A Study of Deploying Intrusion Detection Systems in Mobile Ad Hoc Networks

Ming-Yang Su

***Abstract*—This paper presents an approach to prevent attacks in MANETs by deploying intrusion detection nodes. Some nodes performing Intrusion Detection Systems, IDS nodes for short, are used to mitigate attacks. Two kinds of attacks, wormhole attacks and black hole attacks are addressed in the paper. The modules used to mitigate wormhole and black hole attacks are called AntiWorm and AntiBlackhole, respectively, in this paper. The IDS nodes are set in sniffing mode in order to estimate the suspicious value of a node within the communication range, according to the routing messages transmitted by the node. When the suspicious value of a node exceeds a threshold, an IDS nearby will broadcast a block message to inform all nodes on the network, asking them to cooperatively isolate the malicious node. Experimental results by ns-2 show that the IDS nodes can successfully identify and block the malicious nodes.**

***Index Terms*—Mobile ad hoc networks(MANETs), Intrusion Detection System(IDS), wormhole attacks, black hole attacks, AntiWorm, AntiBlackhole, ns-2**

I. Introduction

The authors in [1] and [2] proposed methods to mitigate the wormhole and black hole attacks, respectively. Since their algorithms have huge difference and thus put them into an IDS node is impossible, in this study we try to do some modifications on their methods to shorten the gap. Our ultimate goal is to design an IDS system that can detect both attacks, not only one of them. The description about the wormhole and black hole attacks are briefly introduced below. Wormhole attacks are two malicious nodes work cooperatively at distinct positions; one transmits the routing message to the other through a secret tunnel. Thus these two malicious nodes appear to be adjacent to each other and the hop count passing the malicious nodes will be shorter than that passing the normal nodes. The malicious nodes increase the chances of grabbing the route for data transmission, thereby eavesdropping or dropping the data packets passing the malicious nodes. The secret tunnel in wormhole attacks can be represented by a packet encapsulated channel, as shown in Figs. 1. In Figure 1, a route is created between *w*1 and *w*2, and node *s* is the source and the node *d* is the destination. When RREQ (Route Request) is initiated and broadcast by *s* and received by *w*1; *w*1 will encapsulate it in a data packet and transmit it via the route between *w*1 and *w*2. As a result, normal nodes *a*, *b*, and *c* will help *w*1 to transmit the encapsulated data packet to *w*2. After the packet is received by *w*2, the packet is unpacked and then the original RREQ is broadcast to destination *d*. Destination *d* will receive three RREQs from different routes, i.e. *s*-*w*1-*w*2-*d*, *s*-*e*-*f*-*g*-*d* and *s*-*h*-*i*-*j*-*k*-*l*-*d*, respectively; the hop count is 3, 4, and 6, respectively. So destination node *d* will choose to send an RREP (Route Reply) in response to *w*2 because this path is the shortest. Hence, the wormhole nodes can grab the route to bypass the subsequent data packets.

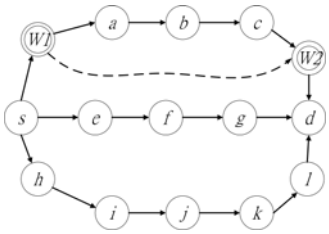
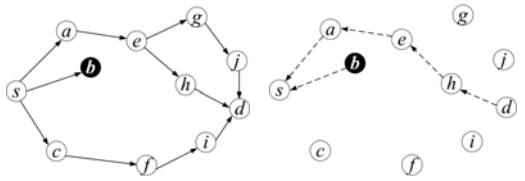


Figure1: Illustration of wormhole attack

On the other hand, a black hole attack can be done by just one node which forges the sequence number and hop count of a routing message in order to forcibly grab the route. Figure 2 shows a black hole attack, where nodes *s* and *d* are the source node and destination node, respectively. By AODV [3] routing protocol, node *s* would broadcast a Route Request (RREQ) packet to search for destination node *d*; the normal intermediate nodes would receive and continuously broadcast the RREQ, rather than the black hole node. As shown in Figure 2(a), the black hole node would directly reply through an RREP with an extremely large sequence number and hop count of 1 to source node *s*. When receiving RREQs from normal nodes, the destination node *d* would also select a route with a minimal hop count, and then, return a Route Reply (RREP) packet, as shown in Figure 2(b). The source node would select the largest sequence number and shortest route to send data packets upon receipt of several RREPs packets. Thus, a route via a black hole node would be selected by node *s*. The black hole node will then eavesdrop, or directly drop the received data packets.



(a) RREQ flooding (b) RREP Replying

Figure2: Illustration of black hole attack

Manuscript received March 13, 2012; revised April 4, 2012. This work was supported in part by the National Science Council, project no. : NSC 99-2628-E-130 -003 and NSC 100-2221-E-130-008.

M. Y. Su is with the Department of Computer Science and Information Engineering, Ming Chuan University, Taoyuan, Taiwan (+886-3-3507001; fax: +886-3-3593874; e-mail: minysu@mail.mcu.edu.tw).

In this paper, Intrusion Detection System nodes, IDS nodes for short, are deployed in MANETs to identify and isolate wormhole/black hole nodes. An IDS node watches every node's routing behavior, in order to judge if any malicious nodes are within its transmission range. Once a malicious node is found, the IDS node sends a Block message through the MANET to isolate the malicious node. The remainder of this paper is organized as follows. Section 2 introduces some related works; Section 3 presents the IDSs for mitigating the wormhole attacks and black hole attacks, respectively; Section 4 shows the experimental results; and conclusions are given in Section 5.

II. Related Works

We first review wormhole papers and then black hole papers in the section. Some wormhole related works are introduced. In [4], the authors proposed a routing algorithm where every node has to keep all neighbors within 2 hops, and assume the Hello message can pass over two hops. When a node transmits the RREQ, it will generate a message authentication code (MAC) for the nodes two hops away. If the adjacent node doesn't increase the hop count, then the nodes two hops away can assure the previous node is a wormhole by checking the MAC. Another purpose of maintaining a 2 hops neighbor list by each node is to help the node recognize if the wormhole node is a hidden wormhole node or an exposed wormhole node [4]. In [5], the authors proposed a routing protocol to alleviate wormhole attacks by modifying the Ariadne [6] routing protocol. The algorithm in [5] can only defend against wormhole attacks in the case of an in-band channel (or packet encapsulated channel). Its main method is to reduce the delay in transmitting RREQ and to calculate the average time in transmitting RREQ by normal nodes. In this way, a normal node can identify a nearby wormhole node that executes in-band wormhole attacks if the RREQ transmitting is particularly long. The authors of [1] presented a method to mitigate wormhole attacks by deploying IDS nodes, but it can't work for mitigating black hole attacks.

In [7], the authors designed a routing algorithm based on OLSR [8] to mitigate the wormhole attacks by using a four message exchange method in route discovery stage. Believing that the wormhole nodes may process a larger number of packets, and may cause longer delays of packet than normal nodes, the authors mainly use Hello messages and ACK messages to confirm the delay. Through exchanging Hello messages, those nodes with an exceptionally long delay would be judged as wormhole nodes. The method proposed in [9] is called TTM (Transmission Time-based Mechanism), which is also based on AODV routing protocol. They based on the assumption if two nodes, subject to wormhole attacks, are misled to be neighbor nodes, the transmission time between the two nodes would be longer than normal neighbor nodes. Khalil et al. proposed two new protocols called LITEWORP [10] and MOBIWORP [11]. Both of these protocols are based on DSR [12] with a few modifications.

As to black hole attacks, the authors in [13] revised the AODV routing protocol to reduce chances for a black hole node to grab routing paths. The source node abandons the first returned RREP, or the first two returned RREPs, but selects any subsequent RREP packets, because RREP replies by a black hole node are generally the first or the second one to arrive at the source node, thus, method [13] is very useful to prevent a black hole node being located nearby a source node. Another AODV-based approach proposed in [14] is that a source node does not immediately send out a data packet upon receipt of the first RREP, but waits in order to collect subsequent RREPs from its neighboring nodes. After comparing all RREPs, the source node selects one (from the neighboring nodes that forward RREPs to the source node), which has the same next hop as other alternative routes (i.e., a node with a distance of 2 from the source node), and begins to send out data packets. The authors of [15] also proposed a revised AODV routing protocol, called PCBHA (Prevention of a Co-operative Black Hole Attack), in order to prevent cooperative black holes. The authors of [16] proposed a dynamic learning method to detect a black hole node. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. The authors of [17] added an authentication mechanism into the AODV routing protocol, by combining hash functions, message authentication codes (MAC), and a pseudo random function (PRF) to prevent black hole attacks. The authors of [18] proposed a routing algorithm based on OLSR (Optimized Link State Routing) [8] to prevent the attack of cooperative black holes, by adding two control packets, namely 3 hop_ACK and HELLO_rep. The authors of [2] presented a method to mitigate black hole attacks by deploying IDS nodes, but it does not work for wormhole attacks.

The motivation of this research is to design an IDS that can mitigate both wormhole and black hole attacks because no one knows what kind of attack would happen in the networks in advance. The approach adopted in this paper is to modify the methods proposed in [1] and [2] to make them compatible in an IDS and eventually merging them into one IDS system.

III. Intrusion Detection Systems for Wormhole Attacks and Black Hole Attacks

Basically we modify the algorithm appeared in [1] and [2] to let them use the same tables to keep routing information needed for both wormhole detection and black hole detection. Once regular nodes and IDS nodes can keep the necessary information for detecting both attacks, the first step to merge the two methods into one system is reached. The two modifications proposed are called AntiWorm and AntiBlackhole in this paper. IDS nodes deployed in this study must estimate the suspicious value of a node according to abnormal transmission of RREQ and RREP messages. That is the common behavior of wormhole attacks and black hole attacks. When the suspicious value of a node exceeds a predefined threshold, neighboring IDS will broadcast the Block message to all nodes in order to cooperatively isolate the suspect node. Regular nodes will add the malicious nodes onto the blacklist after receiving the block messages

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)
(revised on 7 June 2012)

broadcast by IDSs, and then reject all RREPs forwarded by nodes on the blacklist. Therefore, three assumptions are necessary in this paper. Firstly, two neighboring IDS nodes are in the transmission range of each other so as to transmit block messages to each other. Secondly, some authentication mechanisms exist in MANETs so that the identity of each node cannot be falsified and a block message transmitted by an IDS node cannot be modified or falsified. Thirdly, all IDS nodes are set in promiscuous mode to sniff all routing messages within the transmission range.

All of the tables used by both AntiWorm and AntiBlackhole are given in Table 1. Basically RQT is used to keep the RREQ information sniffed by IDS, RPT is used to keep the RREP information sniffed by IDS, and SNT records the suspicious value of nodes. We need two SNTs, i.e., SNT-W and SNT-B, for wormhole attacks and black hole attacks separately because their suspicious values are counted in different ways. The AntiWorm relies on all three tables, however the AntiBlackhole only need RQT and SNT-B.

In this study of wormhole attacks, four types of nodes, i.e., wormhole nodes, tunnel nodes, regular nodes, and IDS nodes, are running different algorithms. Wormhole node executes a WAODV (Wormhole AODV) routing algorithm to behave like wormhole attacks. Tunnel node runs a TAODV (Tunnel AODV) routing algorithm and cooperates with a wormhole node to quickly transmit RREQ and RREP messages to the colluded wormhole node, without increasing the hop count in RREQ. Regular node executes a slightly modified AODV, which is called MAODV (modified AODV), to perform normal routing and cooperate with IDS nodes to block wormhole nodes if necessary. Finally, IDS node executes the AntiWorm algorithm to detect wormhole nodes and broadcast corresponding block messages.

The algorithm of AntiWorm executed on IDS nodes is described below. AntiWorm relies on three tables including the RQT, RPT, and SNT-W, as shown in Table 1. The RQT records RREQs sniffed by an IDS node within its transmission range; for instance, the first row of Table 1(a) indicates the RREQ of (source, destination, source_sequence) = (2, 5, 111) has been broadcast by Nodes 1 and 3, and their maximum hop count is 5. The RPT of Table 1(b) records RREPs sniffed by an IDS node within its transmission range, for instance, the first row of Table 1(b) indicates the RREP of (source, destination, destination_sequence) = (1, 7, 122) has been forwarded by Nodes 5 and 6, and according to AODV the IDS expects to watch the next node forwarding the RREP as Node 3 that is stored in the field of *expected*. This implies that for the RREP, the latest forwarded node is Node 5 and is destined to Node 1. If Node 1 continues to be within the IDS's transmission range and is not the end of the RREP, and does not forward the RREP within a specific period, then the suspicious value of Node 1 will be added with 1 by the IDS. The SNT-W of Table 1(c), records the suspicious values of neighboring nodes within the IDS's transmission range. The suspicious value is an important basis for a IDS, determining whether a neighboring node is a malicious node. For example, the suspicious value of Node 1 in Table 1 (c) is 2. Assuming it is less than the threshold don't block it so far; whereas the suspicious value of Node 3 is 8; assuming that it reaches the threshold, the node should be blocked. When a normal node receives a block message, the malicious node is appended to the Block table, i.e., BT-W, as shown in Table 2, which lists malicious Node 5, as issued by IDS_A; and malicious Node 2, as issued by IDS_C, as well as their timestamps. Every normal node must authenticate the Block messages from IDSs before updating its own Block table, thus, with the exception of the IDS nodes, nodes cannot broadcast validated Block messages.

Table 1: Tables of AntiWorm and AntiBlackhole

(a) RQT

Route			hop_count	nodes
src	dest	src_seq		
2	5	111	5	1, 3
1	6	121	3	2, 4, 7

(b) RPT

route			nodes	expected
src	dest	dest_seq		
1	7	122	5, 6	3
4	3	124	2, 7	5

(c) SNT-W and SNT-B

node	Value	block
1	2	not
3	8	yes

Table 2 BT-W and BT-B for regular nodes

IDS	malicious node	time
A	5	12:19:17-2012
C	2	12:20:18-2012

In the study of blackhole attacks, three types of nodes, i.e., black hole node, regular nodes, and IDS nodes, are running different algorithms. Black hole node executes the Black hole AODV (BAODV) routing algorithm for performing black hole attacks. Regular node executes the MAODV (the same as in the AntiWorm) to conduct normal routing, and also blocks the malicious nodes in collaboration with IDS nodes. IDS node executes AntiBlackhole to detect black hole nodes, and issues a block message, if necessary.

The algorithm of AntiBlackhole executed on IDS nodes is described below. AntiBlackhole uses two tables of Table 1, RQT and SNT-B. The function of RQT table, Table 1(a), is the same as used by AntiWorm, which records RREQ messages information sniffed. SNT-B, Table 1(c), is used for an IDS node to record the suspicious values of nodes within its transmission range. The suspicious value of a node is an important benchmark to judge a malicious node. Basically, if an intermediate node is not the destination node, and it never broadcasts a RREQ for a specific route, but forwards a RREP for the route, then its suspicious value will be increased by 1 in a nearby IDS's SNT-B. If a black hole node is detected by IDS, it will broadcast the malicious node's ID, through a block message, to all nodes within the transmission range.

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

When a normal node receives a block message, the malicious node's ID is added to the Block table, i.e., BT-B. Similarly, every regular node needs two BTs, i.e., BT-W and BT-B, for recording the blacklist of wormhole nodes and black hole nodes separately.

IV. Simulation Results

Ns2 was used to verify the performance of the proposed AntiWorm and AntiBlackhole mechanisms. The network topology is shown in Figure 3. There were fifty random movable regular nodes with maximum speed in 5m/s randomly distributed in an area of 1000m × 1000m, and MAODV was performed for regular routing. In the area, all of the 9 IDS nodes were deployed that performed either AntiWorm or AntiBlackhole. A pair of wormhole nodes, denoted as W1 and W2, was located diagonally in about 350m × 350m area, wherein two tunnel nodes were applied to play the secret tunnel for wormhole attack. Besides, one black hole node was arranged to reside on the lower right. Ten pairs of connections with UDP-CBR in 5KB per second were assumed. Node pause time was considered as 0, 5, 10, and 15, separately. All results in this section refer to the average of 10 experiments with different random scenarios.

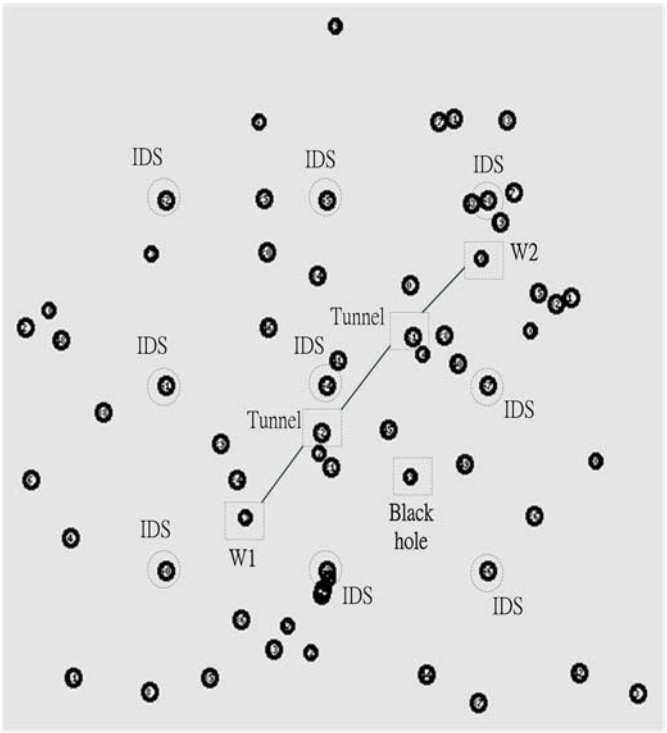


Figure 3: Network topology for ns-2 simulation

We first considered the case of the pair of wormholes was activated. According to the ns2 experiments, the performance of AntiWorm is shown in Figure 4. The average packet loss rate is 10.14% for original AODV and 10.72% for MAODV as there was no wormhole attack; when one pair of wormhole nodes existed, the average rate of total packets lost was increased to 49.63%; through deployment of 9 IDS nodes, the packet loss rate can be decreased to 28.17% in average.

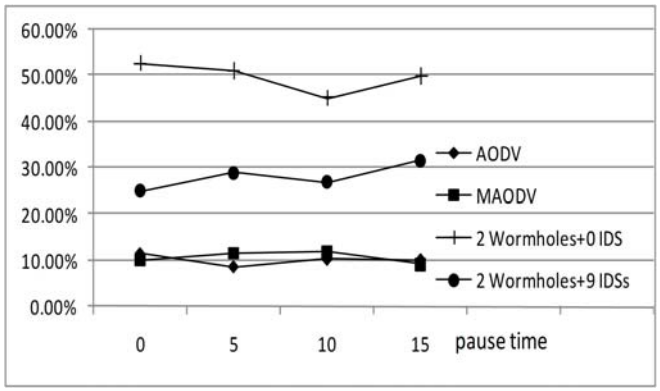


Figure 4: Packet loss rate as two wormhole nodes activate

The performance of AntiBlackhole is shown in Figures 5. In the event of the absence of a black hole node, the total packet loss rates by AODV and MAODV are about 9.62% and 9.87%, respectively; with one fixed black hole node, the total packet loss rate rises sharply to about 90.42%. With the deployment of 9 IDS nodes, the packet loss rate can be successfully reduced to about 15.7%.

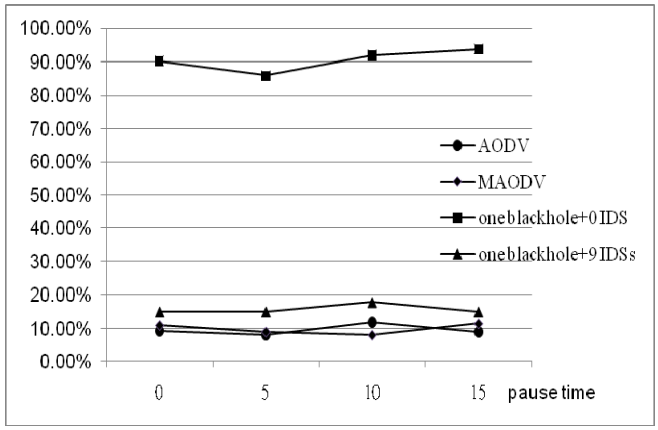


Figure 5 Packet loss rates as one black hole activates

V. Conclusions

This research tried to propose an IDS that can detect both wormhole and black hoe attacks through modifying the algorithms proposed in [1] and [2]. Because in the real world we couldn't predict what kind of attack would occur, so as to deploy a detection system with unique function in advance. The proposed modifications, AntiWorm and AntiBlackhole, now can share the same tables to fight against wormhole attacks and black hole attacks, respectively. That means regular nodes and IDS nodes can keep the necessary information for detecting both attacks. In the near future, we expect to merge the two modules into one multifunctional IDS system. Currently, when there are two (one pair) wormhole nodes, the average rate of total packets lost is increased to 49.63%. With the deployment of 9 IDS nodes performing AntiWorm, the packet loss rate can be decreased to 28.17% in average. As to the black hole attacks, considering one fixed black hole node the total packet loss rate rises to about 90.42%. With the deployed IDSs performing AntiBlackhole, the total packet loss rate can be significantly improved to about 15.7% in average.

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

REFERENCES

[1] M.-Y. Su, "Deployment of Intrusion Detection Nodes to Prevent Wormhole Attacks in Mobile Ad Hoc Networks," *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 7, No. 4, pp. 246-260, 2011.

[2] M.-Y. Su, "Prevention of Selective Black Hole Attacks on Mobile Ad hoc Networks through Intrusion Detection Systems," *Computer Communications*, Vol. 34, Issue 1, pp. 107-117, 2011.

[3] C. E. Perkins, E. Beliding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF Internet Draft, 2004.

[4] G. Lee, D.-kyoo Kim, and J. Seo, "An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks," *Intl Conf. on Inf. Security and Assurance*, pp. 220-225, 2008.

[5] Xu Su and Rajendra V. Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad hoc Networks," *IEEE Intl Conf. on Communications*, pp. 1136-1141, 2007.

[6] Y.-C. Hu, A.Perrig, and Davic B. Johnson, "Ariadne: a Secure On-demand Routing Protocol for Ad Hoc Networks," *ACM Conference on Mobile Computing and Networking* (*Mobicom*), 2002, pp. 12-23.

[7] Farid Naıt-Abdesselam, Brahim Bensaou, and Jinkyu Yoo, "Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol," *IEEE Conf. on Wireless Communications and Networking*, pp. 3117-3122, 2007.

[8] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," IETF RFC 3626, October 2003.

[9] T. V. Phuong, N. T. Canh, Y.-K. Lee, Sungyoung Lee, and Heejo Lee, "Transmission Time-Based Mechanism to Detect Wormhole Attacks," *IEEE Asia-Pacific Service Computing Conf.*, pp.172-178, 2007.

[10] I. Khalil, S. Bagchi, and N. B.Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," *Intl Conf. on Dependable Systems and Networks* (*DSN*), 2005.

[11] I. Khalil, S. Bagchi, and N. B. Shroff, "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks," *IEEE Securecomm and Workshops*, pp. 1-12, 2006.

[12] D. B. Johnson, D.A. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR)," *IETF Internet Draft*, July 2004.

[13] Semih Dokurer, Y. M. Erten, and Can Erkin Acar, "Performance Analysis of Ad-hoc Networks under Black Hole Attacks," *IEEE SoutheastCon*, pp. 148-153, 2007.

[14] Latha Tamilselvan and Dr. V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET," *Intl Conf. on Wireless Broadband and Ultra Wideband Communication*, 2007.

[15] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET," *Journal of Networks*, Vol. 3, No. 5, pp. 13-20, 2008.

[16] S. Kurosawa, H. Nakayama, N. K., A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," *International Journal of Network Security*, Vol.5, No.3, pp.338-346, 2007.

[17] J. Luo, M. Fan, and D. Ye, "Black Hole Attack Prevention Based on Authentication Mechanism," *Intl Conf. on Communication Systems*, pp. 173-177, 2008.

[18] S. D., Farid Nait-Abdesselam, and A. Khokhar, "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol," *IEEE Intl Conf. on Communications (ICC)*, pp. 2780-2785, 2008.

Date of modification: June 7, 2012.
One redundant table was removed and experiments were redone. Some paragraphs were amended to make the motivation of this work more clear.