IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
ISSN: 2278-2834, ISBN: 2278-8735. Volume 3, Issue 2 (Sep-Oct. 2012), PP 20-26
www.iosrjournals.org

Efficient Security for Mobile Ad-Hoc Network

Mr. S. J. Patil[1], Prof. (Mr.) U. A. Patil[2], Ms. A. A. Patil[3]
[1,2](E&TC Department, D.K.T.E's TEI, Ichalkaranji / Shivaji University, India)
[3](IT Department, Dr. JJMCOE, Jaysingpur / Shivaji University, India)

Abstract : *An Ad-hoc network is a dynamically changing network of mobile nodes that communicate without the support of a fixed network. Due to lack of centralized control, secured communication in mobile Ad-hoc network is important matter due to dynamic nature of the network topology. MANETs is affected by new security problems in addition to the problems of regular networks. In this paper, we introduce an efficient security AODV algorithm to enhance the data security in the network. To generate the private key ECDSA algorithm is used. Simulation result shows that our protocol gives better performance than the previous one.*
Keywords – *AODV, ECDSA algorithm, MANET.*

I. INTRODUCTION

1.1 Mobile Ad-Hoc Network (MANET)

The increasingly use of wireless networks in the last years, have pushed a lot of people to study and try to improve the performance of mobile ad hoc network(MANET). A MANET is a collection of mobile nodes (MN) that communicate using wireless links without support from any pre-existing infrastructure network. Packets are delivered from a source to a destination using packet forwarding capabilities of intermediate nodes. Therefore, MNs act as both end systems and routers [12]. An Ad hoc network is a dynamically changing network of mobile nodes that communicate without the support of a fixed structure. There is a direct communication among neighboring devices but communication between non- neighboring devices requires a routing protocol.

Routing protocols are divided into two categories based on how and when routes are discovered, but both find the shortest path to the destination. Proactive routing protocols are table-driven protocols; they always maintain current up-to-date routing information by sending control messages periodically between the hosts which update their routing tables. When there are changes in the structure then the updates are propagated throughout the network. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbors. Other routing protocols are on-demand routing protocols, in other words reactive, ones which create routes when they are needed by the source host and these routes are maintained while they are needed. Such protocols use distance-vector routing algorithms, They have vectors containing information about the cost and the path to the destination. When nodes exchange vectors of information, each host modifies its own routing information when needed [13]

1.2 Security issues in MANET.

The current mobile ad-hoc networks allow for many different types of attacks. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

There are various types of attacks on ad hoc network which are describing following:

Interruption: An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.

Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer. Examples include wiretapping to capture data in a network and the illicit copying of files or programs.

Modification: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.

Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

Location Disclosure: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [14], or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

Black Hole: In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination [15]. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

Replay: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Wormhole: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [16]. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes.

Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [18]. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated.

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [17]. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

In this paper, we propose an efficient security algorithm called ES-AODV in ad hoc wireless networks. The overall goal of this algorithm is to provide a secure solution for communication in ad hoc network applications strong enough to withstand an active internal threat within the network. This protocol will be able to find a trusted end-to-end route free of any malicious entity, effectively isolating any node trying to inject malicious information into the network.

II. RELATED WORK

Unlike the conventional network, a MANET is characterized by having a dynamic network topology due to mobility of nodes as proposed by Song Ci et al.[2]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network. Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work proposed by C. Perkins, E. Belding-Royer, and S. Das et al. in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power. The routing protocols proposed by them are classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [3], nodes find routes only when required. In proactive routing protocols, where as the Optimized Link State Routing (OLSR) protocol nodes obtain routes by periodic exchange of topology information [4]. Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved. However, as suggested by A. Shevtekar, K. Anantharam, and N. Ansari et al. for a hostile environment, a malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks to deny services to legitimate nodes [5]. Recently, several research efforts were launched to counter against these malicious attacks. Most of the previous work focused mainly on providing preventive schemes to protect the routing protocol in a MANET. Most of these schemes are based on key management or encryption techniques to prevent unauthorized nodes from joining the network. In general, the main drawback of these approaches is that they introduce a heavy

traffic load to exchange and verify keys, which is very expensive in terms of the bandwidth-constraint for MANET nodes with limited battery and limited computational capabilities. Y-C Hu and A. Perrig, et al. discuss these preventive schemes (e.g., authenticated routing for ad hoc net-works (ARAN) [6],[7], Ariadne [8], secure AODV (SAODV) [9]) in detail. B. Wu et al. done a survey on attacks and their countermeasures has been reported by them in mobile ad hoc network for five layers: application, transport, network, data link, and physical. For attacks against the network layer, the authors survey countermeasures for impersonation attacks, modification attacks, wormhole attacks, and black hole attacks [10]. However, new attacks and countermeasures against a network layer attack, such as link spoofing and withholding of routing traffic have not been discussed in the literature.

III. OBJECTIVE & OVERVIEW OF PROPOSED WORK

3.1 Objective

To find the misbehavior of the any node called as malicious node from the path in between source and destination node. And excluding that path take another path which is free from malicious node to the destination.

3.2 Overview of the protocol

Our proposed security routing protocol is based on the network layer and the protocol that we propose here is an extension of the Ad hoc On Demand Distance Vector (AODV) routing protocol which we call efficient security AODV. And we assume that all the nodes are identical in their physical characteristics and all communicate via a shared wireless channel. Essentially all routing protocols in the ad hoc community tend to find the shortest path to the destination irrespective of the presence of any malicious node in that path. Our model against that, we think that a path free of malicious node is more important than the shortest path.

Designing ES-AODV comes from finding a trusted end- to-end path free of malicious nodes. The basic idea behind the protocol is for a node to append the trust level of its previous node from which has received the route request packet. Trust levels are defined to be unique values of the level of trustworthiness of a node on another node. A path with maximum trust level will eventually be selected by the destination node and will be sent to the source as the end-to- end active path to be used. A node with malicious intention will try to put itself into that active route by trying to inject malicious trust information.

The protocol will ensure that all the trust level information provided by a node will be checked by its previous node in order to ensure information authenticity. This is ensured by computing a signature with the Private Key of the node by using ECDSA algorithm, along with the trust level computation.

When a node wants to find a route to another node, it sends the RREQ packet. The route request packet header contains a ES previous node whose trust level is being appended, in addition to the other fields in AODV route request. The header also contains a cumulative ES field which reflects the sum of the accumulated trust level of all the nodes in the path. When an intermediate node receives the route request packet, it rebroadcasts it after modifying the ES previous node field to include the trust level of the node that sends it the route request and also increases the cumulative ES field by the trust level of its previous node. Every node checks back the rebroadcasted route request packet from its next node to see whether it has provided the proper information. If not, it immediately broadcasts a warning message questioning the intended malicious action of that node.

The route reply packet has the next hop information. When the source node gets back the first route reply, it waits for a specified amount of time before using that route. If within that time another route reply comes, the source node queries the next hops of the two route replies. The next hop of the malicious route reply will obviously not have the same route to the destination.

3.3 Block diagram

The block diagram of secured system for MANET is shown below.

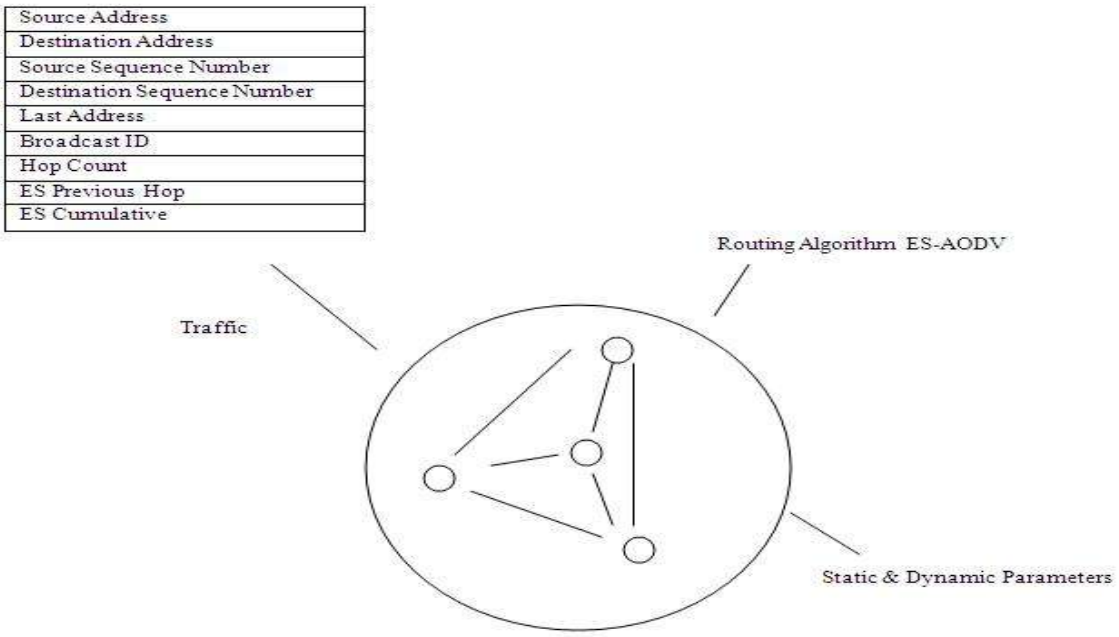

Figure 1 Secured system for MANET

Fig. 1 shows only four nodes like that one can use N number of nodes. The protocol that we implemented here is efficient security AODV. All the nodes are identical in their physical characteristics and all communicate via a shared wireless channel. The fields in route request packet is shown in fig. 1 which is Source address, Destination address etc.

IV. PERFORMANCE EVALUATION

4.1 Simulation model & parameters

Our simulations are implemented in Network Simulator (NS-2) from Lawrence Berkeley National Laboratory (LBNL) with extensions for wireless links form the Monarch project at Carnegie Mellon University. The simulation parameters are summarized as follows:

TABLE 1

Network Simulator	NS-2
Network area	1000 X 1000
Number of nodes	50, 75, 100, 125.
Speed of the nodes	10 m/s.
Traffic load	CBR
MAC protocol	IEEE802.11b
Simulation time	200s. and repeated for various number of nodes.

4.2. Performance metrics

4.2.1 Packet delivery ratio

The fraction of the data packets delivered to the destination nodes to those sent by the source nodes.

4.2.2 Throughput

It is the average rate of successful message delivery over a communication channel.

4.2.3 Normalized routing load

The number of routing packets transmitted per data packet delivered at the destination. Each hop - wise transmission of a routing packet is counted as one transmission. The routing load metric evaluates the efficiency of the routing protocol.

4.2.4 Average End-to-End Delay

Average end to end delay includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets.

4.3 Results

When we designed the security routing protocol, we found that it had a very small increase in packet delivery ratio as compared with AODV as shown in Fig. 2

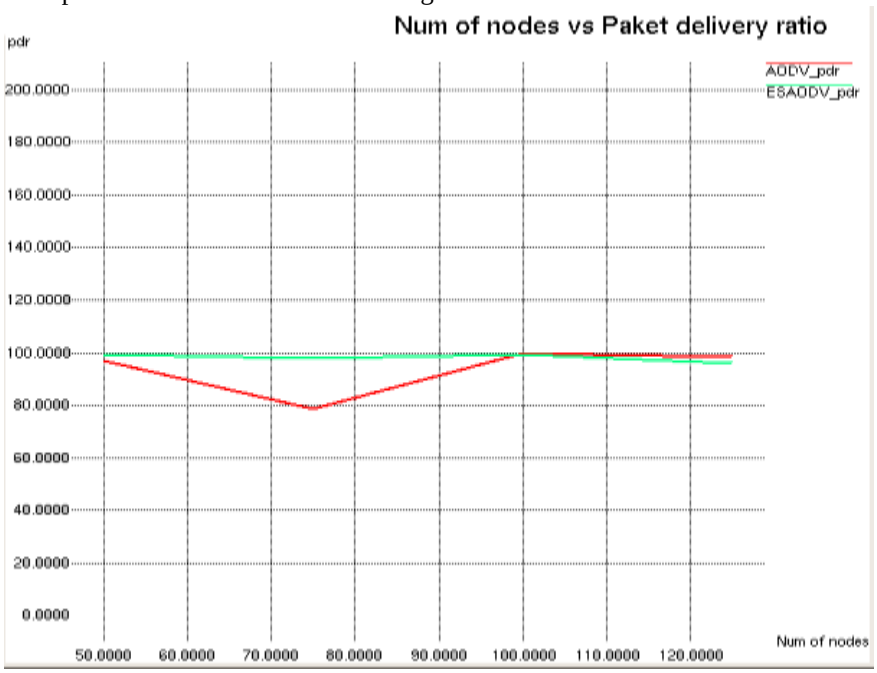

Figure 2 Comparison of packet delivery ratio.

Fig. 3 compares throughput for ES-AODV and AODV. We can see from the figure that ES-AODV has higher throughput than AODV for less number of nodes. In ES-AODV, lesser number of routes reply messages are generated which will result in lower MAC layer load. Hence throughput for ES-AODV increases at a less number of nodes than that of AODV, resulting in higher throughput than AODV with less number of nodes.

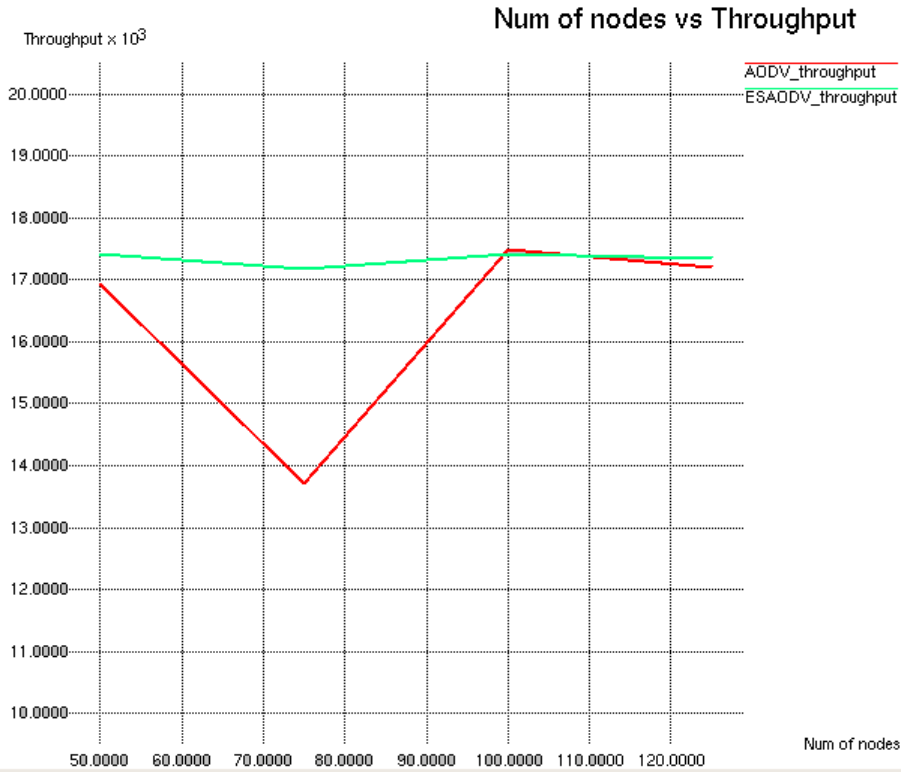

Figure 3 Comparison of Throughput

Fig. 4 compares the normalized routing load and from this we can say that normalized routing load is greater than the AODV, and it increases with increase in the number of nodes.

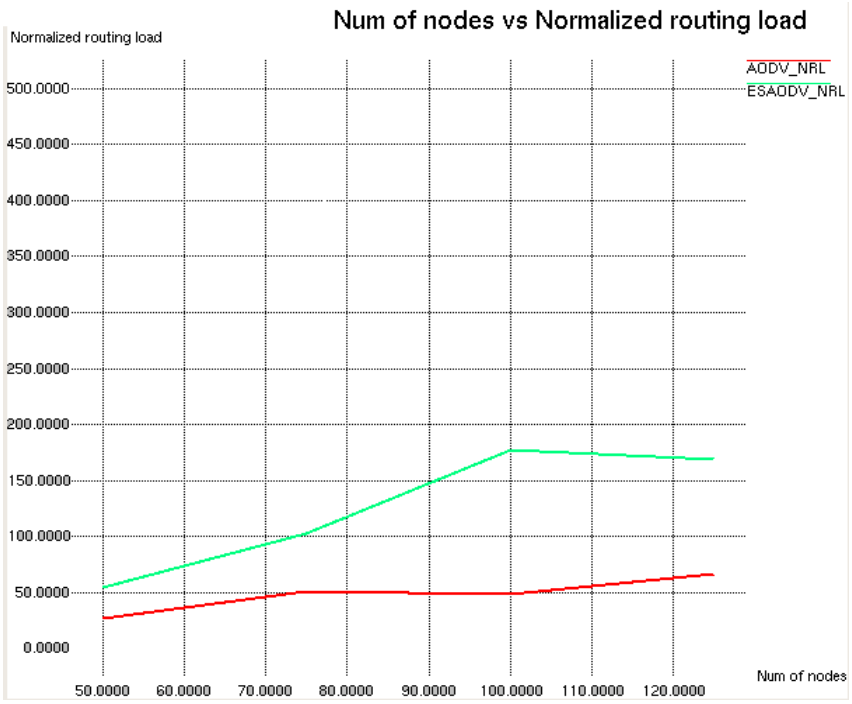

Figure 4 Comparison of Normalized routing load.

Fig. 5 compares the average end-to-end delay for ES-AODV and AODV. There is a random variation in delay, as quite naturally expected because of the Ad-hoc nature of the network. However, the delay for ES-AODV can be found to be in close to that of the original AODV, which also gives the efficiency of our trusted routing protocol.

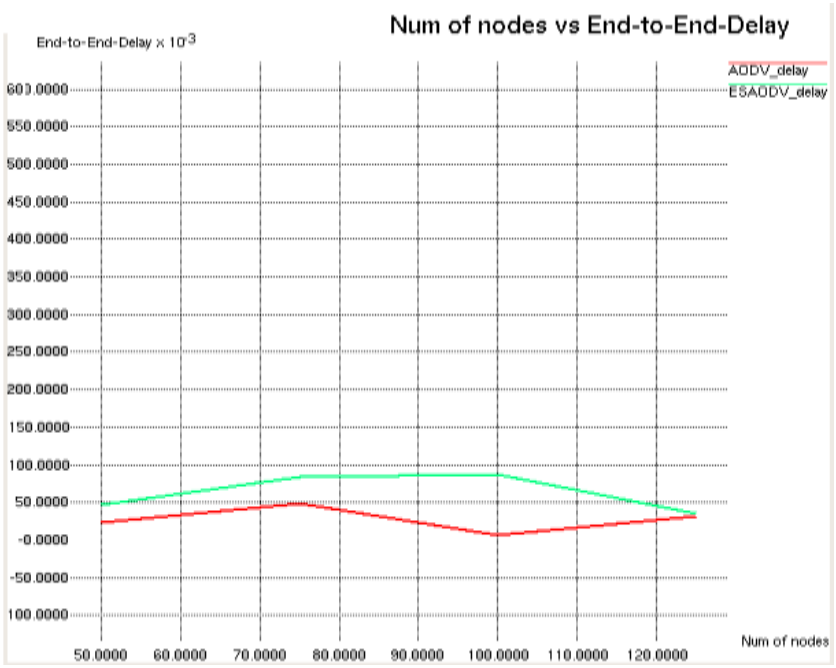

Figure 5 Comparison of End-to End Delay.

The security of our project depends on the verification of information provided by other nodes. We evaluate two types of attack which are black hole and modification attack, in black hole attack the malicious node dropped all packets which are received from the previous node. And in the modification attack the node changed the destination address in the RREQ packet. Our protocol is able to find such type of attack and take corrective action on it.

A malicious node wants to include itself into the path and provides wrong information in the RREQ packet. The malicious node is effectively isolated by the collaborative effort of its neighbors. Furthermore, A node falsely accuses another node and alters the information provided by the previous. The accuser has to append the signature computed by the accused node. In order to alter the information, it has to decrypt the signature, change the original information and recompute it. But it fails to recompute the signature as it lacks the knowledge of the accused node's Private Key. Thus any attempt to alter the original information gets detected. In addition, a node whose trust level has changed, falsely accuses another node by using a copy of the old signature field that the later used at some earlier point of time. This false accusation gets detected as the decryption of the signature will disclose the actual source address. We recognize that the protocol is secure under these threats.

V. CONCLUSION

We implemented an efficient security algorithm ES-AODV to enhance the security in Ad-hoc wireless networks. According to the analysis of the results obtained from simulation, we can conclude that the secure routing protocol gives good results for various numbers of nodes. It has been observed that the routing protocol performs even better than the original AODV routing protocol.

REFERENCES

[1] Z.M.Alfawaer, Saleem Al_zoubi. "A proposed security subsystem for Ad Hoc wireless networks" *In International forum on Computer Science-Technology And Application*. IEEE 2009.

[2] Song. Ci et al, "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks" *IEEE Trans. Vehic. Tech., vol. 55, no. 4, pp. 1302–10,* July 2006.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," *IETF RFC 3561,* July 2003.

[4] Th. Clausen et al., "Optimized Link State Routing Protocol," *IETF Internet draft, draft-ietf-manet-olsr-11.txt,* July 2003.

[5] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," *IEEE Commun. Lett., vol. 9, no. 4, pp. 363–65,* Apr. 2005.

[6] Y-C Hu and A. Perrig, "A Survey of Secure Wireless Ad-Hoc Routing," *IEEE Sec. and Privacy*, May–June 2004.

[7] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," *Proc. 2002 IEEE Int'l. Conf. Network Protocols*, Nov. 2002.

[8] Y-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proc. MobiCom '02*, Atlanta, GA, Sept. 23–28, 2002.

[9] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," *Proc. 2002 ACM Wksp. Wireless Sec. pp. 1–10,* Sept. 2002.

[10] B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless/Mobile Network Security, Springer, vol. 17,* 2006.

[11] C. Perkins and E. Royer, "Ad hoc On-Demand Distance Vector Routing", *In Proc. IEEE Workshop on Mobile Computing Systems and Applications,* 1999.

[12] Jonas Karlsson, Alba Batlle, Andreas J. Kassler and Bu-Sung Lee "TCP Performance in Mobile Ad Ho c Networks Connected to the Internet"

[13] Aleksandr Huhtonen, "Comparing AODV and OLSR Routing Protocols", *HUT T-110.551 Seminar on Internetworking*, April 2004.

[14] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[15] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" *ACMSE'04*, April 2-3, 2004, Huntsville, AL, USA.

[16] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" *In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, April 2003.

[17] I. Aad, J.P.Hubaux and E-W.Knightly, "Denial of Service Resilience in Ad Hoc Networks," *Proc. MobiCom*, 2004.

[18] Patroklos g. Argyroudis and donal o'mahony, "Secure Routing for Mobile Ad hoc Networks", *IEEE Communications Surveys & Tutorials Third Quarter* 2005.