Volume 2, Issue 8, August 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparative study of security protocols in MANETs

Gaurav Dua
CSE Department
DIET, Karnal
India

Sarvjeet Kajal
CSE Department
DIET, Karnal
India

Rinku Kumar
CSE Department
M.M.University, Mullana
India

Anu Dua
CSE Department
ICL-IET, Ambala
India

Abstract- Ad hoc wireless networking is a new approach to wireless communication with potential applications in very unpredictable and dynamic environments. In contrast to wired and cellular networks, an ad hoc wireless network does not depend on any established infrastructure or centralized administration such as a base station. Therefore, its network topology is dynamic in nature and may change rapidly and unpredictably. The security of ad hoc wireless networks is becoming an increasingly complex issue. A common type of attacks targets at the underlying routing protocols. The objectives of this paper are: To explain various scenarios of attacks at MANET and To study the performance and effectiveness of some secure routing protocols in these simulated malicious scenarios, including ARIADNE and the Secure Ad hoc On-demand Distance Vector routing protocol.

Keywords*— *DSR, AODV, ARIADNE, SAODV

I. Introduction

Mobile adhoc network (MANET) is a temporary network setup for a specific purpose without help of any pre-existing infrastructure. The nodes in MANET are empowered to exchange packet using a radio channel. The nodes not in direct reach of each other uses their intermediate nodes to forward packets. Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Figure 1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them. These characteristics make ad hoc networks well suited for military activities, emergency operations, and disaster recoveries.

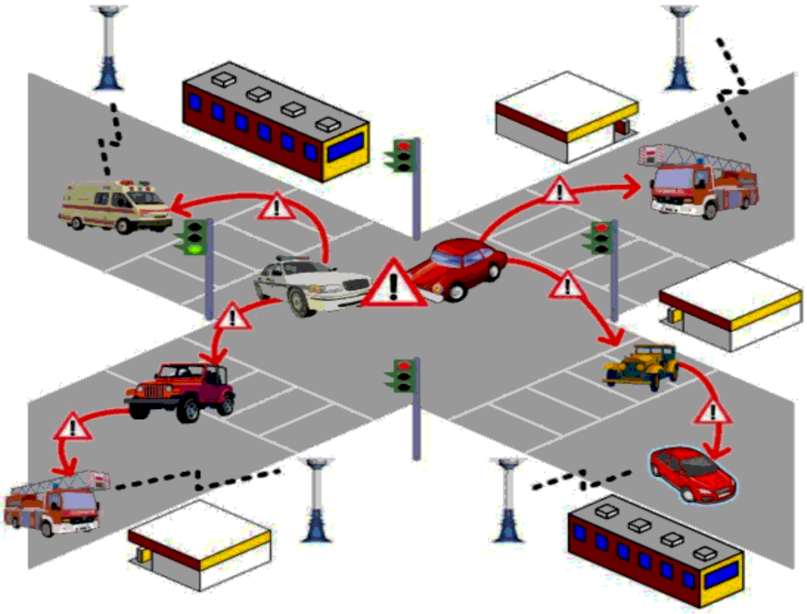

Figure 1: Overview of Mobile Ad-hoc Network [6]

II. ADHOC ROUTING PROTOCOL

A Routing protocols in ad hoc mobile wireless network can generally be divided into three groups as shown below:

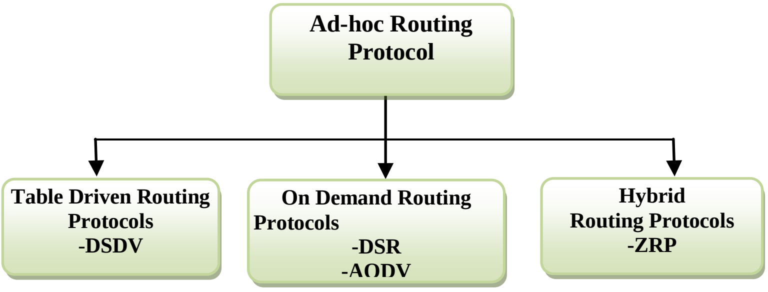

Figure 2: Adhoc Routing Protocols

- **Table driven**: Every node in the network maintains complete routing information about the network by periodically updating the routing table. Thus, when a node needs to send data packets, there is no delay for discovering the route throughout the network. This kind of routing protocols roughly works the same way as that of routing protocols for wired networks.
- **On Demand Driven:** In this type of routing, a node simply maintains routes to active destination that it needs to send data. The routes to active destinations will expire after some time of inactivity, during which the network is not being used.
- **Hybrid:** This type of routing protocols combines features of the above two categories. Nodes belonging to a particular geographical region or within a certain distance from a concerned node are said to be in the routing zone and use table driven routing protocol. Communication between nodes in different zones will rely on the on-demand or source-initiated protocols.

III.DYNAMIC SOURCE ROUTING PROTOCOL

All The Dynamic Source Routing Protocol [5] is one of the on-demand routing protocols, and is based on the concept of *source routing*. In source routing, a sender node has in the packet header the complete list of the path that the packet must travel to the destination node. That is, every node in the path just forwards the packet to its next hop specified in the header without having to check its routing table as in table-driven routing protocols. This saves a lot of network bandwidth. The DSR regularly updates its route cache for the sake of new available easy routes. If some new available routes were found the node will directs the packet to that route [5].The packet has to know about the route direction. So the information about the route was set in the packet to reach its destination from its sender. DSR has two basic mechanisms for its operation i.e. route discovery and route maintenance.

Route Discovery phase

In this phase, the source node searches a route by broadcasting route request (RREQ) packets to its neighbours. Each of the neighbour nodes that has received the RREQ broadcast then checks the packet to determine which of the following conditions apply: (a) was this RREQ received before? (b) Is the TTL (Time to Live) counter greater than zero? (c) Is it itself the destination of the RREQ? (d) Should it broadcast the RREQ to its neighbours? The *request ids* are used to determine if a particular route request has been previously received by the node. Each node maintains a table of RREQs recently received. Each entry in the table is a <*initiator, request id*> pair. If two RREQs with the same <*initiator, request id*> are received by a node, it broadcasts only the one received first and discards the other. This mechanism also prevents formation of routing loops within the network. When the RREQ packet reaches the destination node, the destination node sends a reply packet (RREP) on the reverse path back to the sender. This RREP contains the recorded route to that destination. Figure 3, shows an example of the route discovery phase. Here we have four nodes i.e. A, B, C and D such as node A is the source and node D is destination.

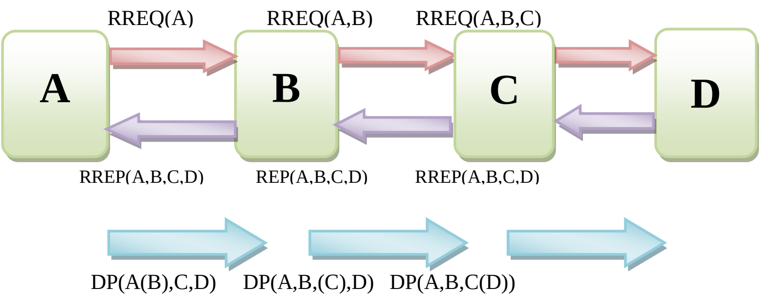

Figure 3: Route Discovery in DSR

Route Maintenance

The route maintenance phase is carried out whenever there is a broken link between two nodes. The route maintenance uses two kind of messages i.e. route error (RERR) and acknowledgement (ACK). The messages successfully received by the destination nodes send an acknowledgement ACK to the sender. Such as the packets transmitted successfully to the next neighbours nodes gets acknowledgement. If there is some problem in the communication network a route error message denoted by RERR is transmitted to the sender, that there is some problem in the transmission. In other words the source didn't get the ACK packet due to some problem. So the source gets the RERR packet in order to re initiate a new route discovery. By receiving the RERR message the nodes remove the route entries.

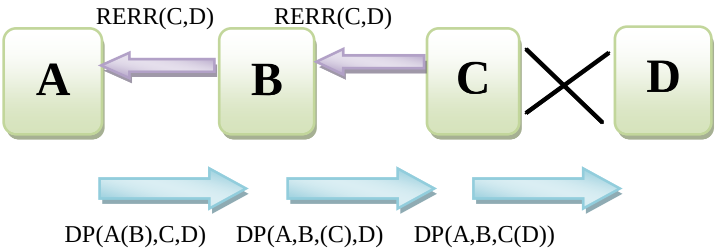

Figure 4: Route Maintenance in DSR

IV. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

To find routes, the AODV routing protocol [11] uses a reactive approach and to identify the most recent path it uses a proactive approach. That is, it uses the route discovery process similar to DSR to find routes and to compute fresh routes it uses destination sequence numbers. The two phases of the AODV [11] routing protocol are described below.

Route Discovery

In this phase, RREQ packets are transmitted by the source node in a way similar to DSR. The components of the RREQ packet include fields such as the source identifier (SId), the destination identifier (DId), the source sequence number (SSeq), the destination sequence number (DSeq), the broadcast identifier (BId), and TTL. When a RREQ packet is received by an intermediate node, it could either forward the RREQ packet or prepare a Route Reply (RREP) packet if there is an available valid route to the destination in its cache. To verify if a particular RREQ has already been received to avoid duplicates, the (SId, BId) pair is used. While transmitting a RREQ packet, every intermediate node enters the previous node's address and its BId. A timer associated with every entry is also maintained by the node in an attempt to delete a RREQ packet in case the reply has not been received before it expires. Figure 5 depicts an example of route discovery mechanism in AODV.

In Figure 5 node C gets a route to G in its cache and its DSeq is greater when compared with that in the RREQ packet. Consequently, it sends a RREP back to the source node A. By doing this, node A has already stored the path A-C-F-G. A RREP is also sent back by the destination node to the source. One possible route is A-B-E-G. The intermediate nodes on the path from source to destination make an update on their routing tables with the latest DSeq in the RREP packet.

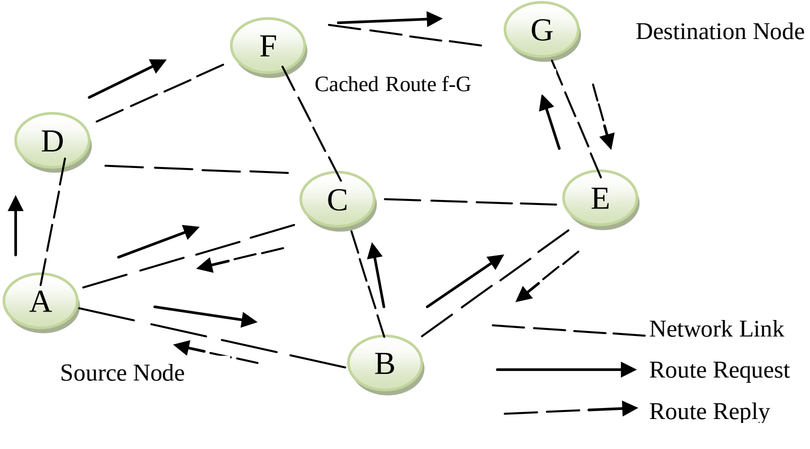

Figure 5: Route discovery in AODV [11]

In Figure 5 node C gets a route to G in its cache and its DSeq is greater when compared with that in the RREQ packet. Consequently, it sends a RREP back to the source node A. By doing this, node A has already stored the path A-C-F-G. A

RREP is also sent back by the destination node to the source. One possible route is A-B-E-G. The intermediate nodes on the path from source to destination make an update on their routing tables with the latest DSeq in the RREP packet.

Route Maintenance

Whenever a node finds out a link break (via link layer acknowledgements or HELLO messages [9], it broadcasts an RERR packet (in a way similar to DSR) to notify the source and the end nodes. This process is illustrated in Figure 6. If the link between nodes C and F breaks on the path A-C-F-G, RERR packets will be sent by both F and C to notify the source and the destination nodes.

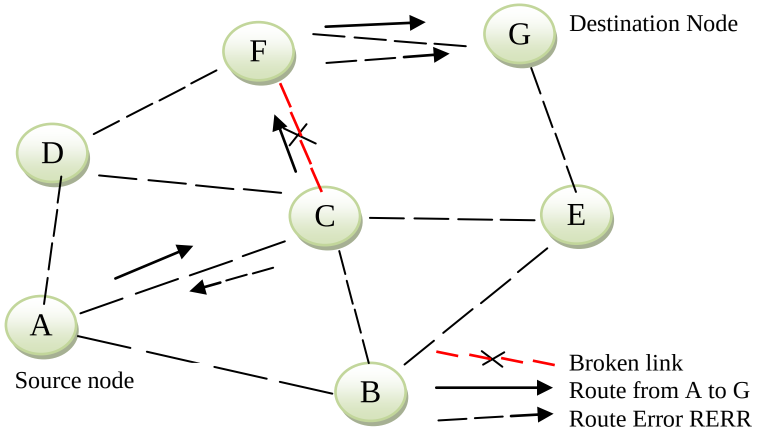

Figure 6: Route Maintenance in AODV

V. ATTACKS ON EXISTING PROTOCOLS

Routing is one of the most vital mechanisms in the ad hoc networks. Improper and insecure routing mechanisms will degrade the performance of the ad hoc networks. Figure 7, depicts a broader classification of the possible attacks in MANETs [7].

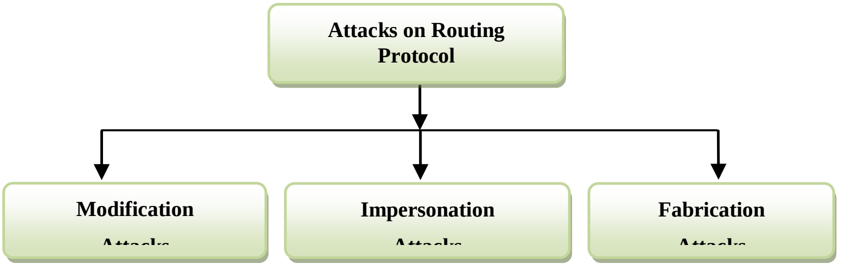

Figure 7: Attacks on MANET routing protocols [7]

❖ Modification Attacks

In modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. In this type of attacks, some of the protocol fields of the messages passed among the nodes are modified, thereby resulting in traffic subversion, redirection or Denial of Service (DoS) attacks. Some of these attacks are:

Modification of route sequence numbers: This attack is possible against the AODV protocol. The malicious node can change the sequence number in the route request packets or route reply packets in order to make the route fresh. In Figure 8, malicious node M receives a route request RREQ from node B that originates from node S and is destined for node X. M unicasts a RREP to B with a higher destination sequence number for X than the value last advertised by X. The node S accepts the RREP and then sends the data to X through M.

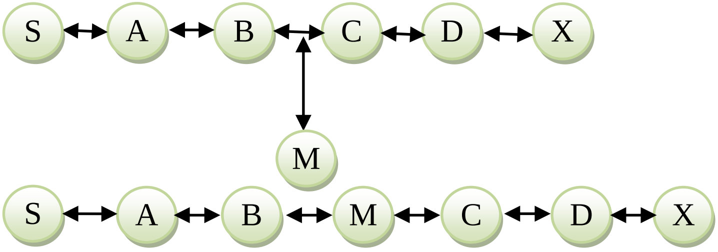

Figure 8: Route modification attack [7]

Modification of source route: This attack is possible against DSR which uses source routes and works as follows. In Figure 8, it is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the list and forwards it to C. C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.

❖ **Impersonation Attacks**

The impersonation attacks, also called the spoofing attacks, are attacks where malicious node assumes the identity of another node in the networks. By impersonating another node, attackers are able to receive routing messages that are directed to the nodes they faked. Impersonation attacks are possible in the ad hoc networks because most of the current ad hoc routing protocols do not authenticate the routing packets.

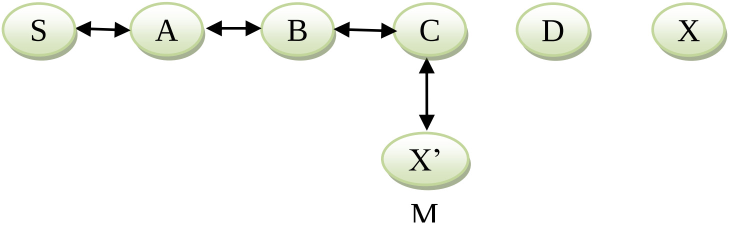

Figure 9: Impersonation attack [7]

❖ **Fabrication Attacks**

In this type of attacks, a malicious node tries to inject fake messages or routing packets to disrupt the routing mechanism. These attacks are difficult to detect in a MANET since the routing packets appear to be legitimate (Logically acceptable) packets to the nodes processing them. Figure 10, is an example of fabrication attacks. Node S wants to send data to node X, so it broadcasts a route request in order to find the route to node X. Malicious node M pretends to have a cached route to the destination X, and returns route reply to the source node (S). The source node, without checking the validity of the RREP, accepts the RREP and starts to send data through M.

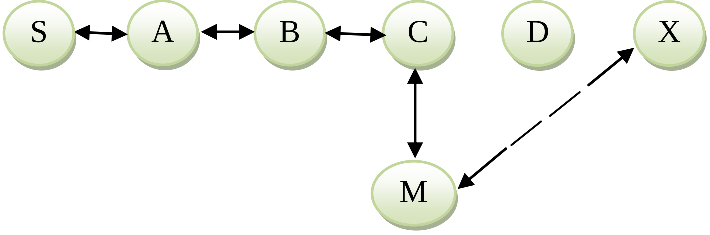

Figure 10: Fabrication attack [7]

VI. EXPERIMENTAL RESULTS

The performance data of four routing protocols (DSR, ARIADNE, AODV and SAODV) are collected. A scenario is set up for data collection. This scenario is run 11 times with 11 different values of the mobility pause time ranging from 0 to 100 seconds. The data is collected according to two metrics:

-Packet Delivery Fraction

-Normalized Routing Load

In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs. The average values of these 11 simulation runs are then calculated for the two metrics and used as a baseline to evaluate the performance of routing protocols in malicious environments. As shown in Figure 11 the percentage of packets delivered in AODV and SAODV is fairly close to each other, and both methods exhibit superior performance (~90% in general) [11]. The security features in SAODV lower the performance a little bit. Actually, the generation and verification of digital signatures depends on the power of the mobile nodes and causes a delay in routing packet processing. In the simulation environments, this delay depends on the simulation running machine and is not high enough to make the significant difference for the PDF metric. On the other hand, the packet delivery fraction in DSR and ARIADNE are 20-40% lower than that of AODV/SAODV across the board given different mobility pause times [10].

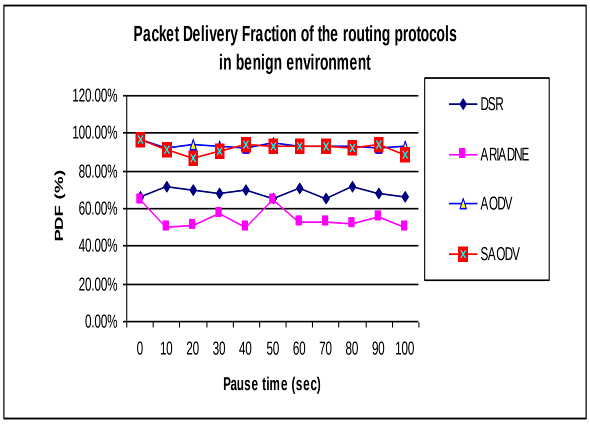

Figure 11: Packet Delivery Fraction vs. pause time values in benign environment

The major difference between AODV and DSR is caused by difference in their respective routing algorithms. It was reported by other researchers that, in high mobility and/or stressful data transmission scenarios, AODV outperforms DSR. The reason is that DSR heavily depends on the cached routes and lack any mechanism to expire stale routes. In the benign environment of our experiments, the default expiry timer of cached route for DSR and ARIADNE is 300 seconds [2], while this number is 3 seconds for AODV and SAODV [3]. In respect to the protocol design, these values are kept unchanged through all the simulation scenarios. Furthermore, DSR and ARIADNE store the complete path to the destination. Hence, if any node moves out of the communication range, the whole route becomes invalid. In MANETs, the nodes are mobile, so route change frequently occurs. Without being aware of most recent route changes, DSR may continue to send data packets along stale routes, leading to the increasing number of data packets being dropped. The situation is even worse for ARIADNE, mainly because ARIADNE relies on the delayed key disclosure mechanism of TESLA when authenticating packets, including the RERR packets. When an intermediate node in ARIADNE notices a broken link, it sends a RERR message to the source node of the data packet. The source node, however, simply saves the RERR message, because it has not yet received from the intermediate node the key needed to authenticate the route error. The source node keeps sending the data until the second route error is triggered, and another RERR is received. Only then would the previous route error be authenticated, and the broken link not be used any more. This explains the worse performance of ARIADNE in comparison with DSR and other protocols.

As shown in Figure 12, the NRL metric is, in general, inversely proportional to the PDF metric. A low PDF value corresponds to a high NRL value.

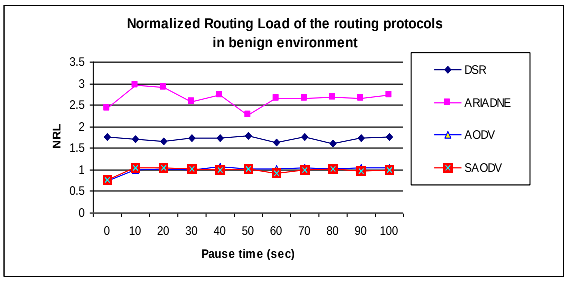

Figure 12: Normalized Routing Load vs. pause time values in benign environment

This relationship between PDF and NRL is further illustrated in Table 1, which lists the average values of the two metrics over 11 simulation runs for each of the four protocols.

Table 1: "Baseline" metrics of the four protocols

Pause Time (seconds)	**Packet Delivery Fraction (%)**	**Normalized Routing Load**
DSR	68.41%	1.72
ARIADNE	54.70%	2.58
AODV	93.45%	1.01
SAODV	92.00%	0.98

VII. CONCLUSION

In this paper, we have implemented two secure routing protocols, ARIADNE and SAODV, based on their respective underlying protocols, DSR and AODV, in the OPNET simulation environment. I have also simulated four popular network attack models that exploit the weakness of the protocols. The attack models are used to make malicious wireless nodes and create various malicious environments, in which the performance of DSR, AODV, ARIADNE, and SAODV are evaluated. AODV and SAODV without pubic key verification are vulnerable to impersonation attacks. The impacts on the two protocols are similar. The more the number of malicious nodes in the network is, the fewer the number of received data packets is. As shown by the experiments, SAODV is secure against impersonation attack only when there is a way to verify the public key of the route reply originator. In other words, a key management centre is really necessary to make SAODV secure against impersonation attacks. This is still an outstanding issue of SAODV. The ultimate goal of a routing protocol is to efficiently deliver the network data to the destinations; therefore, two metrics, Packet Delivery Fraction (PDF) used to evaluate the protocols.

REFERENCES

[1] Frank Kargl, Alfred Geiß, Stefan Schlott, and Michael Weber.“Secure Dynamic Source Routing”. Proceedings of the 38th Hawaii International Conference on System Sciences.2005

[2] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, and Joo-Han Song. “Experimental Comparisons between SAODV and AODV Routing Protocols”.2005

[3] Yi-an Huang and Wenke Lee. “Attack analysis and Detection for Ad-hoc Routing protocols”.September 2004

[4] Y. Hu, A. Perrig, D. Johnson. “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”. March 2003.

[5] D B. Johnson, D A. Maltz, and Y. Hu. “The dynamic source routing protocol for mobile ad hoc network,", Internet-Draft, April 2003.

[6] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer.“A Secure Routing Protocol for Ad Hoc Networks”.Proceedings of 10th IEEE International Conference on Network Protocols (ICNP’02), Paris, France.November 2002,

[7] G. Montenegro and C. Castelluccia. “Statistically unique and cryptographically verifiable identifiers and addresses”. Network and Distributed System Security Symposium Feb 2002.

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks"2002

[9] M. Marina and S. Das. “Performance or Route caching strategies in Dynamic Source Routing”. 2001

[10] Samir R. Das, Charles E. Perkins, Elizabeth M.Royer. “Performance Comparison of Two On-demand Routing Protocols forAdHoc Networks” Proceedings IEEE Infocom page 3-12, March 2000.

[11] C.E. Perkins, E. Royer, and S.R. Das. “Ad hoc on demand distance vector (AODV) routing",2000

[12] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. “Efficient and Secure Source Authentication for Multicast”.2000