Scenario Based Performance Evaluation of Secure Routing in MANETs

Karthik Sadasivam Vishal Changrani T. Andrew Yang

University of Houston-Clear Lake, Houston, TX, USA

ABSTRACT

Security in MANETs is critical when deployed in real-world scenarios, such as battlefield, and event coverage, etc. Traditional MANET routing protocols fail to prevent attacks such as DoS, spoofing, and cache poisoning. One of the primary goals of designing secure routing protocols is to prevent a compromised node from disrupting the route discovery and maintenance mechanisms. However, this added security comes at the cost of performance. In this paper we evaluate the performance of SEAD, a secure routing protocol based upon DSDV, using scenario-based experiments. We compare its performance with DSDV and the reactive protocol DSR, and analyze the tradeoffs between performance and security. The scenarios used depict critical real-world applications such as battlefield and rescue operations, which tend to have contradicting needs. Our performance evaluation gives an insight into the applicability of the three protocols under consideration and helps identify which protocol is more suitable for a given scenario.

KEYWORDS

Ad-hoc networks, secure routing, evaluation, simulation, performance, SEAD

1. Introduction

Secure routing in MANETs has been studied extensively in literature [1] [2] [3] [4] [5]. Designing secure routing protocols for ad hoc networks is challenging for several reasons. On one hand, the protocol must protect against multiple coordinated attacks. Since ad hoc networks are typically deployed in an open environment where all nodes participate in the routing mechanism, designers are faced with issues such as preventing both *active* and *passive* attacks [2]. On the other hand, since the nodes are typically deployed in hostile or inhospitable terrains where power requirements are stringent, the routing protocol must be power-aware. This implies that the cryptographic primitives used for implementing the security measures must be effective. To achieve optimal operations, the tradeoffs between security and performance need to be analyzed.

Past studies [2] [6] have identified the threats which a secure routing protocol must address. First, there exist *external attackers* who try to disrupt the routing by injecting fake packets or false route information. Then, *compromised nodes* might advertise incorrect routing information. Hu etc. [5] provide a model for classification of several types of attacks possible in a MANET. Several secure routing protocols have been proposed, such as SRP [2], SEAD [1], ARIADNE [5] and ARAN [4], each of which protects against some of these attacks, though a ubiquitous solution has not yet been achieved.

Our work was partially motivated by the fact that, though the performance of secure routing protocols for MANETs have been analyzed, they have assumed the Random Waypoint mobility (RWM) model, which fails to converge at higher pause times [7]. Further, the RWM model is not sufficient to capture some realistic scenarios. In order to model the movements of nodes in a realistic terrain, such as a battlefield or rescue operation, we need more sophisticated mobility models. The focus of this paper is on the design of scenario-based experiments, and analysis of the performance of SEAD, a secure table-driven routing protocol based upon DSDV. We compare its performance with DSDV and DSR, a reactive routing protocol. We analyze the tradeoffs between performance and security for specific scenarios. In Section 2, we present a brief background of previous work and describe the working of SEAD. We explain our experimental setup, the scenarios used and the metrics in Section 3. In Section 4 we analyze the results obtained and in Section 5 we conclude the paper with pointers to future work.

2. Background

The routing protocols for MANETs can be broadly classified as on-demand/reactive and periodic/proactive protocols. Reactive routing protocols propagate route updates only when a route to destination is required. There are several reactive routing protocols available for ad hoc networks, including DSR [9], AODV [10], etc. On the other hand, proactive routing protocols such as DSDV [11] maintain an active route to every neighbor. Reactive routing protocols have been demonstrated to perform better with significantly lower overheads than proactive routing protocols in many scenarios [8] since they are able to react quickly to topology changes, yet being able to reduce routing overhead in periods or areas of the network in which changes are less frequent. In this section we discuss briefly the working of three routing protocols – DSDV, SEAD and DSR. Their respective performances are compared in a later section.

2.1 DSDV

The *Destination Sequenced Distance Vector protocol (DSDV)* is a proactive routing protocol based upon the classical Bellman Ford algorithm. In this routing protocol, each mobile host maintains a table consisting of the next-hop neighbor and the distance to the destination in terms of number of hops. It uses *destination sequence numbers* to determine "freshness" of a particular route in order to avoid any short- or long-lived routing loops. If two routes have the same sequence number, the one with smaller distance metric is advertised. All the hosts periodically broadcast their tables to their neighboring nodes. The sequence number is incremented upon every update sent by the host.

2.2 SEAD

The *Secure and Efficient Ad hoc Distance vector routing protocol* (SEAD) is based upon the *DSDV-SQ* routing protocol, a modified version of *DSDV*. It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and sequence number in the routing table. For authenticating a particular sequence number and metric, the node generates a random initial value $x \in \{0,1\}^{\rho}$ where ρ is the length in bits of the output of the hash function, and computes the list of values $h_0, h_1, h_2, h_3, \ldots, h_n$, where $h_0 = x$, and $h_i = H(h_i - 1)$ for $0 < i \leq n$, for some n. As an example, given an authenticated hi value, a node can authenticate h_{i-3} by computing $H(H(H(h_i - 3)))$ and verifying that the resulting value equals h_i.

Each node uses one authentic element of the hash chain in each routing update it sends about itself. This enables the authentication for the lower bound of the metric in other routing updates for that node. The receiving node authenticates the route update by applying the hash function according to the prior authentic hash value obtained, and compares it with the hash value in the routing update message. The update message is authentic if both values match. The source must be authenticated using some kind of broadcast authentication mechanism such as TESLA [12]. Apart from the hash functions used, SEAD does not use average settling time for sending triggered updates as in DSDV in order to prevent eavesdropping from neighboring nodes. SEAD prevents several types of DOS attacks. It also prevents formation of routing loops. However, it does not prevent the *wormhole attack* [6], which results in tunneling of packets via a virtual cut in the network.

2.3 DSR

The *Dynamic Source Routing protocol* (DSR) is a reactive protocol which uses source routing, i.e., each routing packet has a complete list of nodes through which the packet must pass. Since every packet has the complete route, the intermediate nodes need not maintain up-to-date routing information. The protocol itself consists of two phases – route discovery and route maintenance. In the *route discovery* phase, a node S wanting to send a packet to another node D broadcasts a route request packet (RREQ) to neighboring nodes. D unicasts a reply packet (RREP) back to S. During the *route maintenance* phase, a node S detects whether its link to a destination node D is no longer valid. If there is a broken link, S is notified via a Route Error packet (RERR).

3. Experimental Setup

For our scenario-based experiments, we used NS-2 [13]. For generating the scenarios, we used the mobility scenario generation tool, *BonnMotion*. We utilized CMU's wireless extensions to NS-2, which is based on a two-ray ground reflection model. The radio model corresponds to the 802.11 WaveLAN, operating at a maximum airlink rate of 2 Mbps. The MAC protocol used is the IEEE 802.11 Distributed Coordination Function (DCF). The traffic pattern file was generated using "cbrgen.tcl" script, which is provided along with the standard NS-2 distribution. We used CBR traffic with the following parameters for our simulations:

Table 1: Traffic pattern for the scenarios

Max. number of connections	20
Application data payload size	512 bytes
Packet rate	4 packets/sec

Thus, effectively a bandwidth of 16 Kbps was used, which corresponds to applications such as the Combat Network Radio (CNR), which are self-forming networks comprised of highly mobile radios that can transmit voice and data for battlefield operations.

3.1. Metrics

The following are the metrics which we have used for the performance analysis.

a. *Packet Delivery Fraction (PDF)*: This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation.

$$PDF = \frac{numberOfReceivedPackets}{numberOfSentPackets}$$

PDF estimates how successful the protocol is in delivering packets to the application layer. A high value of PDF indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance.

b. *Normalized Routing Load (NRL)*: This is calculated as the ratio of the number of routing packets transmitted to the number of data packets actually received.

$$NRL = \frac{numberOfRoutingPacketsSent}{numberOfDataPacketsReceived}$$

NRL estimates how efficient a routing protocol is since the number of routing packets sent per data packet gives an idea of how well the protocol maintains the routing information updated. Higher NRL indicates higher routing overhead, and thus lower efficiency of the protocol.

c. *Average end to end delay (AED)*: This is defined as the average delay in transmission of a packet between two nodes and is calculated as follows:

$$AED = \frac{\sum_{i=0}^{n}(timePacketReceived_i - timePacketSent_i)}{totalNumberOfPacketsReceived}$$

A higher value of AED means the network is congested and hence the routing protocol does not perform well. The upper bound of AED is application-dependent. For example multimedia traffic such as audio and video cannot tolerate very high values of end-to-end delay when compared to other types of traffic such as FTP.

3.2. Description of the Scenarios

We consider three scenarios for our experiments, in which 50 nodes are distributed over the simulation area. The scenarios depict varying node densities and link changes. The scenarios are explained in the following sub-sections.

3.2.1. The Battlefield Scenario

The *Reference Point Group Mobility (RPGM)* model [14] is used for modeling the battlefield scenario. In RPGM model, a cluster of nodes communicate in groups. The velocity and direction of nodes within the group is determined by a 'group leader' or reference point. We define the parameters in this mobility model as follows:

Table 2: Parameters for battlefield scenario

Parameters	Values
Mobility model	RPGM
Distribution of nodes	10 in each group 5 groups
Simulation Area	2000 * 2000 m
Probability of group change	0.25
Node speed	Max speed: 5 m/s Min speed : 1 m/s
Maximum distance to group center	50 m

We consider a relatively sparsely populated set of nodes for this scenario. The total number of nodes is 50, while each node stays at a maximum of 50 meters from the group leader. We have a probability of 0.25 that there is a change in the group. For example, this may be caused due to death of a soldier or temporary movement for aiding other injured soldiers. The maximum speed of the nodes is taken as 5 m/s (which may depict military vehicles such as tanks) and minimum speed as 1 m/s (movement of soldiers).

3.2.2. The Rescue Operation Scenario

For this scenario, RPGM model is also used. This scenario represents groups of workers operating in a relatively small area. For example, in an avalanche rescue operation we may have set of nodes communicating within a small area. We consider a relatively denser set of nodes than the battlefield scenario. The nodes have lesser probability of changing a group (0.05) as compared to the battlefield scenario. The parameters for this scenario are listed in Table 3.

Table 3: Parameters for rescue op scenario

Parameters	Values
Mobility model	RPGM
Distribution of nodes	5 in each group 10 groups
Simulation Area	1000 * 1000 m
Probability of group change	0.05
Node speed	Max speed: 2 m/s Min.speed : 1 m/s
Maximum distance to group center	100 m

3.2.3. The Event Coverage Scenario

The *Gauss Markov mobility* model [14] was used to model the event coverage scenario. This model was developed in order to address the shortcomings of the Random Waypoint mobility model which generates unrealistic movements such as sudden stops and sharp turns. In this model we vary the degree of randomness by changing a tuning parameter. For our experiments, we vary the speed/angle update frequency to depict varying degrees of mobility within this model. The parameters are as follows:

Table 2: Parameters for event coverage

Parameters	Values
Mobility model	Gauss Markov Model
No. of nodes	50
Simulation Area	500 * 500 m
Maximum speed of nodes	5 m/s
Angle SD	0.5
Speed SD	0.5

We consider a higher density of nodes for this scenario in a smaller simulation area. For example, this may depict the communication between press reporters in a large hall covering some event. The mobility of the nodes are also higher (5m/s) when compared to the rescue operation scenario. The angle and speed standard deviation are each chosen to be 0.5.

4. Results

We varied the pause times from 0 to 1000 sec for the battlefield and rescue operation scenarios. For the event coverage scenario, we vary a parameter of the Gauss Markov mobility model called the speed or angle update frequency which is a measure of mobility. We vary the frequency of update from every 5 sec to every 60 sec. The impact of each scenario on the three metrics is studied for the three protocols chosen.

4.1 Impact on the Packet Delivery Fraction

We found that, for the battlefield scenario, SEAD outperforms DSDV and DSR in terms of packet delivery fraction for pause times of 100-400 sec, as shown in Figure 1.a.

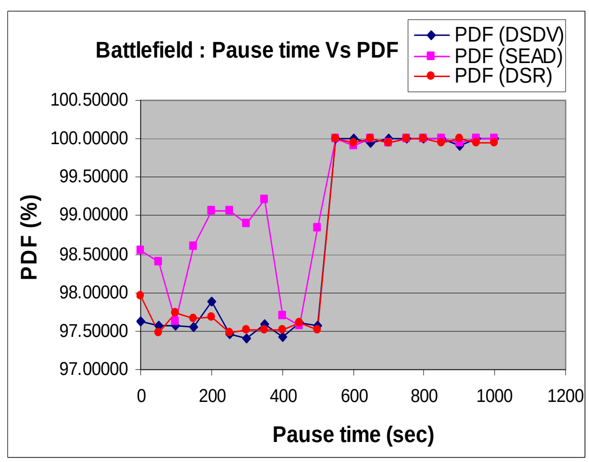

Figure 1.a: Battlefield (PDF)

This can be attributed to the fact that DSDV uses the *weighted settling delay* to reduce the number of routing table updates, which SEAD avoids. Thus SEAD typically has fresher routes at a given time than DSDV, and hence the nodes have more up-to-date routing tables, implying higher number of successfully delivered packets. For higher pause times (greater than 500 sec), all the three protocols converge to give a PDF of almost 100%, because the nodes are almost static and hence the congestion in the network decreases.

For the event coverage scenario, the effect of varying speed/angle update frequency is shown in Figure 1.b. DSR is found to have very high PDF when compared to SEAD and DSDV. This is due to the fact that DSR is a reactive protocol, and hence it adapts to changes in the network better than SEAD or DSDV, which are proactive. The event coverage scenario depicts a network with denser distribution of nodes and higher mobility as compared to the battlefield scenario, which shows that SEAD adapts better to link changes and mobility than DSDV.

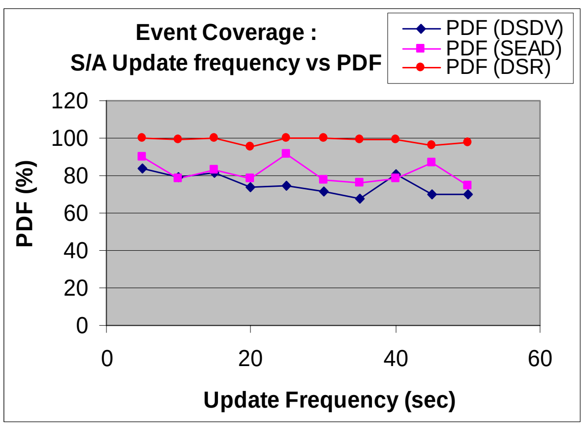

Figure 1.b: Event Coverage (PDF)

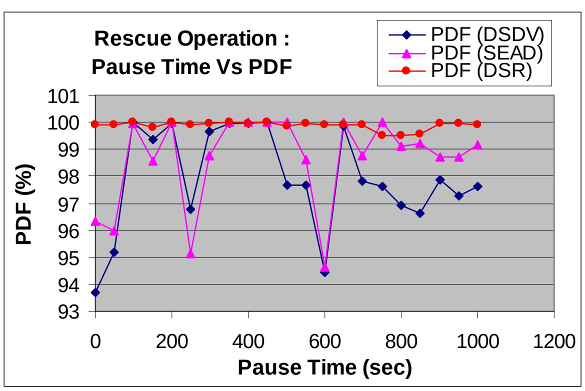

Figure 1.c: Rescue Operation (PDF)

In the rescue operation scenario, as shown in Figure 1.c, DSR again outperforms SEAD and DSDV, and gives a PDF of almost 100% at higher pause times. On the other hand, SEAD and DSDV exhibit varied performance, with SEAD outperforming DSDV for higher pause times (greater than 700).

4.2. Impact on Normalized Routing Load

Figures 2.a, 2.b and 2.c show the impact of varying mobility on the NRL for the scenarios. For all the scenarios, SEAD exhibits a higher routing overhead than DSR and DSDV. DSR has the least overhead of the three due to the fact that it is a reactive protocol and hence advertises routes only when required as opposed to the periodic routing updates in DSDV and SEAD.

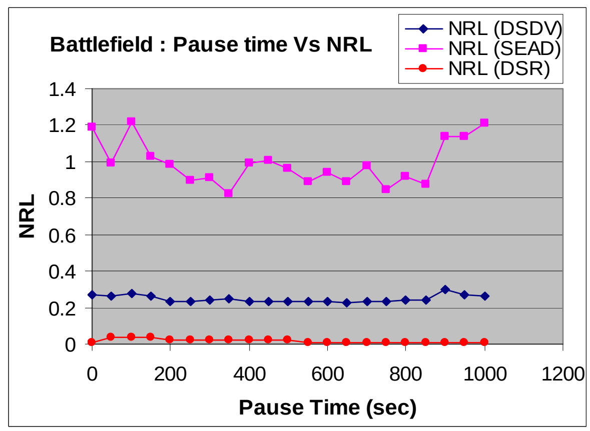

Fig.2.a Battlefield (NRL)

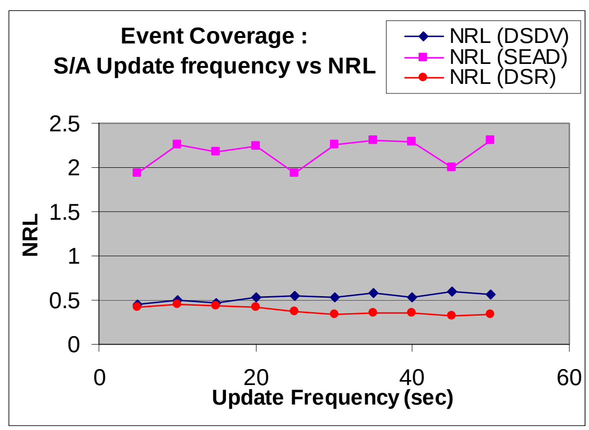

Figure 2.b: Event Coverage (NRL)

As the density of nodes increases, the NRL increases for DSDV and SEAD. The routing load for the event coverage scenario (high density of nodes) varies between 2 and 2.5 (Figure 2.b), whereas for the battlefield scenario (Figure 2.a) it varies between 0.8 and 1.2. DSR, however, exhibits stable values of routing loads across the three scenarios.

The routing load of SEAD is much higher than DSDV and DSR across all the three scenarios due to a higher number of routing advertisements sent by the nodes in the absence of the *average settling delay*.

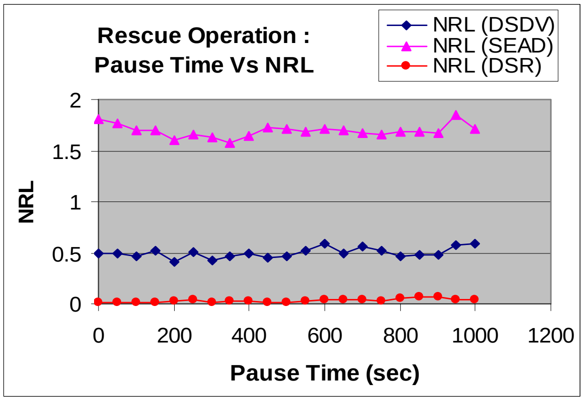

Figure 2.c: Rescue Operation (NRL)

4.3. Impact on Average End-to-end Delay

As shown in Figures 3.a, 3.b. and 3.c, SEAD exhibits a higher delay than DSDV and DSR. The computation of hash functions for authenticating the routes adds to the processing overhead at each node. Further, as the mobility increases, AED also increases. For a low density scenario such as the battlefield, the delay is much lower for SEAD, ranging between 7-8 msec (Figure 3.a), as compared to a higher density scenario such as the event coverage, where it varies from 10 to 16 msec (Figure 3.b).

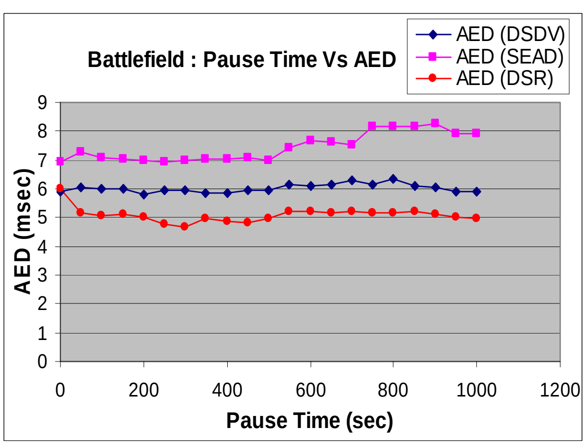

Figure 3.a: Battlefield (AED)

DSR exhibits a lower delay than DSDV and SEAD across all the three scenarios, which bolsters the fact that a reactive protocol tends to be faster than the proactive protocols under varying loads [8]. This may be important for applications such as multimedia which require a strict upper bound on the delay. Thus, DSR will be an ideal choice for such applications when security is not an issue.

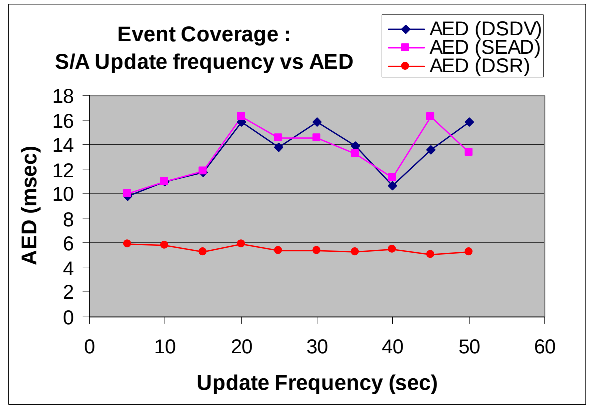

Figure 3.b: Event Coverage (AED)

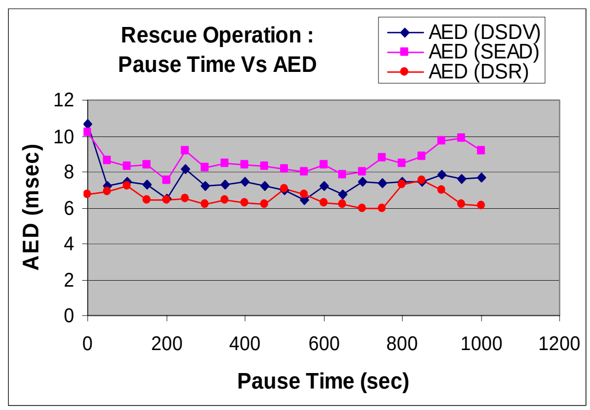

Figure 3.c: Rescue Operation (AED)

5. Conclusions and Future Work

We have performed a scenario-based evaluation of three routing protocols – DSDV, DSR and SEAD. Although prior studies have been conducted to evaluate these routing protocols, few of them have considered these protocols in real-life scenarios which may impose seemingly contradicting constraints including security, reliability, performance, and power conservation. Our set of scenarios – battlefield, rescue operation, and event coverage – represents a domain of critical applications. Take the battlefield scenario as an example. On one hand, it demands high security and high reliability, along with high overall performance; on the other hand, the nodes in this scenario have very limited processing capability and must conserve power.

Other than its security aspect, we find SEAD unsuitable for the *battlefield scenario*, mainly because a high NRL indicates higher network congestion. Besides, higher AED implies not only lower throughput but greater processing power for the nodes. Further, the proactive nature of SEAD causes more power consumption at each node due to higher number of routing advertisements. If security is not an issue, DSR would be an ideal choice for this scenario.

If one can afford to do without a secure protocol in a *rescue operation*, DSDV would be the ideal choice, since at any given point of time the probability of routing tables being up-to-date is higher when compared to DSR.

In the *event coverage* scenario, it is likely that multimedia type of traffic is exchanged between the nodes. Since SEAD exhibits high end-to-end delay it may not be suitable for such scenarios. DSR would be an ideal choice for this scenario due to its low value of NRL.

This line of work may be extended by studying other secure routing protocols such as ARIADNE and ARAN, and comparing their performances by using the scenarios described above. Further, a study of the secure routing protocols under varying network loads and traffic patterns will help designers to choose the right secure routing protocol for a particular scenario.

References

[1] Yih-Chun Hu, David B. Johnson, Adrian Perrig. *"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks"* Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp 3-13, 6/2002.

[2] P. Papadimitratos and Z. Haas. *"Secure routing for mobile ad hoc networks" (SRP)* SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 27--31, 1/2002.

[3] Lidong Zhou and Zygmunt J. Haas. "*Securing Ad Hoc Networks". IEEE Network*, 13(6):24-30, November/December 1999.

[4] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding royer. *"A Secure Routing Protocol for Ad Hoc Networks" (ARAN)* In International Conference on Network Protocols (ICNP), France, 11/2002.

[5] Yih-Chun Hu, Adrian Perrig, David B. Johnson. "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks" MobiCom 2002, 9/23-28, 2002, Atlanta, GA, US.

[6] Stefano Basagni (Ed), Marco Conti (Ed), Silvia Giordano (Ed), Ivan Stojmenovic, (Ed) *Mobile Ad Hoc Networking*, Wiley-IEEE Press*: Chapter 12, Ad hoc networks Security*, by Pietro Michiardi, and Refik Molva.

[7] J. Yoon, M. Liu, and B. Noble. "*Random Waypoint Considered Harmfu"l*. In Proceedings of INFOCOM. IEEE, 2003.

[8] 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*," Proc. *ACM/IEEE Mobile Computing. and Networking*, Dallas, TX, 10/1998.

[9] Johnson, D., and Maltz, D. "*Dynamic Source Routing in Ad Hoc Wireless Networks*". T. Imielinski and H. Korth, (Eds.). Kluwer Academic Publishers, 1996.

[10] C. E. Perkins and E. M. Royer. "*Ad hoc on-demand distance vector routing"*. In 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90-100, 2/1999.

[11] C. Perkins and P. Bhagwat. "*Highly Dynamic Destination-Sequenced Distance-Vector Routing* (*DSDV) for Mobile Computers*". In Proc. of the ACM SIGCOMM, 10/1994.

[12] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song. "*Efficient Authentication and Signing of Multicast Streams over Lossy Channels"*. In *IEEE Symposium on Security and Privacy*, pages 56–73, 5/2000.

[13] K. Fall and K. Varadhan, *The NS Manual*, The VINT Project, UC Berkeley, 1/2002.

[14] T. Camp, J. Boleng, and V. Davies, "*A Survey of Mobility Models for Ad Hoc Network Research*", Appeared in Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, 2(5), pp. 483-502, 2002.