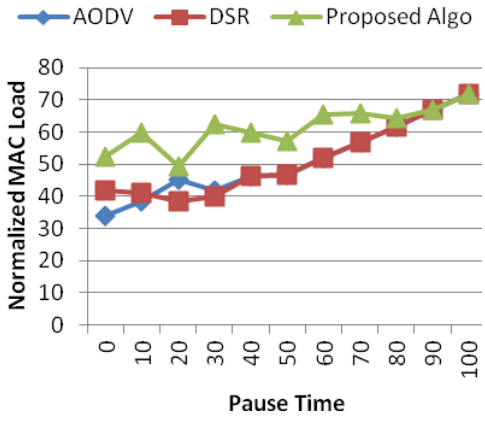

Fig. 8 Normalized MAC Load for 100 nodes

The results from Figure 5, 6, 7 and 8 show that the Normalized MAC Load is increased when reaching towards the end of the simulation. We could see that as the longer pause time taken in the simulations; the more stable the routings could be, either to or from all nodes involved.

5.3 Packet Delivery Fraction Vs Pause Time

From the Figure 9, 10, 11 and 12 the results shows that proposed secure AODV outperform both DSR and AODV in packet delivery fraction. It means that proposed Secure AODV produced more throughputs compared to DSR and AODV in total runtime of the simulations. At lower pause time, DSR and AODV perform a slight different reading, where AODV perform better because key value is changed at every node so overhead should minimum. In overall, packet delivery fractions readings are increased from lower pause time to larger pause time because all nodes involved will be more steady, stable and accessible to all active nodes.

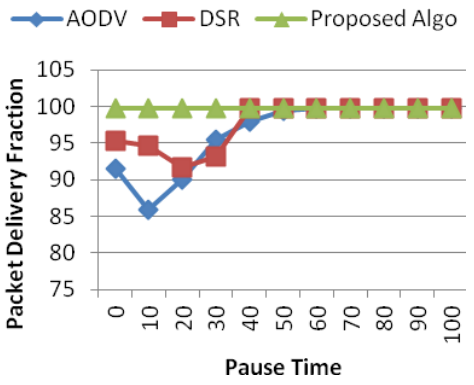

Fig. 9 Packet Delivery Fraction for 25 nodes

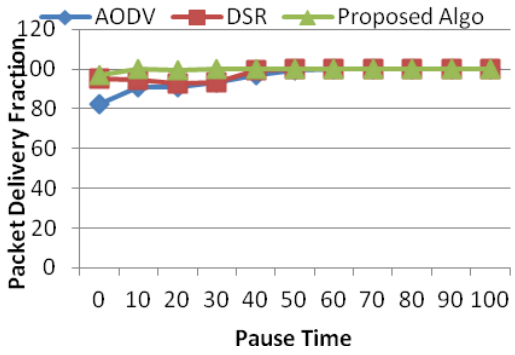

Fig.10 Packet Delivery Fraction for 50 nodes

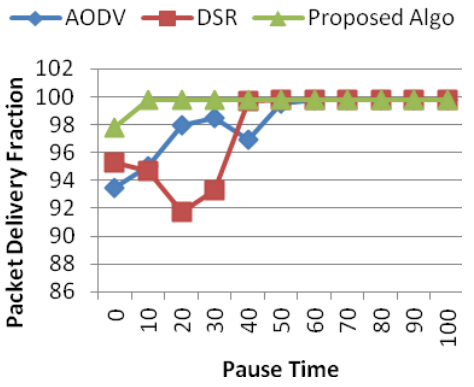

Fig. 11 Packet Delivery Fraction for 75 nodes

5.4 Normalized Routing Load, Normalized MAC Load, Packet Delivery Friction V/s No. of Nodes

From the fig. 13, 14 and 15 it can be noticed that the performance of all the routing protocols is much affected by the number of nodes. This is because all other parameters are affected directly or indirectly by the number of nodes. By increasing the number of nodes in a specified space, the node density will be increased which controls all other parameters. By increasing number of nodes the packet delivery fraction is almost stable but the normalized routing load and normalized MAC load are stable after the node 40 and raises high at end of the simulation. This is mainly because the number of nodes increasing the probability of traffic generation from more number of nodes will be high and so the probability of packet loss will be high with more control packets.

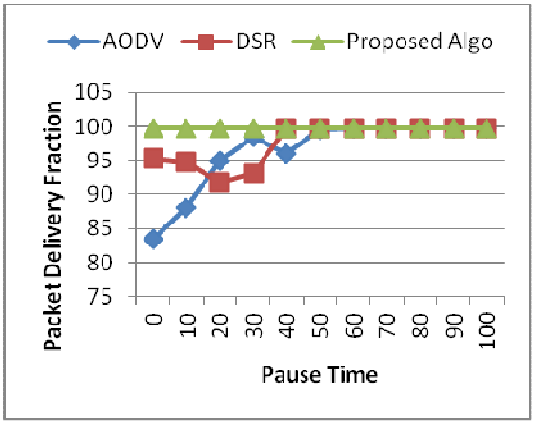

Fig.12 Packet Delivery Fraction for 100 nodes

6. Conclusion

Simulations based on different scenarios, evaluated the protocols in the best possible way. Basic AODV, DSR and proposed Sec-AODV perform evaluation metric of routing protocol for MANET. Proposed Sec-AODV algorithm gave the result of Packet Delivery Fraction metrics which show the maximum no of packet delivered in the network. The packet delivery fractions are most important for best-effort traffic. The normalized routing load will evaluate the efficiency of the routing protocol. Finally, the normalized MAC load is a measure of the effective utilization of the wireless medium or data traffics.

AODV and DSR produce more overhead. Thus, which is included in the data packet as symmetric key is used for security purpose, each time the key overheads are increased with hop by hop count. On adding the concept of session key, reduces the overhead as each time a new session key is generated. Sending packet from next intermediate node the previous generated key is eliminated. AODV and DSR have maximum overhead than Sec-AODV. In conclusion, proposed secure ad hoc routing protocols are a necessity for the secure routing of data. The paper shows the secure routing protocols, the usage of security techniques like digital signatures, authentications and hash chains, cyclic code shift keying have major impacts on the performance. Since it will use more processing power and time. Secure routing protocols available today still need further optimizations to minimize the processing overhead, delays and to maximize the routing throughputs.

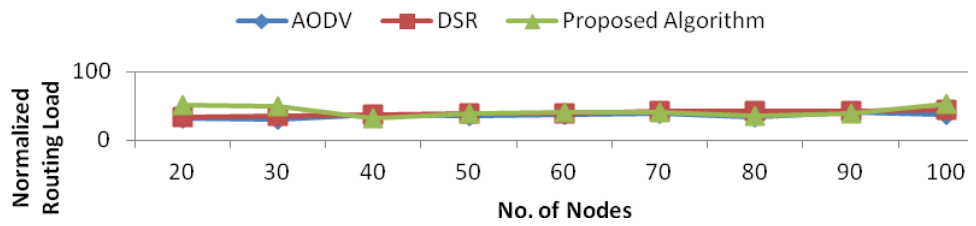

Fig.13 Normalized Routing Load for various nodes

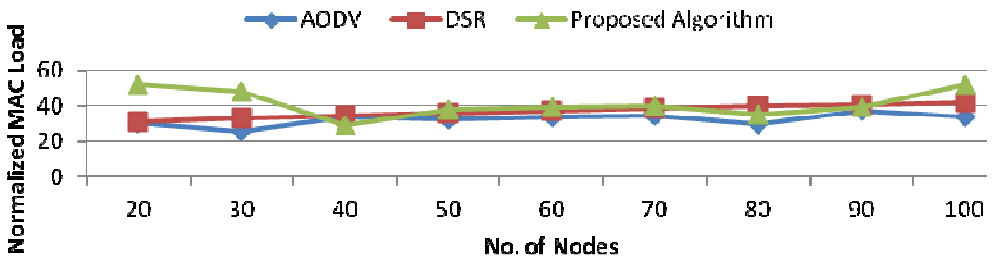

Fig. 14 Normalized MAC Load for various nodes

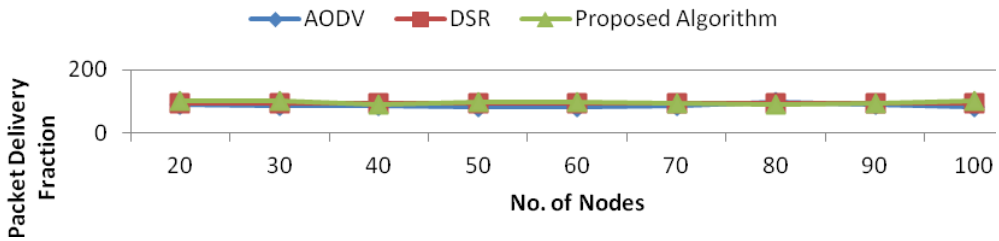

Fig. 15 Packet Delivery Fraction for various nodes

Reference

[1] Charles E. Perkins, "Ad Hoc Networking" Addison-Wesley, 2001.

[2] C. E. Perkins and E. M. Royer, "Ad Hoc On Demand Distance Vector (AODV) Routing", Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

[3] D. B. Johnson and D. A. Maltz, Yih-Chun Hu, "Dynamic Source Routing in Ad-Hoc Wireless Networks", IETF Internet Draft, draft-ietf-manet-dsr-09.txt, April 15, 2003.

[4] R. Perlman. "Fault-tolerant Broadcast of Routing Information". In Computer Networks, n. 7, 1983, pp. 395–405.

[5] L. Zhou and Z. J. Haas. "Securing ad hoc networks". IEEE Network Magazine, 13(6) pp. 24–30, November/December 1999.

[6] B. Dahill, B. N. Levine, E. Royer, and C. Shields. "A secure routing protocol for ad hoc networks". Technical Report UMCS- 2001-037, University of Massachusetts, Department of Computer Science, Aug. 2001.

[7] Manel Guerrero Zapata: "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" INTERNET-DRAFT draft-guerrero-manet-saodv-03.txt. March 2005.

[8] Y. C. Hu, D. Johnson, and A. Perrig. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks". In Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), June 2002, pp. 3–13, June 2002.

[9] Vahid Nazari Talooki and Koorush Ziarati, "Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks" Asia-Pacific Conference on Communications, APCC, 2006, pp. 1 – 5.

[10] Bertocchi, P. Bergamo, G. Mazzini and M. Zorzi, "Performance Comparison of routing protocols for Ad hoc networks", IEEE Global Telecommunications Conference, GLOBECOM, 2003, pp. 1033 – 1037.

[11] Amr M. Hassan, Mohamed I. Youssef and Mohamed M. Zahra, "Evaluation of Ad Hoc Routing Protocols in Real Simulation Environments" ,The 2006 International Conference on Computer Engineering and Systems, 2006, pp. 288 – 293.

[12] Zhijiang Chang, Georgi Gaydadjiev, Stamatis Vassiliadis Routing Protocols for Mobile Ad-hoc

Networks: Current Development and Evaluation, EEMCS, Delft University of Technology Mekelweg

[13] S. F. Lu Henrique M. K. Costa, Marcelo Dias De Amorim, “”Reducing latency and overhead of route repair with controlled Looding”,” in Wireless Networks, vol. 10. IEEE, 2004.

[14] R. Misra and C.R. Mandal, “Performance comparison of AODV/DSR on-demand routing protocols for ad hoc networks in constrained situation” ICPWC International Conference, IEEE, 2005, pp. 86 – 89.

[15] Samir R Das, Charles E Perkins, Elizabeth M Royer, “Performance comparison of two on-demand routing protocols for ad hoc networks” INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings IEEE Vol(1) pp. 3-12.