Measure of Impact of Node Misbehavior in Ad Hoc Routing: A Comparative Approach

Manoj Kumar Mishra[1], Binod Kumar Pattanayak[2], Alok Kumar Jagadev[3], Manojranjan Nayak[4]

**[1]Dept. of Information Technology, SOA University,
Jagamohan Nagar, Jagamara, Bhubaneswar – 751030**

**[2]Dept. of Computer Science & Engg., SOA University,
Jagamohan Nagar, Jagamara, Bhubaneswar – 751030**

**[3]Dept. of Computer Science & Engg., SOA University,
Jagamohan Nagar, Jagamara, Bhubaneswar – 751030**

**[4]President, SOA University,
Jagamohan Nagar, Jagamara, Bhubaneswar – 751030**

Abstract

The major challenge to design and deployment of mobile ad hoc networks (MANETs) is its dynamic nature, which carries with itself a set of security measures to be resolved. In this paper, we compare the behavior of three routing protocols DSDV, DSR and AODV under security attack, where the investigation is carried out with respect to two types of node misbehavior. The parameters taken into consideration for evaluation of network performance are normalized throughput, routing overhead, normalized routing load and average packet delay, when a certain percentage of nodes misbehave. It could be established through simulation results that DSDV is the most robust routing protocol under security attacks as compared to the other two. In addition, it reveals that a proactive routing protocol reduces the impact of security attack by excluding the misbehaving nodes in advance.

Keywords : *Ad hoc network, routing, selfish nodes and security.*

1. Introduction

A group of wireless nodes communicating in a localized wireless environment in the absence of any centralized administration and any fixed infrastructure, is known as a mobile ad hoc network (MANET). Dynamic nature of MANETs requires implementation of proper routing protocols, which should be adaptable to frequent changes in network topology and the nodes should be able to exchange information regarding topology changes to establish routes. Such frequent changes very often bring about the security issues in ad hoc networks. Traditional routing protocols cannot be useful to resolve these security issues in ad hoc networks due to its frequently changing network dynamics. As a result of frequent topology changes, packets exchanged between a pair of wireless nodes may follow different routes at different instants of time, and thereby may be exposed to attacks. At the same time, unlike in wired networks, it is difficult to authenticate the node of a MANET in the absence of on-line servers [1]. The group of commonly encountered attacks may include replay attack, denial of service (DoS), modification, masquerading, routing table overflow, impersonation, energy consumption etc. [2]. A number of solutions have been proposed to protect routing messages from being modified by the attackers or harmful messages being injected to the network [1,3,5 and 6].

Authors in [4] have carried out an analysis of security exposures in MANETs with an assumption that the nodes misbehave under security attacks. The Dynamic Source Routing (DSR) Protocol [9] lists three types of node misbehavior in routing as experienced by MANETs. Simulations suggest that network operation and maintenance can be easily jeopardized and network performance can be severely affected as a result. In this paper, we intend to compare the performance of DSR under security attacks with that of DSDV (Destination Sequenced Distance Vector) [7] and AODV (Ad hoc On-demand Distance Vector) [8] protocols. It should be noted that the performance of above three protocols have been extensively studied in the absence of any security threat prior to the above mentioned comparison [10]. In course of this simulation, the robustness of each of these protocols is observed in the presence of security attack.

The rest of the paper is organized as follows. A brief discussion of the above three protocols is included in section 2 with two types of node misbehavior being taken into consideration. The simulation environment and methodology are covered in section 3. Simulation results are discussed in Section 4 and Section 5 includes the conclusion and the future extensions.

2. Ad Hoc Routing Protocols and Misbehaving Nodes

2.1 Routing Protocols :

The routing protocols implemented in MANETs are globally classified into two categories: proactive or table driven protocols and reactive or on-demand protocols. Table driven protocols rely on a table, which maintains consistent up-to-date information regarding routes to all possible destinations, whereas on-demand routing protocols implement source-initiated route establishment, where a route is created when desired by the node. In this paper, we compare the performance of a table-driven protocol DSDV with two most popular on-demand routing protocols such as DSR and AODV.

Proactive routing protocol DSDV operates with a table driven algorithm, based on Bellman-Ford routing mechanism. In this approach, every mobile node in the network maintains routes to all possible destinations with number of hops in between. Each entry is marked with a sequence number as assigned by the destination node. With the help of sequence numbers, mobile nodes can be able to distinguish stale routes for the new ones, and as a result, routing loops can be avoided.

Reactive routing protocol DSR comprises two mechanisms: route discovery and route maintenance. It enables the mobile nodes in an ad hoc network to discover routes to arbitrary destinations as per requirement. In the beginning, the source node initiates a Route Discovery mechanism comprising two phases: Route Request and Route Reply. On successful completion of these two phases, a route is established between the source and destination following which the source node appends the destination address to its data packets and sends them along the route. The intermediate nodes act as routers of the packets and do not maintain any up-to-date routing information.

Reactive routing protocol AODV is an enhancement of DSDV, which significantly minimizes the number of broadcasts required during route establishment by creating routes on-demand basis. It does not need to maintain all possible routes unlike DSDV, which convincingly reduces the required storage capacity at a node in the MANET. As suggested by authors of AODV, it is a perfect on-demand routing protocol, since nodes not belonging to a route, do not necessarily participate in route discovery, neither maintain up-to-date routing information. A source node needs to initiate a route discovery mechanism, when it has to send to a required destination.

2.2 Node Misbehaviors :

Identification of misbehaving nodes in ad hoc networks is critically important to detect security attack in the network. Two types of misbehaving nodes such as selfish and malicious nodes are taken into consideration in [4]. Selfish nodes do not intend to directly damage other nodes, but however, do not cooperate, saving battery life for their own communications. But malicious nodes do not give priority to saving battery life, and aim at damaging other nodes. In the current research paper, with reference to [4], we introduce two different types of selfish nodes. As the nodes in MANETs are battery powered, energy becomes a precious resource, and thus, role of selfish nodes draws more attention.
Thus, we introduce altogether three routing behaviors of nodes in a MANET.

a) Type 0 : well-behaved node : A well behaved node cooperates in the communication well, performs as required by the routing protocol, and equally participates in the communication activities like route discovery, maintenance, packet forwarding and receiving etc.
b) Type-1 : active selfish node : Such a node does not participate in packet forwarding, and drops every received packet, and thus, it disables the packet forwarding mechanism for the packets which have a destination address, other than this selfish node. In fact, it helps the selfish node to save its own energy, thereby still contributing to network maintenance.
c) Type 2 : passive selfish node : Such a node practically does nothing and stays idle in the network. It does not contribute to any of the activities like packet forwarding, receiving, route discovery, network maintenance.

With respect to above mentioned misbehaving nodes, we evaluate the performance of DSDV, DSR and AODV routing protocols through extensive simulations, where a certain percentage of nodes behave as active and/or passive selfish nodes with the remaining nodes being well-behaved.

3. Simulation Methodology and Simulation Environment

We use network simulator ns2 for our proposed simulations. It comprises the models and modules at physical and data link layers, MAC layer protocols and the ad hoc routing protocols DSDV, DSR, AODV, which we need to compare. Speed of a node in the ad hoc network is uniform (Random way point mobility model). After reaching the destination, a node pauses for a specified interval of time before choosing a random destination and repeating the process. Constant Bit Rate (CBR) traffic is chosen for communication among randomly selected nodes. Two types of node misbehaviors mentioned above are incorporated in ns2 as separate node definition types, which allow picking a selfish model between two possible choices. Table 1 lists some common parameters used in course of the simulation.

Table 1:Fixed parameters for simulation

Parameters	Values
Area	1000m x 1000m
Radio range	250 m
Link capacity	2 Mbps
Pause time	5 seconds
Simulation time	200 seconds
Buffer size	50 packets
Application	Constant bit rate (CBR) traffic
Packet size	512 bytes

In addition to the parameters, specified in Table-1, we change certain aspects of MANETs in order to evaluate the network performance of routing protocols under security attack. Table 2 lists these aspects.

Table 2 : Variable parameters for simulation

Parameters	Values
Network density	High (60 nodes) / low (20 nodes)
Network mobility	High (15 m/s)/ low (20 nodes)
Routing protocols	DSDV / DSR / AODV
Types of selfish node	Type 1 / Type 2
Percentage of SNs	0 – 50%

3.1 Important Aspects for Evaluation of Network Performance:

These aspects are:

a) Network density: It is the number of nodes per unit area in the MANETs. We take into consideration two categories of network densities: high density (60 nodes in an area of 1000m x 1000m) and low density (20 nodes in an area of 1000 m x 1000 m). It should be noted that density of nodes in a MANET significantly influences the performance of routing protocols inversely. An increased density of nodes in the network would subsequently decrease the performance of the routing protocol, and at the same time, might cause the deleterious effect of selfish nodes to reduce thereby .

b) Network Mobility: We have used two types of mobility scenarios during the simulation. With a high mobility scenario, the nodes move at a maximum speed of 15 m/s, and with a low mobility scenario, the nodes are allowed to move at a maximum speed of 2 m/s within the network. In a high mobility network, the performance of routing protocols is supposed to be degraded.

c) Routing Protocols: One table driven (DSDV) routing protocol and two on-demand (DSR, AODV) routing protocols are used in the simulations.

d) Types of selfish nodes: Both types of selfish nodes (Type-1 and Type-2) are used in the simulations. It should be noted that Type-1 (Active) selfish node is more harmful as compared to Type 2 (passive) selfish node, since it participates in route discovery and maintenance, but not in forwarding the packets

e) Percentage of selfish nodes: The number of selfish nodes is set between 0% and 50%, the rest of the nodes being well-behaved. It is quite obvious that the network will suffer more, if more number of well behaved nodes is compromised to selfish nodes.

3.2 Performance Metrics :

The following metrics are taken into consideration for evaluation of performance of three routing protocols mentioned above.

a) Normalized throughput: This is the ratio of packets received by the CBR sink to the number of packets sent by the CBR source, at the application level. Often this ratio may be found to be less than 1, as some packets may be lost due to link failures, congestion and so on.

b) Average packet delay: The average delay is calculated for the packets, which are received by the destination. Obviously, the lost packets have an infinite delay.

c) Routing overhead: It represents the total number of routing packets transmitted at the network layer during the simulations. A packet traversing multiple hops is subject to multiple transmissions, i.e. one transmission for each hop.

d) Normalized routing load: It is the ratio of the total number of packets transmitted at the network layer to the total number of CBR packets received by the destination at the application layer.

A Proper evaluation of the routing protocols could be achieved with these metrics. The completeness and correctness of the routing protocol can be established by normalized throughput. Efficiency of the protocol to correctly deliver a packet and average network congestion can be obtained from average packet delay. A measure of scalability of the routing protocol and its power consumption efficiency can be determined by the routing overhead. Finally, normalized routing load determines the average number of hops between the source and the destination and the efficiency too.

4. Results and Discussions

Simulation results of ad hoc network with low node density are demonstrated and analyzed. The results for normalized throughput, average delay, routing overhead and normalized routing load of network with low node density are depicted in Figures 1, 2, 3 and 4 respectively. Both types of node mobility (high & low) and both types of selfish nodes (Type1 and Type 2) are incorporated in the simulations. It can be observed that DSR and AODV demonstrate degraded performance under both types of selfish nodes, whereas DSDV shows comparatively more robustness, although its performance is degraded too.

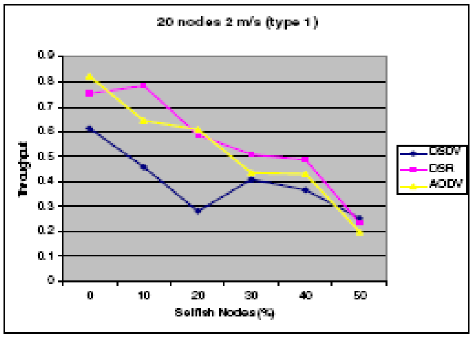

Fig. 1.a : Throughput for low mobility, type 1

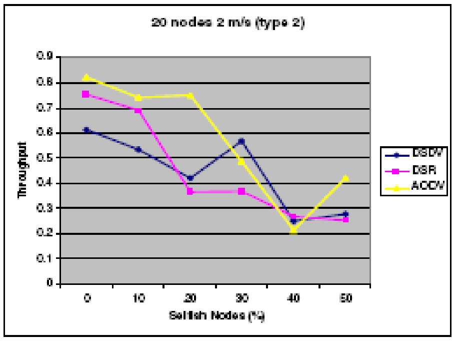

Fig. 1.b : Throughput for low mobility, type 2

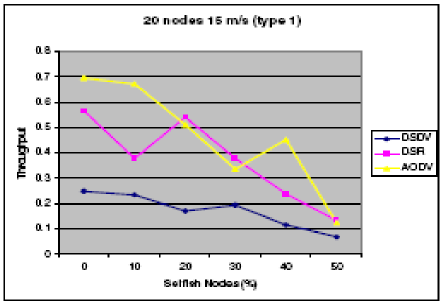

Fig. 1.c : Throughput for high mobility, type 1

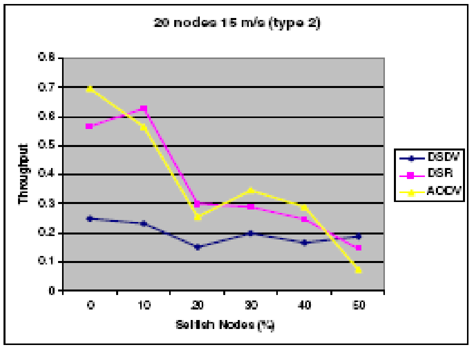

Fig. 1.d : Throughput for high mobility, type 2

4.1 Normalized Throughput :

Normalized throughput of DSDV, DSR and AODV are presented in Fig. 1, with low node density, low/high node mobility, and with increasing percentage of Type 1 and Type 2 selfish nodes in the network. In the absence of selfish nodes in a low mobility network, DSR and AODV maintain higher throughput being able to deliver 80% of the offered load as compared to that of DSDV, which delivers only 60% of the offered load. (Fig. 1a and 1b). As the percentage of selfish nodes increases, throughput of all three protocols degrades. However, in a high mobility network, the impact of selfish nodes on throughput of DSDV is not significant (10% to 30% of normalized throughput) (Fig. 1c and 1d), whereas the normalized throughput of DSR and AODV drops significantly (10% to 60% for DSR and 10% to 70% for AODV). The reason for such a degradation of performance is that the selfish nodes do not cooperate like the well behaved nodes do. Active (Type 1) selfish nodes do not forward the received packets, whereas the passive (Type 2) nodes do not participate in any routing activity. This results in reduction in packet delivery ratio and degradation of the performance of the ad hoc network as a whole.

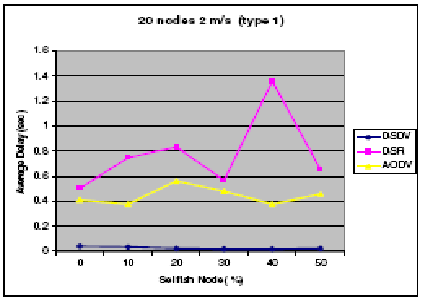

Fig. 2.a : Average delay for low mobility, Type 1

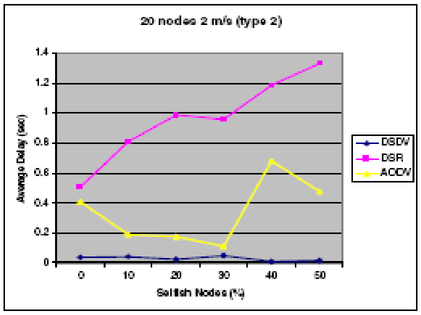

Fig. 2.b: Average delay for low mobility,Type-2

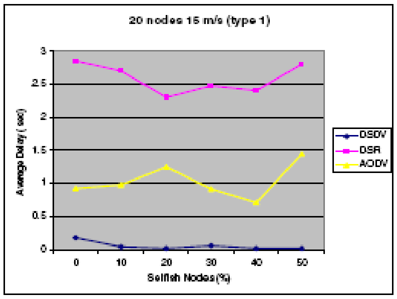

Fig. 2.c : Average delay for high mobility, Type 1

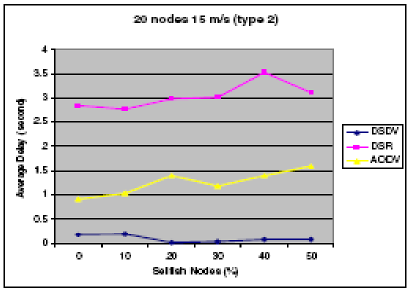

Fig. 2.d: Average delay for high mobility,Type-2

4.2 Average Packet Delay :

In a low mobility ad hoc network with low/high mobility of nodes, the average packet delay in DSR, AODV and DSDV with increasing percentage of selfish nodes (both Type 1 and Type 2) is depicted in Fig.-2. It can be noticed that the impact of the selfish nodes on packet delay for all three protocols is not significant. However, under low mobility, with increasing percentage of passive (Type 2) selfish nodes, packet delay in DSR increases significantly (Fig. 2a, 2b) and the same occurs in AODV under high node mobility (Fig. 2c & 2d).

As a whole, it can be observed that DSR has the higher packet delay among all three routing protocols, and DSDV has the lowest packet delay with or without the selfish nodes. The reason for this is that DSR involves additional latency for route discovery phase and during link breakages, whereas DSDV permanently maintains routes to all possible destinations and does not require a route discovery phase.

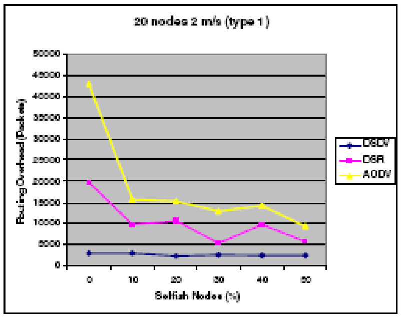

Fig. 3.a : Routing overhead for low mobility, Type 1

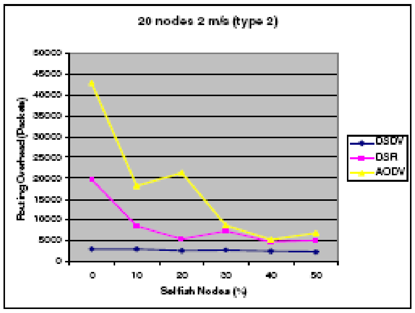

Fig. 3.b: Routing overhead for low mobility,Type-2

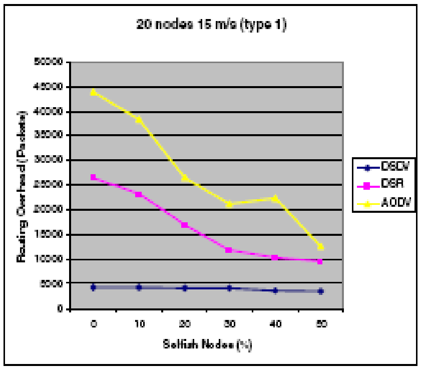

Fig. 3.c : Routing overhead for high mobility, Type 1

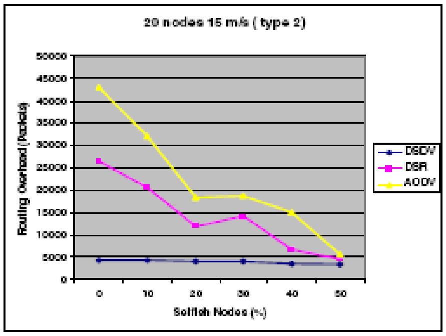

Fig. 3.d: Routing overhead for high mobility,Type-2

4.3. Routing Overhead:

Routing overhead with low node density ad hoc network under low/high node mobility for routing protocols, DSDV, DSR and AODV protocols with increasing percentage of selfish nodes are shown in Fig. 3. In low mobility scenario, routing overhead for AODV decreases convincingly from 45000 packets (with no selfish nodes) to 1500 packets (with 10% selfish nodes) (Fig. 3a and 3b), and then decreases less significantly when the percentage of selfish nodes increases further. The same trend is observed in case of DSR, obviously both DSR and AODV being on-demand routing protocols. As the normalized throughput of DSR and AODV gets severely affected by the selfish nodes (Fig. 1), more packets are dropped and thus, the routing overhead becomes less. On the other hand, the routing overhead in DSDV remains almost constant, irrespective of whether the selfish nodes are present or not, since DSDV is a table-driven routing protocol and hence, it has a relatively stable routing overhead (Fig. 1).

In a high mobility scenario, the routing overhead of DSR and AODV decreases with increasing percentage of selfish nodes in the network, but that of DSDV remains almost unaffected.

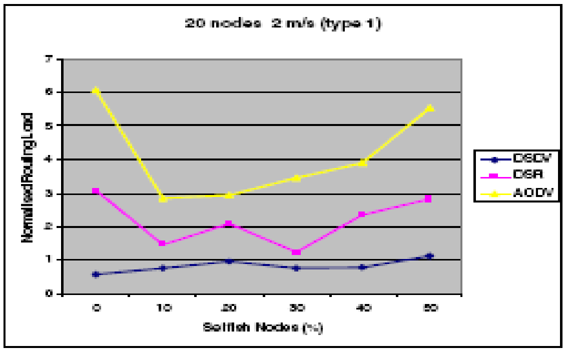

Fig. 4.a: Normalized routing load for low mobility, Type1

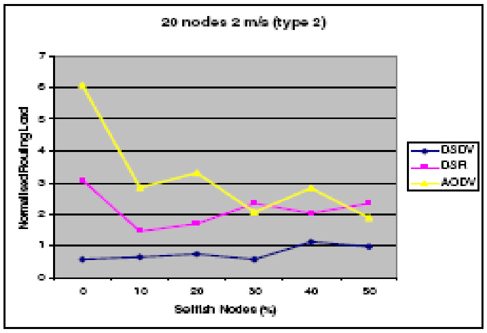

Fig. 4.b:Normalized routing load for low mobility1, Type2

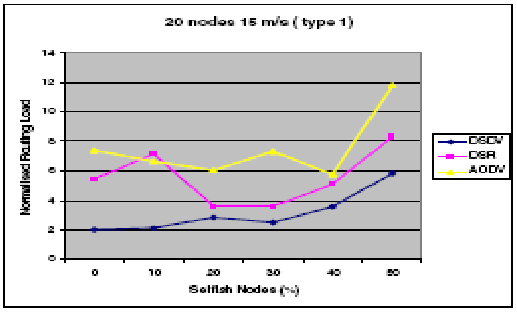

Fig. 4.c :Normalized routing load for high mobility, Type1

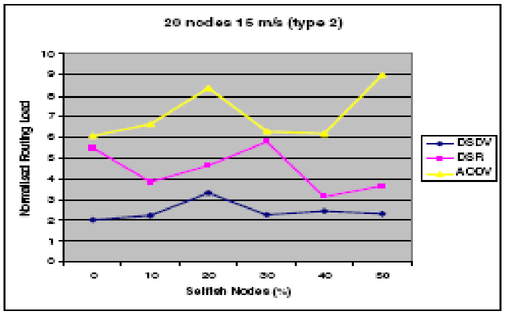

Fig. 4.d : Normalized routing load for high mobility, Type2

4.3 Normalized Routing Load:

The normalized routing load under low node density and low/high mobility for DSDV, DSR and AODV with increasing percentage of selfish nodes are shown in Fig. 4. Unlike the previous scenarios, no constant trend can be observed from AODV. With low mobility and in presence of active (Type-1) selfish nodes, the normalized routing load increases with increase in percentage of such nodes in the network (Fig. 4a). However, this trend does not hold for passive (Types) selfish nodes (Fig. 4b). With high mobility, the normalized routing load remains unaffected in the presence of both types of selfish nodes (Fig. 4 c and 4 d). No obvious trend is observed for DSR in either case. But, in case of DSDV, the normalized routing load increases slightly with the increase of selfish nodes in the network (Fig. 4a, 4b, 4c and 4d). It shows that a packet needs to travel more hops to reach the destination, when more nodes are compromised.

5. Conclusion and Future Work

In this paper, performance of three ad hoc routing protocols DSR, AODV, DSDV are compared under security attack. The performance parameters taken into consideration are normalized throughput, average packet delay, routing overhead and normalized routing load, in the presence of selfish nodes in the network. It could be concluded from the simulation results that DSDV is identified to be more robust under security attack as compared to DSR and AODV in terms of all performance parameters. Thus, a table-driven routing protocol has the potential to maintain the robustness in the presence of misbehaving nodes in the network. In future, we intend to carry out the same comparison over a wide range of routing protocols, thereby devising methods of detection of selfish nodes in ad hoc networks.

References

[1] H. Li and M. Singhal. A secure routing protocol for wireless ad hoc networks. In *HICSS'06: Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, page 225.1, Washington, DC, USA, 2006. IEEE Computer Society.

[2] H. Deng, W. Li, and D. P. Agrawal. Routing security wireless ad hoc networks. *IEEE Communications Magazine*, 2(1), 2002.

[3] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. In *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 125–134, New York, NY, USA, 2003. ACM Press.

[4] P. Michiardi and R. Molva. Simulation-based analysis of security exposures in mobile ad hoc networks. In *Proceedings of European Wireless Conference*, 2002.

[5] K. Paul and D. Westhoff. Context aware detection of selfish nodes in DSR based ad-hoc networks. In *IEEE GLOBECOM 2002, Taipei, Taiwan*, November 2002.

[6] P. Papadimitratos and Z. J. Haas. Securing routing for mobile ad hoc networks. In *Proceedings SCS (CNDS2002)*, 2002.

[7] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM'94*, pages 234–244, London, England, August 1994.

[8] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In *IEEE WMCSA'99*, pages 90–100, New Orleans, 1999.

[9] D. B. Johnson. Routing in ad hoc networks of mobile hosts. In *IEEE Workshop on Mobile Computing Systems and Applications*, pages 158–163, December 1994.

[10] J. Broch, D. A.Maltz, D. B. Johnson, Y. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 85–97, New York, NY, USA, 1998. ACM Press.