International Journal of Wireless Networks and Communications.
ISSN 0975-6507 Volume 4, Number 2 (2012), pp. 83-93

http://www.irphouse.com

Efficient Monitoring of Intrusion Detection in Mobile Ad-Hoc Network using Monitoring based Approach

Pebam Binodini and S. Madhan Kumar

M.E. (Computer Science), ME, Asst.Professor,
Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai
E-mail: tambipebam@gmail.com, madhan866@gmail.com

Abstract

It is well known that Mobile Ad Hoc Networks (MANETs) are susceptible to numerous attacks. Communication is done in the absence of fixed infrastructure by seeking the help of the intermediate nodes. In such, malicious intermediate nodes can be a threat to the security of conversation between the mobile nodes. Security schemes have been proposed that depend on cooperation among the nodes that are exhibiting malicious behavior such as packet dropping. This false positive cannot be observed in popular ad-hoc network simulator such as ns2, OPNET or Glomosim. The proposed sliding window is therefore simple and improves both communications and security performance and also results in significant improvement in total packet delivery.

Index Terms: Mobile ad hoc networks, Intrusion Detection, Passive Monitoring, False positives, Noise Modeling, Performance Analysis

INTRODUCTION

MANET has become an exciting and important technology in recent years because of the rapid increase in wireless devices. It is a collection of mobile nodes and nodes can move randomly in any directions. Since MANETs can be set up easily and inexpensively, they have a wide range of applications, especially in military operations and emergency and disaster relief camps. Communication is done in the absence of fixed infrastructure by seeking the help of intermediate nodes. In such network, malicious intermediate nodes can be a threat to the security of conversation between the mobile nodes. Intrusion detection systems (IDSs), which attempt to detect and mitigate an attack, are very important to MANET security. In a monitoring-based IDT, some or all nodes monitor transmission activities of other

nodes and/or analyze packet contents to detect and mitigate active attackers. Intuitively, it is easy to see that monitoring based intrusion detection is not likely to be accurate for ad hoc networks due to varying noise levels and varying signal propagation characteristics in different directions. An IDT uses additional mechanisms such as trust values for nodes before considering nodes to be suspicious. The paper, quantify false positives and analyze their impact on the accuracy of monitoring-based intrusion detection. A combination of experimental, analytical, and simulation analyses for the purpose is used. First, using a linear chain of three off-the-shelf wireless routers, a sender of data packets falsely suspects, based on the monitoring of transmission activities is shown in its radio range, its next hop of not forwarding its packets (though 98 per cent of its packets are delivered to its destination). The experimental results is validated by deriving a Markov chain to model monitoring and estimate the average time it takes for a sender to suspect its next hop. Sliding window is used to keep track of monitoring.

The paper is organized as follows. The related works in this field are discussed in Section 2.Section 3 provides an overview on the three node configuration test-bed experiment. The analytical model is depicted in section 4. Section 5 provides an overview of the architercture. From section 6 we can know about analyzing the forwarding behavior. Section 7 provides the simulation of MANET. Finally, the conclusion is provided in Section 8.

RELATED WORK

Several security schemes have been proposed that depend on cooperation among the nodes and also several IDTs for MANET have been proposed in literature. The IDTs have been classified as: signature-based detection, anomaly detection, and specification-based detection. IDTs for MANETs can be divided into three approaches: monitoring-based, probing-based, or explicit feedback among intermediate nodes in routes. The first monitoring based technique proposed for ad-hoc are Watchdog and pathrater. In this, approach, nodes monitor transmission activities of neighboring nodes and analyze packet contents to detect and mitigate an attack after it is started. When a node starts suspecting its next hop, it will send an alarm message back to source node. Pathrater is used to punish suspicious nodes by not including them in routing. However, monitoring-based intrusion detection is not likely to be accurate for ad hoc networks due to varying noise levels, varying signal propagation characteristics in different directions, and interference due to competing transmissions within the network.

In this paper, we showed monitoring gives very high false positives when environmental noise effects are considered. We tried to complement the existing results by quantifying the benefits and overheads of watchdog in more realistic noise conditions. The Watchdog technique has been extensively studied for its deficiency, false positives and has been modified or supplemented it with other mechanisms to make it more accurate. Specific results include CONFIDANT CORE, and LARS .These results use different policies to propagate monitored information (trust) to others in order to mitigate misbehavior and enforce cooperation.

In particular, Buchegger and Le Boudec present a Bayesian approach to assign trust and reputation ratings the CONFIDANT system. Their simulation results show that incorporating secondary trust information gathered from other nodes with the primary trust information directly gathered (by monitoring) can significantly speed up the detection of misbehaved nodes. The effectiveness of these approaches needs to be carefully evaluated with more realistic noise simulation models or experiments.

There are several other papers on using a reputation/trust system for MANETs. Luo et al. describe a localized trust model in which multiple nodes are collaboratively used to provide authentication services. Eschenauer et al. describe a trust framework which encompasses Pretty Good Privacy (PGP) like trust models. Liu et al. present a dynamic trust model to address packet drops by selfish and malicious nodes. In general, a trust system requires propagation and dissemination of trust. Also trust evidence must be distributed redundantly to handle the unreliable connectivity in MANETs . Trust propagation is complex, not well understood in the context of ad hoc networks, in which trust collection and dissemination may be incomplete and problematic and has high computational requirements (e.g., collaborative authentication) and communication overhead (requiring localized or limited distance network floods .

This paper intends to find effective features in detecting intrusions in MANET. None of the above works present a method to measure effectiveness of the features and a way tofind and select them.

THREE NODE CONFIGURATION TESTBED EXPERIMENT

This is the testbed experiment for three node configuration. Here each node monitors the forwarding behavior of its neighboring node. But, in most cases, a node only monitors its next hop in a route. The three nodes are denoted as node 1(source or the node closer to the source), node 2 and node 3(destination or the node closer to the destination), then node 2 is the next hop of node 1 and 3 is the next hop of node2. When node 1 transmits a data packet to node 2, it expects to hear node 2's transmission of this packet to node 3 within some specified amount of time. If the fraction of packets not overheard by node 1 exceeds a specified threshold, then node 1 concludes that node 2 is dropping too many data packets and suspects it to be a malicious node. For monitoring purposes, node 1keeps track of a window of packets that it sent recently to its next hop. Two types of windows can be used to keep track of monitoring: fixed window or sliding window. Let W be the monitoring window size. Also, assume that each packet is given a sequence number, starting at 1. Let j be the sequence number of the most recent packet sent to the next hop. With fixed window monitoring, packets numbered are monitored. The size of the monitoring window varies from 1 to W. With sliding window, packets j –W+1,…,j for j>W or 1,….,j, for j<=W, are monitored A detection scenario with a threshold of T is considered; so if L =⌈WT packets are not overhead within the current window, then the next hop is suspected. To understand the similarities and differences between the fixed and sliding windows, let us assume that noise does not impact the overhearing of transmissions within a node's radio range. In such a scenario, a malicious node can

drop up to L - 1 packets out of W on the average without risking suspicion by neighbors. However, the temporary drop rates can be different. For example, a malicious node can drop as many as L - 1 packets at the end of one window and another L - 1 at the beginning of the next window and still not be suspected when fixed windows are used for monitoring. The sliding window approach is free of this deficiency since in any consecutive W transmitted packets, a malicious node may drop at most L-1 packets without risking suspicion by neighbors. Therefore, with the fixed windows approach, a malicious node can afford to drop packets at a faster rate, at times. While in the case of sliding window it results in significant improvement in total packet delivery.

EXPERIMENTAL REQUIREMENTS FOR TESTBED

It requires a processor with Pentium III 500Mhz, RAM of 512MB and above, hard Disk of 40GB and above. The software required is open wrt Linux but this experiment is done using cygwin software to provide the environment of linux and to test the software. The simulator used for implementation is Network Simulator version 2. The language in which the experiment is done is TCL(Tool command language)

ANALYTICAL MODEL

Analytical model to validated in this section. Let ti, ri,and oi denote, respectively, the number of packets transmitted by node i, number of packets received by node i and number of packets by node i, for I = 1, 2, 3. It is clear that r1 = o2 = t3 = o3 = 0 for the three-node setup used in the experiments. If node 2 is not malicious and no packets are lost due to congestion then r2=t2.The overall not-overheard rate is calculated due to environmental noise, denoted q, as follows:

$$q = \frac{r_2 - o_1}{r_2}$$

$p_{i,i+1}$=

$$P\{\textit{The oldest packet in current window is not overheared} \cap \textit{The newest packet in next window is overheard} \mid \textit{current state= si}] = \frac{i}{W}(1-q)$$

$p_{i,i+1}$=

$$P\{\textit{The oldest packet in current window is overheared} \cap \textit{The newest packet in next window is not overheard current state= si}] = (1-\frac{i}{W})$$

SLIDING WINDOW PROTOCOL

In this paper we have proposed a sliding window mechanism for group multi-communications. The proposed scheme improves both routing performance and increases the security of the ad hoc network, particularly at high node mobility. This is significant due to the increasing difficulty in reliable packet delivery and secure communications as mobility increases.

This model uses a discrete-time Markov chain. More specifically, it uses the number of not-overheard packets in the monitoring window as the state of the monitoring by node 1. Fig.1 shows how sliding window works. The window slides to the right with each packet received by node 2. Therefore, packet receptions of node 2 are the time steps in the Markov chain. The purpose of the Markov model is to determine analytically the expected time to suspect its next hop by a monitoring node.

The discrete-time Markov chain has L+1 states, where $\frac{L-1}{W} < T \leq \frac{L}{W}$, The state i, denoted as si,indicates the case where i packets in the current window are not overheard by node 1. State s0 denotes the state where all of the W packets in the current window are overheard. State sL indicates the state where L of the most recent W packets is not overheard, which means the fraction of not-overheard packets is beyond the threshold to suspect the monitored node. The purpose of the Markov model is to determine analytically the expected time to suspect its next hop by a monitoring node. Therefore, sL is an absorbing state. Such Markov models are commonly used to analyze the expected time to encounter a bug in a software system.

Each request contains the following information: the Initiator of the request, the destinations, the time-to-live parameter and a unique request id. Each route request also contains a record listing the address of each intermediate node through which this particular copy of the route request has been forwarded. A inner is started when a route request is transmitted. If a timeout occurs before a route reply is returned, the route discovery for the affected nodes is retransmitted (see below) as an example, routes are requested for destinations c, f and k. The sliding window will have three entries, c, f and k the request is broadcast.

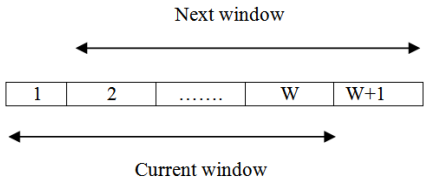

Figure 1: Sliding window

Assume that one path in the network contains nodes a,b,c,d,e,f,g. When a node receives this route request, it checks if it is a target of the route discovery. If it is not (such as node b), it decrements the time-to-live value. It next checks the time-to-live value and if it is greater than 0, the request is forwarded. If the node is a target of the Route request (such as node c), it sets the flag for node c in the route request packet,

decrements the time-to-live value and forwards the request, if the value is greater than 0. The request is not forwarded if the time-to-live is 0 or if all the destination nodes flags have been set in the route request or if a route request with the same id had been received earlier by the node. If a route request is not forwarded, a "Route Reply" is returned to the initiator of the Route Discovery, giving a copy of the accumulated route record from the Route Request; when the initiator receives this Route Reply, it processes the route record and caches the routes in its Route Caches for use in sending subsequent packets to the destinations. The route A,B,C will be cached for destination C and A,B,C,D,E,F for destination F. The sliding window at the origin will remove C and F, leaving K in the window. As in the DSR protocol, in order to reduce the overhead from Route Discoveries for nodes which may not be reachable, a node should use an exponential back-off algorithm to limit the rate at which it initiates new Route Discoveries for the same target.

ARCHITECTURE

The following is the architecture proposed in this paper:

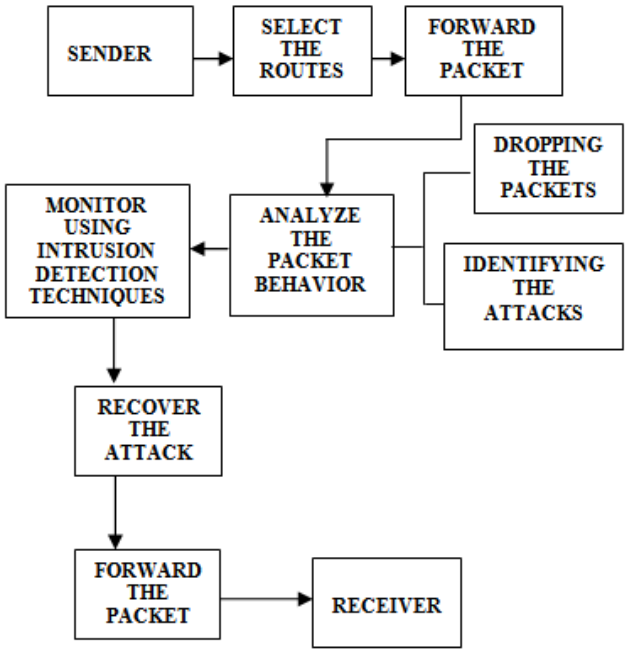

Figure 2: Proposed architecture

First, the sender which is the source node will select the best route, i.e. the shortest route (from source to destination) from the routes it receives from its neighbors. Fig2 shows the proposed architecture. Then, it will start forwarding the packets through this route. While doing so the neighboring nodes will start monitoring the nodes by analyzing its behavior. Here, nodes send package through intermediate nodes so if any

intermediate nodes tends to misbehave (packet dropping), then it will identify and try to mitigate the attack using the intrusion detection technique implemented. After recovering the attack it will forward the packet to its receiver.

ANALYZING THE FORWARDING BEHAVIOR

Nodes send out a ROUTE REQUEST message, all nodes that receive this message forward it to their neighbors and put themselves into the source route unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or gratuitous. After receiving one or several routes, the source picks the best (by default the shortest), stores it, and sends messages along that path. In case of a link failure, the node that cannot forward the packet to the next node sends an error message toward the source. One end router (denoted as node 1) sends packets to the other end router (node 3) via the intermediate router (node 2). This use static route in node 1 and node 2 to ensure that the next hop for packets transmitting from node 1 is node 2 and the next hop for packets transmitting from node 2 is node 3. RTS/CTS handshake is used to reduce frame collisions due to the hidden terminal problem. Node 1 is set to promiscuous mode and monitors (overhears) transmissions from node 2 to node 3. A single CBR over UDP connection is used. Even though the overall packet delivery ratio is about 98 percent, node 1 suspects node 2 within a short period of time. Pre-processed packet traces is used to compute the percentage of packets received by node 2, but not overheard by node 1. If l is the number of packets in the monitoring window that is not overheard, then is the fraction of successfully transmitted packets, but not overheard for the current window. The following is the graph showing the time to suspect next hop in monitoring-based approach in a three-node wireless test bed. W=100 which corresponds to a three second interval for the packet rates used.

SIMULATION OF MANET

We use network simulator ns-2, version 2.30 to evaluate the effectiveness of monitoring in larger mobile ad-hoc networks using a standard noise model. The actual not-overheard rate is higher due to interference from competing transmission in an ad-hoc network . Each node maintains a monitoring window for each traffic flow connection through it. In each traffic flow, each data packet sent from the source node is assigned an increasing ID. Only when current node overhears next node forwarding packets j, it will consider packets with ID between I and j as not overheard , where I is ID of the last overheard packet and i<j. Therefore, it can avoid false positives due to random back offs at the MAC layer.

Watchdog intrusion detection technique is implemented as a representative of monitoring based intrusion detection technique. Implementation has three

components: watchdog, pathrater and sending extra route request message when all the routes in the network contains one or more suspicious node. In the watchdog component, each node that sends or forwards data packets monitors its next hop. When a node suspects its next hop, it will sends an ALARM message to the source node if the node suspected is not the source node. When a route break occurs, the monitoring windows in the broken route path are cleared. Nodes that are not suspected are given a small positive value less than 1as their initial rating, which is increased gradually with passage of time. When the source node of a route receives an alarm message, it will assign a rating of -100 to the suspected node. The rating of a path is the average of the ratings of the nodes on the path. The source chooses the highest rated path if there are multiple positive paths to the same destination. If all paths to its destination have negative ratings, then a new route discovery is initiated (the second component of the IDT) to find a path with positive rating. Although WD is a simple IDT, its primary element— monitoring—may be used as the key step to initiate the detection process in more elaborate IDSs. We used only sliding window monitors in our simulations. the results for the sliding window is presented. The simulation parameters are listed in Fig.3. The number of nodes used is 25.Inorder to avoid packet losses due to congestion, we only used 100 kbps traffic load. We use the following performance metrics to evaluate the effectiveness of monitoring.

Number of nodes suspected: The total number of nodes suspected by one or more nodes in the network.

Total false positives: The total number of times that normal nodes are suspected.

No of nodes	25
Node speed	[1-15]m/s
Pause Time	0
Warm up time	100s
Total simulation time	1600s
	400s
Attack time	250m
Radio Range	6
No of traffic pairs	100kbps
Traffic Load	AODV
Routing Protocol	500bytes
Data packet payload	2Mbps
Link Bandwidth	
Monitoring:	
Threshold	10%
Window size	100
Window type	Sliding Window

Figure 3: Simulation table

MONITORING BASED INTRUSION DETECTION TECHNIQUE

The project quantifies false positives and analyzes their impact on the accuracy of monitoring based intrusion detection. This use a combination of experimental, analytical and simulation analysis for this purpose. This validate the experimental results by deriving a Markov chain to model monitoring and estimate the average time it takes for a sender to suspect its next hop. The results indicate that monitoring-based intrusion detection has very high false positives, which impact its capability to mitigate the effect of attacks in networks with attackers. In monitoring-based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes. In most cases, a node only monitors its next hop in a route.

Two types of windows can be used to keep track of monitoring: fixed window or sliding window. But since, sliding window can give the exact reason of packet dropping we use sliding window in our project. One end router (denoted as node 1) sends packets to the other end router (node 3) via the intermediate router (node 2). It use static routes in node 1 and node 2 to ensure that the next hop for packets transmitting from node 1 is node 2 and the next hop for packets transmitting from node 2 is node 3. RTS/CTS handshake is used to reduce frame collisions due to the hidden terminal problem. Node 1 is set to promiscuous mode and monitors (overhears) transmissions from node 2 to node 3. In each experiment, node 1 transmits at a rate of 200 Kbps (fifty 500 byte packets /s) for up to 80 seconds. A single CBR over UDP connection is used. Node 2 transmits every packet it receives from node 1 to node 3.

Every node records the ID of each packet it receives, transmits, or overhears. The packet trace from each router is sent to a desktop machine via the Ethernet connection of the routers. After the experiment, then analyzed the packet traces obtained from the three nodes. It removes the traces for the first 500 packets, which were considered to be part of the network warm-up.

With the MAC level ACK mechanism in the 802.11 protocol, node 1 can determine if a packet it transmitted is received successfully by node 2.

Therefore it considers only the packets that were successfully received by node 2 in our analysis of false positives. The three-node testbed is small, nodes are stationary, and only one connection between the end nodes with static routes is used to eliminate routing overhead and contention among the test nodes. Since there is only one active connection, there is no interference noise from other node transmissions within the network. If monitoring is not effective in a three-node network, it likely to be even less effective in a larger MANET where there is interference due to transmissions by other nodes which adds to the background noise.

Inorder to understand the monitoring based intrusion detection technique, lets consider an example of cluster consisting 4 nodes label as node 1, node2, node3 and node4. In each node IDS is installed. It works in the following four steps:1view formation 2. Local View exchange 3. Local view update 4. Global view. Each node has an inbuilt IDS. Lets consider node 1 as the source node and node 3 as the destination. Node 2 sends packet to node 3 through the intermediate node 2. If node 2 tends to misbehave by dropping packets and not forwarding to the destination. In this, the neighboring node will start suspecting node 2 and a view will be formed that node

2 is malicious. The neighboring node will start exchanging local view that node 2 is malicious and care should be taken in forwarding the packets through this intermediate node 2. After this the neighboring node will update its routing table and a global view will be formed that the packets should not be forwarded through the node 2 and should be discarded from the cluster.

Given that monitoring is imperfect and environmental noise could increase false positives, it is surprising that none of the published results on monitoring-based intrusion detection techniques analyzed the impact of noise. Also, to the best of our knowledge, there are no extensive evaluations of monitoring techniques using testbeds (with 10 seconds of nodes), and most large network evaluations were done using simulations.

FALSE POSITIVES IN NORMAL MOBILE AD HOC NETWORKS

When sliding window noise model is used, nodes are suspected much faster and more false positives occur.

If the simulation is run for long enough time, all nodes in the network will be suspected. Even when default constant background noise is used, there are many false positives due to interference noise from competing transmissions. It is interesting to note that false positives are higher in low-density networks than in high-density networks though the interference noise is likely to be less in the former networks. The reason is, in low-density networks, the hop distances are larger and signals overheard during monitoring are weaker correspondingly. Also, since there are more hops in each route in the low-density network, there are more chances that nodes will be suspected. Although fewer false positives occur when the threshold is higher (e.g., 15 per cent), malicious nodes can take advantage of it and drop more packets without being detected. Therefore, in the remaining his paper, 10 per cent as the detection threshold is chosen.

IMPACT OF INTRUSION DETECTION TECHNIQUE ON NORMAL ATTACKS

Too many false positives occurred when monitoring is used in normal mobile ad hoc networks, especially when the background noise is simulated. However, it is not clear if the false positives have any impact on the network performance: since there may be multiple paths between a source and its destination, when a node is suspected, an alternate path that does not involve the node may be used without any loss of performance. Therefore, in this set of simulations, the overall network throughput is used as the performance metric. the network throughput is measured with and without noise model. Then, turned on the Watchdog IDT (explained above), reran the same configurations and measured the network throughput. In a high-density network, WD does not affect the network throughput significantly since sources can find alternate paths to get around the false positives. But in low-density networks, due to very high

false positives and due to relatively fewer alternate paths, WD hurts the network performance, especially when noise model is used.

CONCLUSION

The monitoring based intrusion detection technique we have evaluated is a simple one .The paper presented quantitative evaluation of false positive in monitoring based intrusion detection for ad hoc networks. We can also see that the three node configuration also suffers from high false positive. The experiment is validated by using a Markov chain model. We can also reduce the dropping of packets by not allowing the malicious node to participate in forwarding of packets. In future we would like to develop new IDT that avoids the problem of passive monitoring.

REFERENCES

[1] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Research Report cs. NI/0307012, Standford Univ., 2003.

[2] R.V. Boppana and S. Desilva, "Evaluation of a Stastical Technique to Mitigate Malicious Control Packets in Ad Hoc Networks," Proc. Int'l Symp.

[3] R.V. Boppana and X. Su, "An Analysis of Monitoring Based Intrusion Detection for Ad Hoc Networks," Proc. IEEE Globecom: Computer and Comm. Network Security Symp., Dec. 2008.

[4] S. Buchegger, C. Tissieres, and J.Y. Le Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-Hoc Networks – How Much Can Watchdogs Really Do?" Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA '04), 2004.

[5] R. Burchfield, E. Nourbakhsh, J. Dix, K. Sahu, S. Venkatesan, and R. Prakash, "RF in the Jungle: Effect of Environment Assumptions on Wireless Experiment Repeatability.

[6] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An Acknowledgement Based Approach for Detection of Routing Misbehavior in Manets," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 488-502, May 2007.

[7] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 488-502, May 2007.

[8] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-Securing Ad Hoc Wireless Networks," Proc. Seventh IEEE Symp. Computers and Comm. (ISCC '02), 2002.

[9] X. Su and R.V. Boppana, "Crosscheck Mechanism to Identify Malicious Nodes in Ad Hoc Networks," Security and Comm. Networks, vol. 2, no. 1, pp. 45-54, 2009.

[10] W. Yu, Y. Sun, and K.J.R. Liu, "HADOF: Defense against Routing Disruption in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.