Improving the Reliability of Ad-hoc on Demand Distance Vector Protocol

Houssein Hallani and Seyed A. Shahrestani

School of Computing and Mathematics
University of Western Sydney, Locked Bag 1797
Penrith South DC, NSW 1797, Australia

Abstract: — Ad-hoc networks are a collection of mobile nodes that can be deployed without the need for any centralized management infrastructure. As such, the very basic operation of these networks is dependent on the cooperation of their nodes to provide communication routes. Furthermore, such networks are prone to several security risks. Consequently, when some nodes behave maliciously or in a selfish manner, the operation of the whole network can be severely affected. The behavior of such nodes can result in degradation of the performance of the network or even disruption of its operation altogether. This work reports the results of studying the Ad-hoc network performance in the presence of malicious nodes. It also proposes an approach that takes the behaviour history of member nodes into account, to improve network reliability. The reported approach, namely Behavior Ad-hoc On Demand Distance Vector approach, is based on discovery of communication paths with minimal number of selfish or malicious nodes. Using OPNET simulator, several situations of practical significance have been studied and analyzed. The results of these studies show that by applying the proposed approach, marked improvements in the performance and reliability of the Ad-hoc networks depend on AODV protocol can be achieved.

Keywords: — Ad-hoc networks, AODV, Behavior analysis, Malicious node, Selfish node.

1 Introduction

A wireless Ad-hoc network consists of a group of wireless devices capable of communication without the need for any pre-arranged infrastructure [1]. In such networks, to establish the needed communication paths, each node must act as a router allowing nodes that are not within radio range of others to interconnect [2]. A key feature of these networks is their ease of deployment, which makes them suitable for military fields, disaster and rescue operations, conferences, as well as home and mesh networking.

In Ad-hoc networks, a node may be considered as misbehaving for different reasons, for instance when it acts selfishly, refusing to forward packets. In some circumstances, the node can be overloaded, or they simply want to save their resources by not forwarding packets unless they are of direct interest to the node itself. Conversely, these nodes may still be expecting others to forward packets on their behalf [3].

In our previous works, performance evaluation and simulation validation of Ad-hoc networks using OPNET Modeler have been reported [4]. In this study, we expand those works to include the effects of the presence of malicious and selfish nodes in an Ad-hoc network. Different parameters are identified and combined to determine, if a node is reliable or if it is acting maliciously or selfishly. This can also assist with the detection of nodes that are not reliable or worse, misuse the trust placed in

them. Based on the results of those analyses, an approach referred to as Behaviour Ad-hoc On Demand Distance Vector (BAODV) approach that utilises the behaviour history of the network nodes is proposed. The main objective of BAODV is to discover communication paths with a minimal number of malicious or selfish nodes.

To achieve this, the remainder of this paper is organized as follows. In section 2, related work and motivations for this work are discussed. A detailed explanation of the proposed BAODV approach is presented in Section 3. In Section 4, an outline of the simulation setup together with results and their analysis are reported. This is followed by the concluding remarks in Section 5.

2 Malicious And Selfish Nodes In Ad-hoc Networks

Compared to conventional wired networks, wireless networks are more vulnerable to attacks. Unlike wired networks where an attacker must first gain access to the media, in Ad-hoc networks access to communication media is already available. Many attacks on Ad-hoc networks can be launched from inside as well as from outside the network. In this work, only internal attacks caused by malicious nodes or the effect of nodes acting selfishly are studied. Such nodes may try to broadcast traffic to all nodes in the network or simply drop packets. An inside attacker can generate fake routing messages causing a break down between the source and the destination, eventually leading to an invaded route or isolated node.

Given that Ad-hoc on demand distance vector (AODV) protocol [5] is the routing protocol used in this study, the following attacks are of concern. An attacker can invade a route by generating a fake Route Request (RREQ) message. Also the attacker may create a Route Reply (RREP) message to disrupt an existing route between two communicating nodes. Further, an inside attacker can form a loop in the network to consume resources of the nodes in the loop by generating faked RREP. Finally, the attacker may send fake Route Error (RERR) messages to disrupt routes [6].

Significant work has been done to improve routing in wireless Ad-hoc networks. Some of them apply a reputation analysis to tackle the problems associated with malicious and selfish nodes. Others make use of the public and symmetric key infrastructure by designing secure routing solutions. This is an ongoing and active area of research [7] and [8]. Many important problems and challenges still need to be addressed. These include the absence of a fixed infrastructure and centralized administration, as key management becomes a complicated problem and in turn making it difficult to provide proper security solutions [1].

An extension to AODV to secure it has also been proposed [9]. In this approach, it is claimed that the hop count information is the only mutual field in AODV and so used hash chains to secure this field. This approach also works under the assumption that an efficient key management system that distributes public keys to all nodes of the network is present. This is a serious drawback for its application in Ad-hoc networks in most practical situations.

A reputation-based scheme to identify malicious nodes has also been studied [10]. If a node fails to route the packet, it gets a low reputation mark that over time can result in expulsion of the node from the network. However, this approach has the serious drawback of requiring acknowledgment to be sent by the destination to achieve higher reputation for the routing nodes that behave properly.

3 Behavior Ad-hoc on Demand Distance Vector Protocol

In the proposed BAODV approach the source node attempts to find a route to the destination node that is free of malicious and selfish nodes. This is somehow different from the traditional AODV protocol, trying to choose the shortest route. To achieve this, a new parameter is added to AODV protocol relating to the behaviour

history of the nodes. For each node, this parameter is a function of the packets relayed by that node, including control and data packets. In the initial stage, this parameter is the same for all nodes. Every time a node forwards a packet the parameter is incremented. Conversely, when a node fails to transmit a packet that it is supposed to relay, the parameter is decremented.

As with AODV, when a source node S has a packet destined for a destination node D, the routing module of the source node broadcasts a route request for a route from node S to node D. All the neighbours of node S receive the route request and check their local routing tables for a path to D. If any of them has a route to D, it sends a route reply back to node S. If multiple neighbours have routes to node D, they all reply back to node S. When multiple paths exist, using BAODV, node S chooses the route from the neighbour with the highest value of the parameter that indicates the trustworthiness.

In BAODV the node does not need to wait to receive an acknowledgment from the destination in order to update the parameter that indicates the behaviour history. Instead, the update is done after the node forwards the packet. This is different from the solution reported in [10]. The BAODV technique solves the possible problem of not receiving the acknowledgment due to reasons related to poor signal or availability. So, it overcomes one of the shortcomings of the solution reported in [10] where the entire route receives a negative feedback for a reason other than that caused by a malicious attack or acting selfishly. In BAODV, if an intermediate node drops the packet, it will not affect all the nodes in the corresponding route. This process is repeated until the packet reaches the destination node.

It should be noted here that there is a possibility that an intermediate node forwards the packet to a third node that is not a part of the route in order to deceive the originator node. This is solved by checking the acknowledgment sent back from the destination node to the source node. When an intermediate node receives the acknowledgment packet, it retrieves the record corresponding to the IP address of the packet. The record contains the previous-hop and the next-hop nodes of the IP address. If the information matches, it forwards the acknowledgment to the previous-hop. In addition, it deletes the entry for the IP address from the routing table. If the information does not match, the intermediate node will decrement the behaviour parameter of the node that delivered the acknowledgment and aborts the packet.

4 Simulation Study Results

The simulation studies are carried out using OPNET Modeler V11.5. OPNET Modeler is used to construct models for two different purposes: to study system behaviour and performance; and to deliver a modeling environment to end users [11]. A network model may contain any number of communicating entities called nodes. Nodes are instances of node models; developed using the Node Editor. Network models consist of nodes and links that can be deployed within a geographical context. Node models consist of modules and connections. Each simulation scenario consists of fifty nodes, an Application Configuration, and a Profile Configuration. Fig. 1 shows a snapshot of the simulation setup. The Application and Profile Configuration are used to define the type of traffic sent between the nodes. The channel speed of the wireless LAN is set to 11 Mbps. The routing protocol used in the simulation is the AODV protocol. The MAC layer model is the OPNET implementation of IEEE 802.11 WLAN model.

To study the effects of the presence of malicious nodes in Ad-hoc networks, two performance metrics will be measured for a number of scenarios and situations. These are the throughput, and the packet loss rate. In this work, the total measured throughput is considered as the average amount of data payload transmitted and received over a period of time between two nodes [12]. It is measured

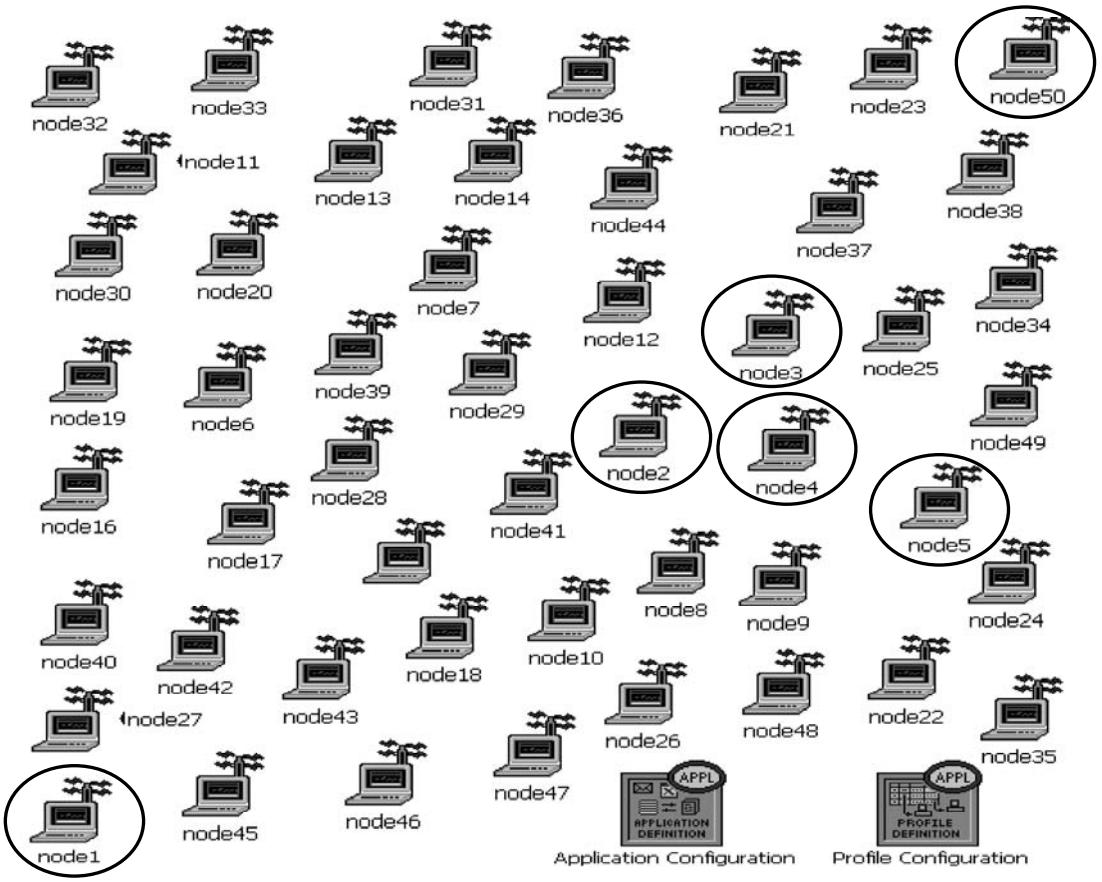

Fig. 1 A snapshot of the OPNET simulation setup

in Mbps. The packet loss percentage at nodeX for transmission between nodeX and nodeY describes the percentage of packets transmitted from nodeX over the network that did not reach nodeY.

The simulation study consists of number of scenarios replicating practical situations. For more information about the physical set-up of simulations please see [4]. In the first part we concentrate on the effects of malicious nodes trying to interfere with the communicating nodes by sending background traffic. Each scenario is running in five different situations. In the first situation, no malicious nodes are present in the network's fifty nodes, and only nodes involved in the communication are sending and receiving data. In the second situation, five random nodes out of the fifty nodes are malicious nodes. Ten malicious nodes are present in the third situation, whilst in the fourth; fifteen nodes are considered malicious nodes. In the fifth situation, twenty out of the fifty nodes are malicious nodes.

In the baseline scenario, only node2 and node4 are involved in the communication. TCP traffic is sent from node2 to node4 and the throughput, and the packet loss rate are measured at node2. In the first scenario node2 and node3 are set up to send TCP traffic to node4. While in the second scenario node5, node3, and node2 are communicating simultaneously with node4. In the third scenario node2 is sending TCP traffic to node5 through other nodes acting as relay nodes between the source and the destination.

To check the effect of the transport protocol used between the communicating nodes on the performance of the Ad-hoc network, the same scenarios are repeated when the communicating

	Description
Baseline Scenario	only two nodes involved in the communication, node2 is sending TCP traffic to node4
First Scenario	node2 and node3 are communicating simultaneously with node4 sending TCP traffic
Second Scenario	node 4 is receiving TCP traffic generated and sent at the same time from node2, node3, and node5
Third Scenario	node2 is sending TCP traffic to node5 (node2 is not within the range of node5 so node2 uses other nodes as relay nodes)
Fourth Scenario	only two nodes involved in the communication, node2 is sending UDP traffic to node4
Fifth Scenario	node2 and node3 are communicating simultaneously with node4 sending UDP traffic
Sixth Scenario	node 4 is receiving UDP traffic generated and sent at the same time from node2, node3, and node5
Seventh Scenario	node2 is sending UDP traffic to node5 (node2 is not within the range of node5 so node2 uses other nodes as relay nodes)
Eighth Scenario	node1 is sending TCP traffic to node50 (all nodes are motionless)
Ninth Scenario	node1 is sending TCP traffic to node50 (all nodes are mobile at a speed of 10m/s following a defined trajectory)
Tenth Scenario	node1 is sending UDP traffic to node50 (all nodes are motionless)
Eleventh Scenario	node1 is sending UDP traffic to node50 (all nodes are mobile at a speed of 10m/s following a defined trajectory)

Table 1 Description of the scenarios used

nodes are sending UDP data traffic.

In the second part of simulation we have tried to make the situation more random and general by changing the way malicious nodes are acting. Thus four categories of malicious nodes are defined here. In the first type, malicious nodes are dropping packets based on the simulation time (for example dropping all packets when the simulation time is between 50 and 100 sec). In the second group, malicious nodes are dropping every second packet, while in the third type nodes are dropping every fifth packet. For the last category, nodes are dropping every eighth packet.

To further study the effect of node mobility on the performance of Ad-hoc networks, all nodes are moving randomly with a maximum speed of 10 m/s. After the start of the simulation, mobile nodes wait for 60 seconds before they start to move randomly for 20 seconds Table 1 shows a brief description of the

	Malicious TCP Traffic (Measured in Mbps)	Malicious UDP Traffic (Measured in Mbps)
Baseline Scenario	4.59	4.79
First Scenario	2	2.14
Second Scenario	1.45	1.62
Third Scenario	1.71	1.83

Table 2 Throughput comparison for the baseline, first, second and third scenarios measured in Mbps

	Malicious TCP Traffic	Malicious UDP Traffic
Baseline Scenario	13.8%	9.82%
First Scenario	27.74%	22.68%
Second Scenario	28.5%	23.12%
Third Scenario	28.9%	22.27%

Table 3 Packet Loss comparison for the baseline, first, second and third scenarios

scenarios used.

All simulations run for five minutes. Table 2 shows the throughput variation values collected at node2 and when 40% of the nodes are acting maliciously. This table shows both situations where the malicious nodes are sending UDP and TCP traffic. It is clear from these values that the impact on the throughput is less when the malicious nodes are using UDP traffic rather than TCP traffic. This is attributed to the nature of TCP, which ensures that the data is delivered error free and in order. As the receiving node does not distinguish between malicious and data traffic, delays at node2 can be expected. This is in line with previously published results [3].

Table 3 shows the packet loss percentage variation for the baseline, first, second and third scenarios while the destination node is receiving TCP traffic. Also these values represent both situations where the malicious nodes are sending UDP and TCP traffic. It is also clear from these values that the packet loss rate is affected by the presence of the malicious nodes in the network. This table also shows that this performance metric is also weighed down by the transport protocol that the malicious nodes are using. This might be attributed to the fact that malicious nodes are trying to retransmit their traffic when using TCP. This process at nodes2 cannot distinguish between normal and malicious traffic causing higher packet loss rate compared to when malicious nodes are using UDP.

The following section displays the results of the fourth, fifth, sixth, and seventh scenarios when the communicating nodes are sending UDP data traffic. As stated before, this has been done to check the effect of the transport protocol on the performance of Ad-hoc networks. The values in Table 4 show the throughput variation for these scenarios. The measurement is made at the sending node (node2) and the table shows both situations where the malicious nodes are sending UDP and TCP traffic. It is noticeable from this table that the malicious nodes have affected the throughput between the communicating nodes for all scenarios. These values also indicate that the impact on the throughput is less when the malicious nodes are using UDP traffic. This can be attributed to the use of the window mechanism to control the flow of data in TCP. When a TCP connection is established each end of the connection allocates a buffer to hold incoming data. If the receiving application can read data as quickly as it arrives, the receiver will send a positive window advertisement with each acknowledgement.

	Malicious TCP Traffic (Measured in Mbps)	Malicious UDP Traffic (Measured in Mbps)
Fourth Scenario	4.91	5.15
Fifth Scenario	2.38	2.71
Sixth Scenario	1.51	1.72
Seventh Scenario	2.11	2.23

Table 4 Throughput comparison for the fourth, fifth, sixth and seventh scenarios measured in Mbps

However, it is well known that if the sender is faster than the receiver, incoming data will eventually fill the receiver's buffer.

Thus, as data and malicious traffic arrive at node2, node2 sends acknowledgements to each node causing delay and full buffer at node2. In this situation node2 advertises a zero window. A sender that receives a zero window advertisement must stop sending until it receives a positive window, causing delays at node2.

Table 5 shows the packet loss percentage variation for the fourth, fifth, sixth, and seventh scenarios. Also this table shows both situations where the malicious nodes are sending UDP and TCP traffic. It is also clear from these values that the packet loss rate is affected by the presence of the malicious nodes in the network. These values also show that this impact differs based on what transport protocol the malicious nodes are using. For example in the fifth scenario, the packet loss rate when 40% of the nodes are acting maliciously has raised from 0 to around 8% when malicious nodes are using

	Malicious TCP Traffic	Malicious UDP Traffic
Fourth Scenario	8.05%	3.37%
Fifth Scenario	18.6%	7.14%
Sixth Scenario	19.1%	7.59%
Seventh Scenario	12.25%	9.96%

Table 5 Packet Loss comparison for the fourth, fifth, sixth and seventh scenarios

UDP protocol compared to 19% when malicious nodes are sending TCP background traffic. By comparing the values in these four tables, it is noticeable that the throughput and packet loss rate when nodes are communicating using TCP protocol is higher compared to when they are using UDP protocol which might be due to the use of the windows mechanism in the connection oriented TCP protocol.

The following section discusses the results of the second part of the simulation. As stated before, in this part node1 is communicating with node50 via other nodes as shown in Fig. 1, which act as relay nodes between the source and the destination. Several scenarios and simulations were performed before and after applying the proposed BAODV approach in order to study the effect of the use of the behaviour history of the nodes on the overall performance.

In the eighth scenario the communicating nodes are sending TCP data traffic while the throughput comparison measured at node50. The results for this case clearly show that the throughput increases when BAODV is used. This is due to the fact that node1 is now sending the packets to node50 through a route which has a reduced number of malicious nodes, compared to using AODV alone.

The graphs in 2 show the throughput comparison for the ninth scenario. In this scenario nodes are moving according to the defined trajectory given earlier in the paper. Studying these graphs, it is noticeable that the throughput has also increased when applying the proposed approach. It is also clear that the throughput is higher when the nodes are motionless. This is due to the fact that when moving, the node can drop the connection with its neighbors causing the routing protocol to reinitiate the route between source and destination.

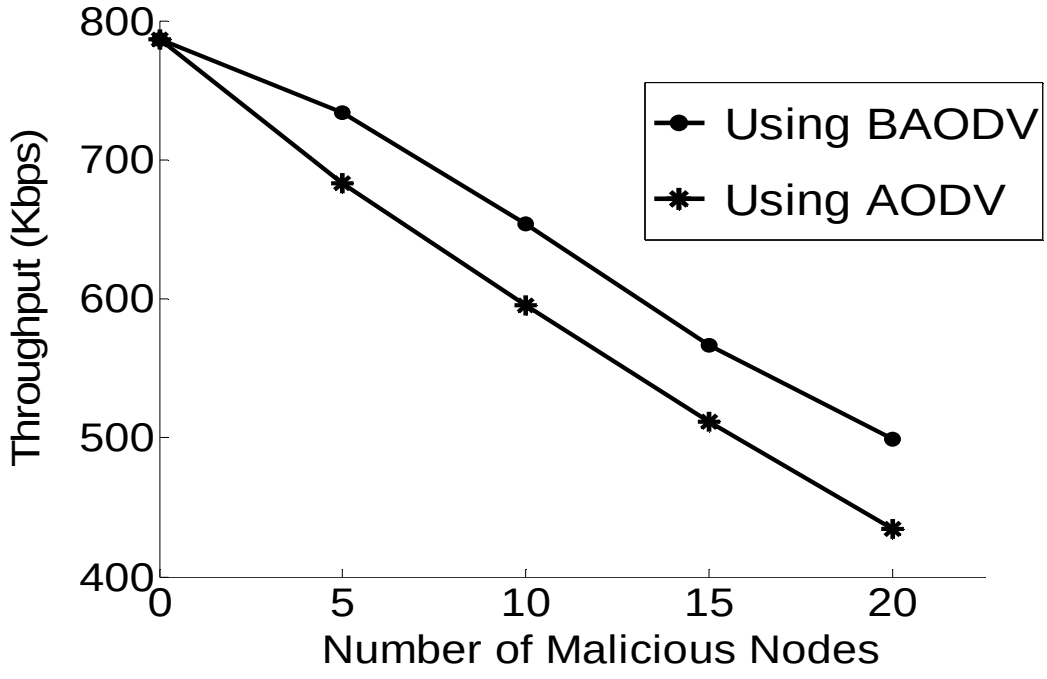

Fig. 2- Throughput comparison for the tenth scenario measured at node50. In this scenario node1 is sending UDP traffic

	Without the Proposed Approach	With the Proposed Approach
Eighth Scenario	51%	45%
Ninth Scenario	57%	49%
Tenth Scenario	44%	36%
Eleventh Scenario	52%	44%

Table 6 Packet Loss comparisons for the eighth, ninth, tenth, and eleventh scenarios

Table 6 shows the packet loss percentage values for the eighth, ninth, tenth and eleventh scenarios when 40% of the nodes are acting maliciously. This table shows both situations before and after applying the proposed approach. It is noticeable here that the packet loss rate has decreased with the proposed approach for all scenarios. The decrease in the packet loss can also be credited to the fact that the new route between source and destination has none, or less, malicious nodes. It can also be noted that the packet loss is lower when the nodes are motionless. This can be attributed to the fact that packets are dropped when losing the connection between the moving nodes.

5 Conclusions

In this paper, the effect of malicious and selfish nodes on the performance of Ad-hoc networks is presented. With the lack of central infrastructure in these networks, evaluating and establishing trust and dependability between their comprising nodes is not an easy task. To overcome this difficulty, a new approach based on utilization of past behaviour of nodes is proposed. The approach referred to as BAODV, is an extension of the AODV protocol. This approach is based on the behaviour history of all member nodes of Ad-hoc networks.

The results of a number of simulation studies based on using conventional routing techniques with and without implementing the proposed approach are also reported. The results corresponding to cases where the proposed approach has been implemented show significant improvements in the performance and reliability of the wireless Ad-hoc networks in the presence of malicious or selfish nodes. For instance, with 40% of the nodes of the Ad-hoc network acting maliciously, and nodes being either stationary or mobile, increases in the throughput of 11% and 13% respectively, can be achieved.

Acknowledgement

We would like to thank OPNET for their kindness in providing us with Modeler software license, which has greatly assisted in finalizing this paper. We also would like to thank Cisco for the generous scholarship which has permitted us to reach forward with our studies.

References:

[1] C. E. Perkins, "Ad-hoc Networking," *Addison-Wesley*, 2000.

[2] K. S. Ng and W. K. G. Seah, "Routing security and data confidentiality for mobile Ad-hoc networks," in *57th IEEE Semiannual Vehicular Technology Conf. (VTC 2003-Spring)*, 2003, pp. 1821-1825 vol.3.

[3] A. S. Marti, A. T. J. Giuli, A. K. Lai, and A. M. Baker, "Mitigating routing misbehavior in mobile Ad-hoc networks," in *6th Int. Conf. on Mobile computing and networking*, Boston, Massachusetts, United States, 2000, pp. 255-265.

[4] H. Hallani and S. A. Shahrestani, "Performance Evaluation and Simulation Verification for Wireless Ad-hoc Networks," *WSEAS Transactions on Communications*, vol. 4, pp. 355-362, July 2005.

[5] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Mobile Computing Systems and Applications*, 1999, pp. 90-100.

[6] P. Ning and K. Sun, "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols," *Ad Hoc Networks*, vol. 3, pp. 795-819, 2005/11 2005.

[7] G. C. Hadjichristofi, W. J. Adams, and N. J. Davis, IV, "A framework for key management in mobile Ad-hoc networks," in *Int. Conf. on Information Technology: Coding and Computing, (ITCC 2005)*, 2005, pp. 568-573 Vol. 2.

[8] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad-hoc Networks," in *3rd IEEE Int. Conf. on Pervasive Computing and Communications, (PerCom 2005)*, 2005, pp. 191-199.

[9] M. G. Zapata, *Secure ad hoc on-demand distance vector (saodv) routing*: Internet Engineering Task Force (IETF) Draft, 2004.

[10] P. Dewan, P. Dasgupta, and A. Bhattacharya, "On using reputations in Ad-hoc networks to counter malicious nodes," in *10th Int. Conf. on Parallel and Distributed Systems, (ICPADS 04)*. 2004, pp. 665-672.

[11] OPNET Modeller, http://www.opnet.com.

[12] S. Ci and H. Sharif, "A link adaptation scheme for improving throughput in the IEEE 802.11 wireless LAN," in *27th Annual IEEE Conf. on Local Computer Networks (LCN 2002)*. 2002, pp. 205-208.

[13] Kumudu S. Munasinghe and Seyed A. Shahrestani, "Performance Analysis of Multi-tunnel Virtual Private Networks in Wireless Environments," *WSEAS Transactions on Communications*, vol 4, pp 334-345, 2005.