Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks

Vikram Gupta[+], **Srikanth Krishnamurthy**[§], and **Michalis Faloutsos**[§]

[§]Department of Computer Science and
Engineering, UC Riverside,
Riverside, CA 92521.
{krish,michalis}@cs.ucr.edu

[+]Department of Electrical Engineering,
UC Riverside,
Riverside, CA, 92521
vgupta@ee.ucr.edu

Abstract

In this paper we analyze attacks that deny channel access by causing pockets of congestion in mobile ad hoc networks. Such attacks would essentially prevent one or more nodes from accessing or providing specific services. In particular, we focus on the properties of the popular medium access control (MAC) protocol, the IEEE 802.11x MAC protocol, which enable such attacks. We consider various traffic patterns that an intelligent attacker(s) might generate in order to cause denial of service. We show that conventional methods used in wire-line networks will not be able to help in prevention or detection of such attacks. Our analysis and simulations show that providing MAC layer fairness alleviates the effects of such attacks.

1. Introduction

Denials of Service (DoS) attacks are commonplace in the Internet. Guarding against DoS attacks is a critical component of any security system. While DoS has been studied extensively for the wire-line networks, there is lack of research for preventing such attacks in mobile ad hoc networks. Due to deployment in tactical battlefield missions these networks are susceptible to attacks of malicious intruders. These intruders might attempt to disrupt/degrade the functioning of the whole network or may harm a specific node. Traditional DoS attacks involve overwhelming a particular host. However, in mobile ad hoc networks, mobility, limited bandwidth, routing functionalities associated with each node, etc, present many new opportunities for launching a DoS. While we defer the discussion of the various types of DoS attacks in ad hoc networks to a later sub-section we point out that these attacks might be at the routing layer or at the MAC layer. The former would result in a disruption of routing functionalities while the latter could potentially disrupt channel access and may cause wastage of resources in terms of bandwidth and power. Distributed Denial of Service (DDoS) attacks usually refer to an attack by use of multiple sources that are distributed throughout the network.

In this paper we focus on DoS attacks in wireless ad hoc networks. More specifically, we investigate attacks at the medium access control layer. An attacker causes congestion in the network by either generating an excessive amount of traffic by itself, or by having other nodes generate excessive amounts of traffic. In wireless networks, DoS attacks are difficult to prevent and protect against. They can cause a severe degradation of network performance in terms of the achieved throughput and latency. We start out with listing possible DoS attacks and identifying possible methods to alleviate these attacks. Next, we investigate in detail the vulnerabilities of the IEEE 802.11 MAC protocol that make DoS attacks easy. We identify that the capture effect and the lack of fairness that arise when this MAC protocol is used may be especially exploited to cause disruptions in accessing important services. To our knowledge this work is one of the first attempts to characterize and quantify the effects of DoS attacks at the MAC layer in ad hoc networks. To gain an understanding of how fairness may prevent some of the DoS attacks, we emulate a perfectly Fair MAC (FAIRMAC) protocol[1]. We simulate various scenarios to understand the local and global effects of various types of DoS attacks with both the IEEE 802.11 MAC protocol and with FAIRMAC and discuss possible solutions to overcome or alleviate these effects. Our results show that the extent to which the performance of a wireless network or a service degrades on DoS depends on many factors such as location of malicious nodes, their traffic patterns, fairness provided in the network resources.

The paper is organized as follows. In Section 2 we provide the background in terms of prior work in the areas of security and intrusion detection in ad hoc networks. We also provide a description of the IEEE 802.11 MAC protocol and briefly describe some of the fairly well known problems that arise when it is deployed in ad hoc networks. In Section 3 we identify possible DoS attacks and suggest methods that may be used to overcome them. In Section 4, we explicitly look at

∗ This material is based upon work supported by the National Science Foundation under Grant No. 9985195, DARPA award N660001-00-18936

[1] We do not claim that such FAIRMAC can be implemented in a distributed manner or is an acceptable choice in terms of throughput. However, in absence of a clear choice for a fair MAC protocol for ad hoc networks we emulate a protocol that provides fairness and our objective is to understand how fairness may help in prevention against some DoS attacks.

attacks at the MAC layer; we present our simulations and discuss the effects on the network when (a) the IEEE 802.11 MAC protocol is used and (b) when FAIRMAC is used and generate an intuition for possible solutions that may be used to alleviate these effects.

2. Background

Prior work on Ad Hoc Network Security

Security in ad hoc networks has been the focus of attention in recent times [1,2,3,8]. However, DoS attacks have not been addressed. In [2], Zhang and Lee point out the various attacks that are possible at different layers of the protocol stack. They do discuss possible solutions to a few of these attacks but the discussion is mainly focused on intrusion detection in ad hoc networks. In [3] a methodology for providing a secure routing is discussed. The authors suggest that in order to ensure that a particular flow does not hog the channel, flows that have received the least time-share of the capacity within a pre-determined time window should be given a priority.

The IEEE 802.11 MAC protocol

A detailed description and analysis of the protocol may be found in [4]. We briefly describe the IEEE 802.11 MAC protocol and point out its vulnerabilities to DoS attacks. The protocol addresses the fact that Collision Sense Multiple Access (CSMA) is not sufficient to eliminate collisions in ad hoc networks or wireless LANs. It uses a distributed co-ordination function or DCF that is based on the exchange of control messages. A sender sends a Request to Send (RTS) message and in response a receiver sends a Clear to Send or (CTS) message if it is able to accept the message. Any node that overhears either of the messages is rendered silent. Thus the channel is available for the exclusive use of the communication under discussion. When a node wishes to transmit data it senses the channel to find out if any transmissions are in the vicinity. If there are any nearby transmissions or if a response to an RTS message is not received within a pre-determined number of attempts the node backs off in accordance to the binary exponential back-off scheme [4,5]. The binary exponential scheme favors the last winner amongst the contending node. This leads to what is called as the *capture effect*. Nodes that are heavily loaded tend to capture the channel by continually transmitting data thereby causing lightly loaded neighbors to back off again and again. These as well as other difficulties associated with using IEEE 802.11 in multi-hop wireless can be found in [5]. The capture effect may be exploited to create pockets of congestion in the network. However if a malicious node attempts to send large amounts of data to a distant node, the fact that the data has to traverse multiple hops leads to other ramifications and we examine these in detail in Section 4.

3. Types of Denial of Service Attacks and Preventive Measures

In this section we discuss some interesting DoS attacks in the wireless environment and suggest possible solutions. Our description is brief as exhaustive listing of such attacks; their prevention methods, and the evaluation of prevention methods are beyond the scope of this paper. In wireless networks DoS attacks could be mainly classified into two types, those that are at the routing layer and those that are at the MAC layer. Attacks at the routing layer could consist of the following:

a) The malicious node participates in a route but simply drops a certain number of the data packets. This causes the quality of the connections to deteriorate and further ramifications on the performance if TCP is the transport layer protocol that is used.

b) The malicious node transmits falsified route updates. The effects could lead to frequent route failures thereby deteriorating performance.

c) The malicious node could potentially replay stale updates. This might again lead to false routes and degradation in performance.

d) Reduce the TTL (time-to-live) field in the IP header so that the packet never reaches the destination.

Notice that all of the above could lead to congestion due to data that is either retransmitted or transmitted on erroneous routes only to be dropped at a later time. Some of these issues are addressed in recent literature [3,6]. In [6], the authors propose the use of the *promiscuous* mode wherein a node overhears the transmission of its neighbors and infers if the behavior and responses are normal. However, this overhearing may be very much dependent upon other transmissions in the vicinity and the MAC protocol in use. In [3] the authors prove that if end-to-end authentication is enforced, attacks by independent malicious nodes of types (b) and (c) may be thwarted. An attack of type (a) may be handled by assigning confidence levels to nodes, and using routes that provide the highest level of confidence. Of course, multiple paths might have to be maintained. An attack of type (d) may be thwarted simply by making it mandatory that a relay node ensures that the TTL field is set to a value greater than the hop count to the intended destination. If nodes collude, the authentication mechanisms fail and it is an open problem to provide protection against such routing attacks.

At the MAC layer the following attacks can be attempted:

a) Since we assume that there is a single channel that is re-used, keeping the channel busy in the vicinity of a node leads to a denial of service attack at that node.

b) By using a particular node to continually relay spurious data the battery life of that node may be drained.

An end-to-end authentication may prevent these attacks from being launched. If the node does not include a certificate of authentication it might be prevented from accessing the channel. However, if nodes collude and one of the nodes is the sending node and the other is the destination, MAC layer attacks are very much feasible. We will investigate the effects of these attacks and identify possible solutions in the following section.

4. Simulations and Discussion

In this section we quantify and evaluate attacks at the MAC layer. We have used we have used GLOMOSIM [7] for our simulations. Mobility and randomness of the topology complicate the analysis. In order to keep our analysis simple we test various attack scenarios for a static 12 x 12 grid topology, consisting of 144 nodes. Each node is separated from its neighbor by 350 meters. The transmission range of each node is fixed at 376m. A representative example of the topological structure of the network is shown below in figure 1. The metric for quantifying the effects of DoS attacks are the achieved throughputs as seen by 8 clients from a particular server. The clients are placed at the corners (nodes 1,3,6 and 8 in fig.1) and mid-way (nodes 2,4,5 and 7 in fig.1) along the edges of the grid. The server is placed approximately at the center of the grid. The nodes R1 and R2 in the figure represent nodes that route data through the server.

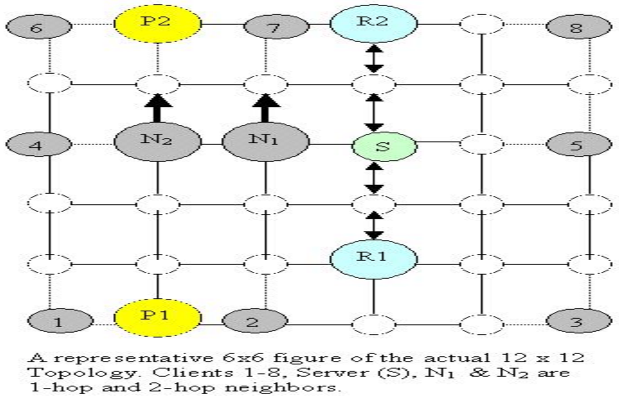
6
P2
7
R2
8
N2
N1
4
S
5
R1
1
P1
2
3
A representative 6x6 figure of the actual 12 x 12 Topology. Clients 1-8, Server (S), N1 & N2 are 1-hop and 2-hop neighbors.

Figure 1. Illustrative example of Server, Clients and Attackers.

We use FTP application clients in GLOMOSIM for the TCP connections. Each client sends 10 packets of variable size to the server by establishing a TCP connection with it. The simulation time is 900 seconds. The attack is simulated as a Constant Bit Rate (CBR) application client using UDP. The rate at which the attacker sends data is different for various attacks that we have simulated. We have extended GLOMOSIM to include a perfectly fair MAC protocol (FAIRMAC) by use of fixed time slots. Since we simulate a simple grid topology, we ensure that slot reuse is maximized. Through the comparison of performance of the network in presence of DoS attacks with 802.11 and FAIRMAC, we aim to characterize the effects of MAC layer fairness on a node's ability to withstand DoS[2].

Attack 1: *Objective:* The objective of this experiment is to show that a service is vulnerable to an attack from any of its 1-hop neighbors. The attacking node creates congestion by continually transmitting packets in the neighborhood of the service. For example, Node N_1 (in figure 1) sends data continuously to one of its neighbors (as shown by the arrow).

The simulation results with both the IEEE 802.11 MAC and FAIRMAC are shown in figure 2.

Observations:

a) Under the attack when the IEEE 802.11 MAC is used throughput goes down to almost zero for all nodes. This is because of the server's inability to receive data or to transmit TCP ACK packets.

b) Under the attack the FAIRMAC throughput does not suffer degradation in throughput in most cases.

c) One of the nodes (Node 4) does not get any bandwidth even with FAIRMAC. This is because the attacking node lies on the path from node 4 to the server. Packets from Node 4 suffer large queuing delays at node N1, thereby causing the degradation in throughput.

Discussion: We notice that node N1 was able to capture the media completely when the IEEE 802.11 MAC was used. However, the degradation in the case of FAIRMAC is not severe. Thus, ***MAC layer fairness*** is ***necessary*** in preventing attacks that capture the channel. Furthermore, our inability to provide any bandwidth to Node 4, even through a perfectly fair MAC (FAIRMAC), proves that MAC layer fairness is ***not sufficient*** as a prevention mechanism for such attacks.

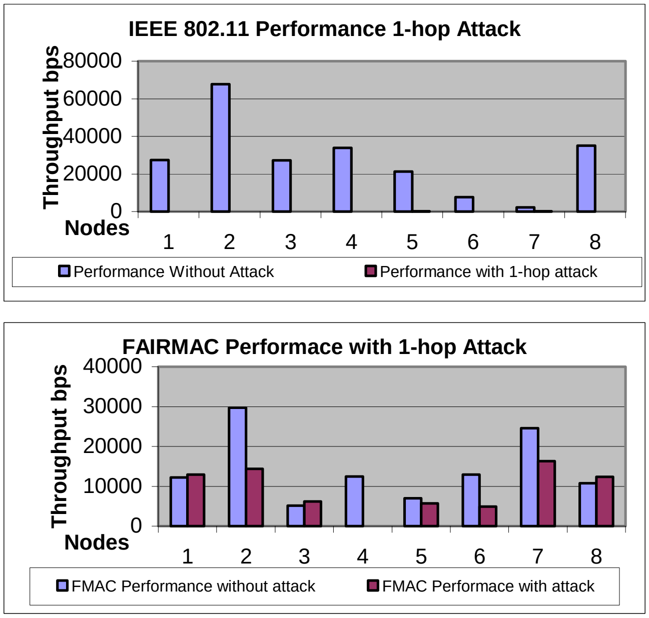

Figure 2. Neighbor Attack

Attack 2: *Objective:* The objective of this experiment is to show that a service is vulnerable to an attack from a node that is two hops away from it. For example, Node N2 (in figure 1) sends data continuously to one of its neighbors (as shown by the arrow from N2 in fig 1.). We experiment with 2 different scenarios; (a) Node N2 sends data to node N1 (that is in the neighborhood of the service) and in the other case to a different neighbor. The simulation results for both IEEE 802.11 MAC and FAIRMAC are shown in figure 3.

Observations:

a) We observe that even if the attack is from 2-hops away from the server, the degradation in the throughput with IEEE 802.11 MAC is very high.

b) When the IEEE 802.11 MAC is used and the attack is launched through N1, the *average throughput* of the server goes down. This is because the server has to wait for the duration indicated in the CTS messages sent by node N1 before it can receive data from any neighbor. Furthermore, the TCP ACK packets that it has to send get delayed resulting in timeouts at the client's TCP Layer.

c) We ran a similar simulation, except for the fact that the

[2] It should be noted that we do not attempt compare the performance of the two MAC Protocols; rather we only consider the absolute degradation in throughput

server node S was sending data to the clients (1-8) instead of receiving data from them. We found the IEEE 802.11 MAC degradation in throughput to be equally bad for the first case (node does not send packets to N1). However, the attack through N1 did not affect the throughput much. This is because the server node was able to capture the channel at times and send many packets, making an RTS-CTS message exchange less probable between node N1 & N2. Furthermore, the TCP ACK packets did not suffer from congestion related delays, as explained in (b) above.

d) FAIRMAC throughput is not degraded for any attack. The only node to suffer was node 4 (the reason is similar to case of attack 1). This is an expected result.

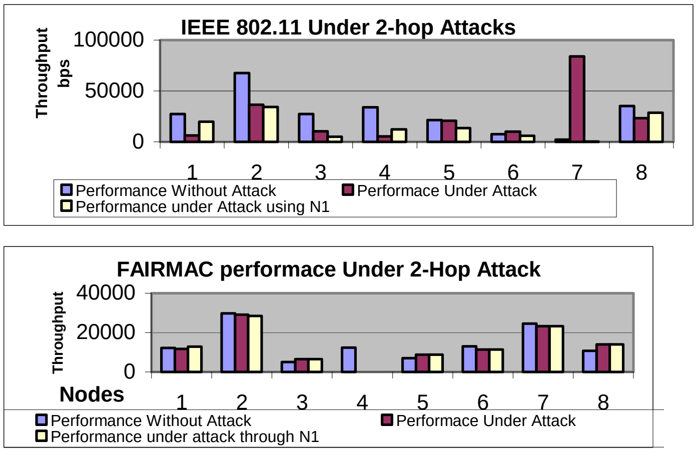

Figure 3. Attack From 2-hop Neighbor

Discussion: We notice that when using the IEEE 802.11 MAC a service is affected even if the attacking nodes are 2-hops away. From the observations (b) and (c) above, we find that throughput of server node S is affected because node N1 keeps sending CTS messages in response to N2's RTS messages. If node N1 identifies Node N2 to be a source of unwarranted flows, then it will stop responding to Node N2's RTS messages. Such a scheme is beyond MAC layer functionality and needs support from the network and other layers. Arguably, ***corroboration amongst different neighbor of the malicious node might be essential in isolating the node from harming the entire network***.

Attack 3: *Objective:* The objective of this attack is to show that two colluding nodes can attack a server even when they are not in the neighborhood of the node hosting the server. In figure 1, Nodes R1 and R2 establish a UDP session; the server node S is on the route from R1 to R2. In particular, for our experiment, a neighbor of 4 (refer fig. 1) sends data through the server node S to a neighbor of node 5 (the path length is 10 hop in a 12x12 grid). We have simulated two attack scenarios. In the first scenario the attacker sends data at a low rate of 10 packets/second (each packet is 1000Bytes in length) while in the second scenario the attacker sends packets at a high rate of 100 packets/second. The simulation results with the IEEE 802.11 MAC and FAIRMAC are shown in figure 4.

Observations:

a) With the attacker sending data at a low rate using the IEEE 802.11 MAC, the throughput is reduced for most nodes.

b) With the higher data rate we see that the throughput for many of the nodes is higher in comparison with the low data rate scenario. The decrease in the throughput for node 4 (near the attacking sender) and the corresponding increase in throughput for node 5 (near the attacking receiver) indicates that the attacker's strategy of sending data at a high rate may lead to ***localized congestion*** and the attacking flow does not harm the whole network.

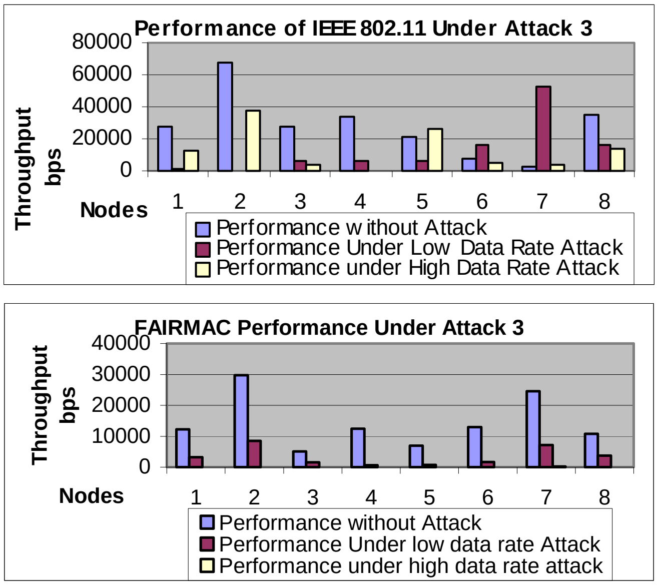

Figure 4. Attack by Distant Nodes

c) The FAIRMAC performance is also degraded for all nodes for both the case when the attacker transmits with the high rate and the case when it transmits at a low rate. Interestingly, the throughput goes to zero if there is a high data rate from the attacking source. This is counterintuitive. However, upon analysis, we find that whenever the server has a large number of packets to route, the acknowledgements packets for all the TCP connections suffer large ***queuing delays***, resulting in timeouts at the TCP client. This leads to degradation in throughput even for nodes that lie on paths that do not intersect with the attack flow.

d) In a similar experiment we used CBR application clients using UDP instead of the FTP based TCP sessions. In this case many of the clients did not suffer any degradation in throughput.

Discussion: We observe that it was possible for nodes R1 and R2 to attack the server, even when the source and destination of attacking flow were many hops away from the server. Importantly, if nodes R1 and R2 were colluding nodes they would have been able to authenticate themselves. Thus any ***end-to-end authentication scheme fails*** in preventing such an attack. However, such a scheme is still desirable because in its absence a malicious node can assume a false identity and convince a node to send large volume of data to any location in the network. Such attacks can be mitigated in environments where it is possible to **determine the legitimacy of a particular communication from its source-destination pair (by associating capabilities with them)**. Thus, R2 would have to refuse to participate in any such session if R1 is not "capable" of receiving/sending in large volumes or else risk being detected as a malicious node itself. We should note here the importance of routing information in this attack. R1 and R2 need to place themselves in such a way that S is on the path between them. Otherwise, they will need to manipulate the routing information so as to convince other nodes to route through S. In mobile environments routing information may be changing. Thus, it is more **difficult for malicious nodes to launch a DoS attack on a specific node that is at a large distance from them.**

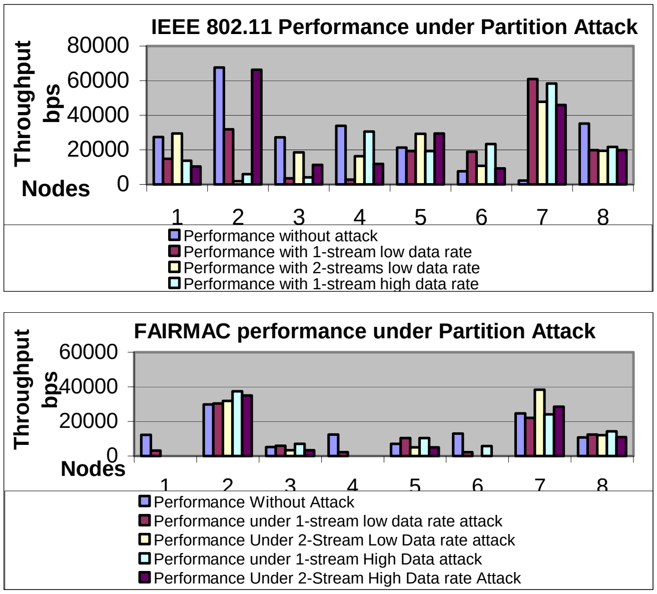

Figure 5. Network Partition Attack

Attack 4: *Objective:* The objective of this experiment is to show that it is possible for 2 colluding nodes to launch a DoS attack so as to separate a set of nodes from the rest of the network. These nodes P1 and P2 (in figure 1) establish UDP session(s) with each other in order to create a partition in the network by preventing data transfer between nodes that are on the opposite sides of their flow(s). We present simulation results for unidirectional and bi-directional flows and for low (10 packets/sec) and high (100 packets/sec) data rates. The results are presented in figure 5. We expect to see a DoS to nodes 1,4, and 6 (see fig. 1) that are separated from the server due to the partition created by the attacking flow(s). The unidirectional stream from p1originates near node 1 and terminates near node 6 at P2.

Observations:

a) When the IEEE 802.11 MAC is used, it is difficult for attacking nodes to create partition by unidirectional streams on long paths (fig. 5, node 4 gets affected but node 6 doesn't).

b) Sending data at a higher rate leads to **localized** congestion.

c) With the FAIRMAC, all of the attacks simulated affect the nodes 1,4,and 6. This is due to formation of **long queues** at the nodes along the attack path, leading to a partition of the network.

Discussion: It is possible for malicious nodes to partition the network. The effectiveness of **the partition depends on factors like traffic patterns** generated by the attacking node, **number of hops** on the path traversed by the malicious flow and topology of the network.

5. Conclusions and Future Work

In this paper we have shown how the 802.11 MAC protocol weaknesses can be exploited to launch DoS attacks in wireless ad hoc environment in various ways. We conclude that:

- The fundamental cause that DoS at MAC layer can take place is the capture effect and unfairness in media access.
- Our simulations and analysis show that MAC layer fairness, although certainly necessary, is not sufficient to alleviate the effects of various types of DoS attack.
- End-to-End authentication scheme fails in preventing an attack by two colluding nodes.
- Traffic patterns generated by an attacking node, its location in the network, availability of other compromised nodes, availability of routing information are key factors in determining the efficacy of the DoS.

In our studies so far we assumed that a malicious node would not tamper with the MAC protocol. However, MAC protocol should be made robust so that the effect of tampering is identified and not propagated. Such a scheme may need support in the form of corroboration from the neighbors. Many of the attacks that we have simulated are possible even when end-to-end authentication is enforced for each flow in the network. One of the possible ways of preventing unchecked flows is by the assignment of capabilities to nodes.

Our future effort will be address these issues.

6. REFERENCES

[1] L. Zhou and Z. Haas. Securing ad hoc networks. IEEE Network, 13(6):24--30, November/December 1999.

[2] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," ACM MOBICOM, 2000.

[3] P.Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[4] "Draft International Standard ISO/IEC 8802-11 IEEE P802.11/D10, Jan 1999", LAN MAN standards Committee of IEEE Computer Society.

[5] S.Xu and T.Saadawi, "Does the IEEE 802.11 MAC protocol work well in multi-hop wireless ad hoc networks," *IEEE Communications Magazine*, vol.39, Issue 6., June 2001.

[6] S.Marti, T.Giuli, K.Lai and M.Baker, "Mitigating Routing Behavior in Mobile Ad Hoc Networks", *Proceedings of Mobicom 2001*, Rome,2001.

[7] X Zeng, R. Bagrodia, and M. Gerla. *GloMoSim: a library for parallel simulation of large-scale wireless networks.* In Proceedings of the 12th Workshop on Parallel and Distributed Simulations, May 1998. 11.

[8] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun, "The Quest for Security in Mobile Ad Hoc Networks", In *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Long Beach, CA, USA, October 2001.