This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks

Bounpadith Kannhavong, Hidehisa Nakayama[†],
Yoshiaki Nemoto, and Nei Kato
Graduate School of Information Sciences
Tohoku University
Sendai-shi, Miyagi, 980–8579, Japan
[†]hidehisa@it.ecei.tohoku.ac.jp

Abbas Jamalipour
School of Electrical and Information Engineering
The University of Sydney
Sydney NSW 2006, Australia

***Abstract*— Currently, Mobile Ad Hoc Network (MANET) has drawn great attention for being part of the ubiquitous network. Unlike the conventional network, MANETs have many unique features such as node resource constraint. That is why several efficient routing protocols have been proposed specifically for MANETs. Among these protocols, Optimized Link State Routing (OLSR) is one of the four important routing protocol identified by IETF. The current OLSR protocol assumes that all nodes are trusted. However, in hostile environment, the OLSR is known to be vulnerable to various kinds of malicious attacks. In this paper, we propose a new Security Aware Optimized Link State Routing (SA-OLSR) which is a secured version of current OLSR. Our approach is based on exchanging acknowledgement between 2-hop neighbors when the control traffic is successfully received. The main advantage of our approach is that it can protect against many sophisticated attacks such as link spoofing, colluding misrelay attack, and wormhole attack without requiring any location information as well as the knowledge of complete network topology. Our simulation results show that the proposed solution can achieve higher packet delivery ratio compared to the network using the standard OLSR in the presence of malicious nodes.**

Keyword: ***MANET, Routing, OLSR, Security Extension***

I. Introduction

Along with the increasing use of mobile devices and advances in wireless technologies, Mobile Ad hoc Networks (MANETs) are receiving more and more attention from the networking research and industry community. A MANET is a collection of mobile nodes interconnected by wireless links without relying on any fixed infrastructure or centralized access point such as a base station. In MANET, each node acts both as a host and as a router to forward messages for other nodes that are not within the same radio range. The nodes are free to move and form an dynamic topology. MANET can be established in situation where no infrastructure exists, or when deployment of infrastructure is inconvenient or expensive. This inherent flexibility makes it attractive for applications such as emergency operation, disaster recovery, maritime communication, military operation, one-off meeting network, vehicle-to-vehicle network, sensor network and so on.

MANET is characterized by having an open medium, dynamic topology, lacking of a centralized administration, and being bandwidth- and energy-constrained. These features make it difficult to employ existing routing mechanism the same with that of wired network. Therefore, currently, several efficient routing protocols have been designed specifically for MANET environment. Among these protocols, OLSR is the one that provides a promising performance in term of routing overhead and is one of the four routing protocols (i.e., AODV [1], DSR [2], OLSR [3], TBRPF [4]) identified by the Internet Engineering Task Force (IETF). However, the current version of OLSR assumes a cooperative environment where all nodes are trusted and well behaved. As a result, it is vulnerable to various kinds of routing attacks in the presence of malicious nodes.

Current OLSR is known to be vulnerable to identity spoofing, link withholding, link spoofing, misrelay attack, replay attack, wormhole attack and colluding misrelay attack. Recently, several research have appeared [6]–[15] in order to counter against these kinds of attacks. Although they can solve some of these problems, the issue of link spoofing, wormhole attack, colluding misrelay attack are not totally solved.

In this paper, we propose a new Security Aware OLSR which is a security extension for current OLSR protocol. Our approach is based on exchanging of authenticated acknowledgement message (ACK) which is generated by 2-hop neighbors only. By utilizing ACK, our approach allows each node to assure that the message it generated can be successfully received by all its 2-hop neighbors. It also enable each node to verify the existence of link advertised by its 1-hop neighbors.

The rest of this paper is organized as follows. Section II provides an overview of OLSR protocol. In section III, we introduce three severe attacks in OLSR protocol. Section IV discusses the related work on OLSR security. Then we propose a Security Aware OLSR in section V. In section VI, we perform simulation to show the effectiveness our proposed solution. Section VII concludes the paper.

II. Overview of the Optimized Link State Routing (OLSR) Protocol

The Optimized Link State Routing (OLSR) protocol [3] is a proactive routing protocol designed for mobile ad hoc networks. It employs periodic exchange of link state information to maintain topology information of the network at each

978-1-4244-2075-9/08/$25.00 ©2008 IEEE

node. Based on topology information, each node is able to calculate the optimal route to a destination. In OLSR, routes are immediately available when needed.

The key concept of the protocol is the use of *"multipoint relays"* (MPR). Each node selects a set of its 1-hop neighbor nodes as MPR. Only nodes, selected as such MPRs, are responsible for generating and forwarding topology information, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding topology information by reducing the number of transmissions required. The protocol is best suitable for large and dense network as the technique of MPRs work well in this context.

A. Routing Messages in OLSR

In OLSR, two types of control message are used, namely, HELLO message and Topology Control (TC) message.

1) HELLO message: HELLO messages are used for neighbor sensing and MPR selection. Each node broadcasts a HELLO message periodically. The HELLO messages are broadcasted within only one hop and are not forwarded further.

A node's HELLO message contains its own address, a list of its 1-hop neighbors and a list of its MPR set. Therefore, by exchanging HELLO messages, each node is able to obtain the information about its 1-hop and 2-hop neighbors and can find out which node has chosen it as an MPR.

2) TC message: TC messages are used for topology diffusion and it is the message that is used for calculating routing table.

Each node which is selected as an MPR node periodically generate TC message to containing its MPR selector (nodes who has selected this node as MPR) list and only its MPR nodes are allowed to forward TC messages.

Upon receiving TC messages from all MPR nodes in the network, each node learn all node's MPR set and hence obtains knowledge of the whole network topology. Based on these topology, nodes are able to calculate routing table.

B. MPR Selection

Each node independently selects a subset of its 1-hop neighbors as an MPR set. This subset is selected such that it covers the node's all 2-hop neighbors in term of radio range. In case there is multiple choice the minimum subset is selected as an MPR set.

III. Attacks on OLSR Protocol

In this section, we introduce three attacks which is powerful against the current OLSR protocol.

1. *Link Spoofing:* In this attack, a malicious node advertises that it has a direct link with a far away node in its HELLO message or TC message to intercept the control/data traffic or disrupt routing operation. Fig. 1 shows an example of the link spoofing where a malicious node M advertises that it has a direct link (fake link) with node F who is not its direct neighbor. This will cause all traffic from node T to node F routed through M, where M can drop, modify, record or delay such traffic.

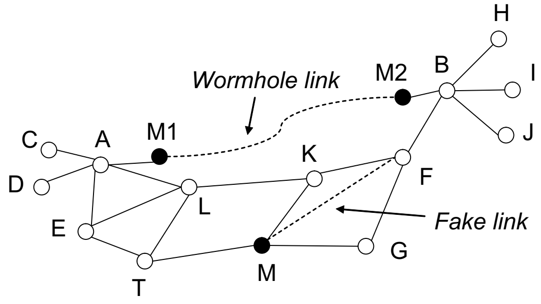


Fig. 1. Example of Link Spoofing and Wormhole Attack

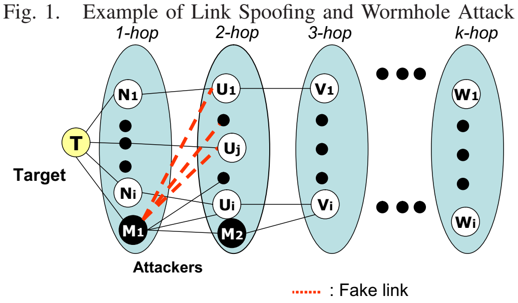


Fig. 2. A Colluding Misrelay Attack Model

2. *Wormhole Attack:* Wormhole attack [5] is one of the most sophisticated and severe attacks in MANET. In this attack, a pair of colluding attackers record packet at one location and replay them at another location using private high speed network. The seriousness of this attack is that it can be launched even against all communications which provides authenticity and confidentiality. Fig. 1 shows an example of the wormhole attack in which two malicious nodes M_1 and M_2 work in collusion to tunnel routing packets, e.g, HELLO messages and TC messages between nodes A and B. This will cause nodes A and B to believe that they are direct neighbors (1-hop neighbors). This will also cause nodes C, D, E to conclude that nodes B is their 2-hop neighbors. As a result, all data traffic from C, D, E to B will be routed the wormhole link which is believed to be the shortest route.
3. *Colluding Misrelay Attack:* The misrelay attack which is launched by one malicious node can be detected by overhearing approach (e.g., [9], [10]). However, in colluding misrelay attack, multiple attackers work in collusion to misrelay packet to avoid being detected by these overhearing schemes. Fig. 2 shows the model of this attack where two nodes work in collusion. In this attack, the first attacker M_1 sends HELLO messages to the target node T advertising that it has direct links with T's all 2-hops neighbors and one unique extra link. According to the protocol, the target node T will choose M_1 as it's only MPR. Therefore, all TC traffic generated/transmitted from T will be routed through M_1 only. M_1 then chooses the second attacker M_2 as its the only MPR. By doing this, M_2 can perform the misrelay attack, i.e., drop or modify packets without being noticed by node T.

IV. Related Work on OLSR Security

Recently, many research have appeared in order to improve security in MANET. In this section, we discuss the main contributions for security in OLSR MANET.

In [6], a fully distributed Certificate Authority (CA) based on threshold cryptography is proposed.

In [7], [8], the use of timestamps are proposed in order to counter against replay attack. The authors of [8] also proposed the use of signature to ensure authentication in order to prevent the identity spoofing attack.

In [9], [10], the authors proposed a simple mechanism to detect the link withholding and misrelay launched by MPR nodes based on overhearing of traffic generated by 1-hop neighbors.

The authors of [11] proposed intrusion detection scheme to detect the misbehavior in OLSR based on intrinsic properties of OLSR messages. However, their approach could not detect the link spoofing attack where a malicious node advertises fake links in HELLO message.

In [12], Raffo et al. proposed a security mechanism based on location information in order to detect the link spoofing and wormhole attack. The main drawback of this approach is that it requires a specialized hardware such as GPS which makes it difficult to realize in practice.

In [13], Vilela et al. proposed a cooperative security scheme based on a Complete Path Message (CPM) and rating table. This approach requires each node who received TC to send CPM back to the TC source. Since the CPM records the path traversed, based on path information from CPM, a node can detect the link spoofing attack. A drawback of this approach is that it incurs a large overhead in terms of additional traffic, since it requires all nodes who received TC message to generate CPM. Since CPM contains complete path it traversed, the size the message will be large as network size increases.

In [14], we have studied a colluding misrelay attack and presented a detection approach by adding the list of 2-hop neighbors in HELLO message. The main idea of this approach is to identify fake link advertised by the first attacker by comparing link information of each neighbor's HELLO message. The main drawback of this approach is that it increases the size of HELLO message. Although this approach can detect the inconsistency during the attack, it cannot judge whether which node is the misbehaving node.

In [15], the author proposed a detection scheme for wormhole attack in OLSR protocol. In this approach, two types of new control packet HELLO$_{req}$ and HELLO$_{rep}$ are defined in order to detect suspicious link by computing delay between the time when a node sends HELLO$_{req}$ and receives HELLO$_{rep}$. Although this approach can deal with wormhole attack, it is still vulnerable to other attacks such as the link spoofing attack or colluding misrelay attack.

As we can see although several research have been carried on and some security issues such as identity spoofing, link withholding and replay attack have been solved, link spoofing, wormhole attack and colluding misrelay attack in OLSR are still problems and therefore more efficient solution are needed. In this article, we present a Security Aware OLSR which can prevent against each of these attacks.

TABLE I
Example of Trust Table

1-hop neighbors	2-hop neighbors	Trust Value
N1_A	N2_A	0
...	...	...
N1_K	N2_K	0

V. A Security Aware OLSR

A. Overview

In this section, we propose a security aware OLSR (SA-OLSR), an improved version of current OLSR in terms of security. The goal of our approach is to assure that routing traffic generated/forwarded by a node can be successfully received by all its 2-hop neighbors and to enable each node to verify the existence of link advertised by its 1-hop neighbors.

To achieve this, we require only 2-hop neighbors to send Acknowledgement (ACK) back to $TC\ source$, the originator of TC message. In our approach, we assume that authentication mechanism [8] is applied in order to identify the exact origin of each packet which prevent malicious node from sending forged ACK. To enable nodes to detect the unreliable link such as fake link and wormhole link, the following two elements are added:

- *Acknowledgement message (ACK$_{TC}$) :* ACK$_{TC}$ is used to assure that TC messages are successfully received by each node's 2-hop neighbors. A node generates ACK$_{TC}$ message only when it received TC message from its 2-hop neighbors.
- *Trust Table:* Each node maintains a Trust Table which contains *2-hop neighbor link tuple* and its *trust value* as shown in Table I in order to observe behavior of it's own 1-hop and 2-hop neighbors. Initially, the trust value of each tuple is set to be 0 as shown in Table I.

B. Proposed Security Extension

The followings describe our proposed modification on the original OLSR.

1. When a node received a TC message from a TC source node, it checks whether or not the source node is its 2-hop neighbor. If the source node is its 2-hop neighbor, it sends ACK$_{TC}$ back to the TC source node. Otherwise it does not generate any ACK$_{TC}$.
2. When a TC source node correctly received ACK$_{TC}$ from its 2-hop neighbor, it judges that the link toward such 2-hop neighbor truly exists and judges that the TC message is successfully received by this 2-hop neighbor node. Then it sets the trust value of that link tuple to be 1.
3. If there exists any 2-hop neighbor link tuple whose Trust Value is 0, a node judges that this link tuple is not reliable since there is possibility that the link toward this 2-hop neighbor is fake or the packets might be dropped by

malicious node (there is also possiblity that the 2-hop neighbor itself does not generate ACK$_{TC}$ intentionally or there might be packet loss due to link error).

4. During MPR selection, a node avoids selecting the node in the suspicious link tuple as its only MPR.

C. Protection Offered

We now show how our approach can thwart against attacks mentioned in section III.

1) Protection against link spoofing attack: Link spoofing will cause the trust value of the fake link to be 0 and hence can be detected. For example in Fig. 1 where M advertises that it has a direct link with F, in this case, T will conclude that F is its 2-hop neighbor. However, in fact F is 3 hops far away from T. Since our approach requires only 2-hop neighbor to generate ACK$_{TC}$, F who is T's 3-hop neighbor will not send ACK$_{TC}$ back to T. This will enable T to learn that F is not its 2-hop neighbor and judge that there is possibility that link $M - F$ does not exist.

2) Protection against colluding misrelay attack: Note that in colluding misrelay attack (see Fig. 2), link between the first attacker A_1 and some of Target T's 2-hop neighbor is fake, even A_1 correctly relayed TC messages, these messages will not reach such 2-hop neighbors $(U_1, ...U_j)$. Therefore, T will not receive ACK$_{TC}$ from these 2-hop neighbors and hence T can detect the anomaly due to this attack.

3) Protection against wormhole attack: Our approach can detect the wormhole attack by calculating the delay between the time a node sends TC (t_s) and the time a node received the corresponding ACK$_{TC}$ (t_r). In normal operation (Fig. 3(a)), $t_r - t_s$ must satisfy the following formula:

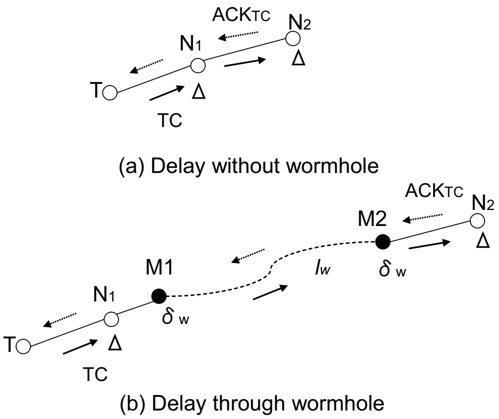
$$t_r - t_s \leq \frac{4r}{v} + 3\Delta \tag{1}$$

where r is the maximum transmission range, v is the travel speed of wireless medium, Δ is the maximum processing time at each node. However, during the attack (Fig. 3(b)), let l_W denotes the length of wormhole link ($l_w > r$), v_w denotes the transmission speed in wormhole link, and δ_w denotes the processing time at wormhole attackers, the delay $t_r - t_s$ is $t_r - t_s = \frac{6r}{v} + \frac{2l_w}{v_w} + 3\Delta + 4\delta_w > \frac{4r}{v} + 3\Delta$, which will not satisfy formula (1). Therefore, by checking whether $t_r - t_s$ satisfies formula (1), nodes in SA-OLSR are able to detect the wormhole attack.

D. Overhead

We can mathematically evaluate the overhead incurred by using additional ACK compared with the security scheme which uses CPM [13]. Let n denotes the total number of nodes in network, m denotes the number of MPR nodes, i.e., TC source. Let $nb2_k$ denotes the number of node K's 2-hop neighbors and $Average(nb2)$ denotes the average number of each TC source's 2-hop neighbors ($Average(nb2) < n$). Then the number of messages increased by using CPM is :

$$\sum_{k=1}^{m}(n-1) = m(n-1)$$



(a) Delay without wormhole

(b) Delay through wormhole

Fig. 3. Detecting Wormhole Attack

TABLE II
SIMULATION PARAMETERS

Simulator	NS-2 (ver.2.28)
Simulation time	50 seconds
Transmission range	250m
Link bandwidth	2 Mbps
Traffic type	CBR
Data payload	512 bytes
Packet rate	4 pkt/s
Number of total nodes	17
Number of attackers	2
Number of connections	1

While the number of ACK message incurred by our approach is :

$$\sum_{k=1}^{m}(nb2_k) = m \times Average(nb2)$$

Since $Average(nb2) < n$, our approach can provide security while generating fewer overhead than the approach applying CPM. Furthermore, the size of ACK is far less than the size of CPM which contains complete path it traversed. As the network size gets larger, n will be increased, i.e., $n \gg Average(nb2)$, which indicates that our approach generates overhead less than that of the one using CPM. Therefore, we can say that our approach is more scalable.

VI. Simulation and Results

To evaluate the effectiveness of our approach, we have implemented the SA-OLSR in a network simulator NS-2 [16]. The parameters used in our simulations are shown in Table II. In our simulation, there are 17 wireless nodes including 2 colluding attackers and 1 target node on a 1000 meters by 1000 meters area.

As a case study, we simulated the colluding misrelay attack in which the first attacker advertises fake link with the target's 2-hop neighbors, while the second attacker drops TC messages that routed through itself. In the simulation, each node moves according to random waypoint model, i.e, after it arrives at a random location, it stays there for a pause time seconds before moving to the next random destination and repeating the same

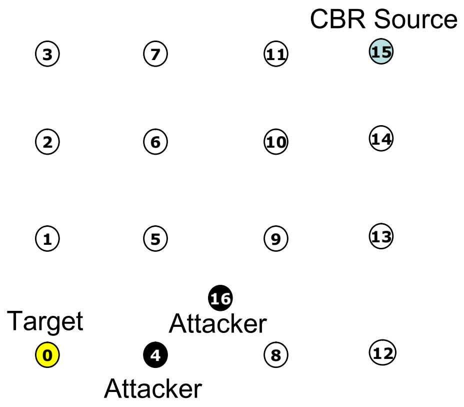


Fig. 4. Example of simulation topology

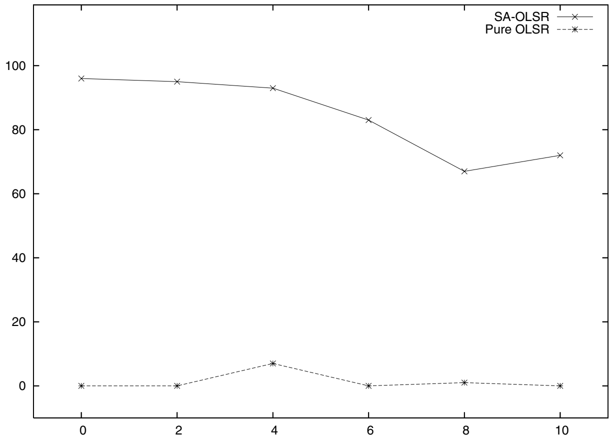


Fig. 5. Delivery ratio for varying maximum speed of nodes

process. Here we set the pause time to be 0. To study the impact of the attack, packet delivery ratio has been observed. Here, we define the delivery ratio as the ratio between number of data packets generated by the application layer CBR source and the number of packets received by the destination.

Fig. 4 shows an example of topology used in our simulations. In the simulation, there are one CBR connection to a target node from a source node whose distance is further than two hops away from it. Each node moves to a random destination with a random speed. We vary the maximum speed of each node node from 0 m/s to 10 m/s in 2 m/s increments and observe the packet delivery ratio of CBR traffic sent from the CBR source node to the target node for each scenario. Then we compare the packet delivery ratio obtained by our approach and the original OLSR.

The simulation results are shown in Fig. 5. As we can see from the result, during the attack, the target node in OLSR can hardly receive data packets. Our approach can achieve much higher packet delivery ratio. From these experiments, it is easy to see that in the current OLSR protocol, attackers can easily prevent a target node from receiving data packets from other nodes and it also indicates that our approach can provide effective protection against the malicious attack.

VII. Conclusions

In this paper, we have presented a Security Aware OLSR (SA-OLSR) as a security extension to the original OLSR protocol. Our approach is based on exchanging acknowledgement between two hop neighbors. The main advantage of our approach is that it does not require any specialized hardware such as GPS and does not require complete knowledge of the whole network while being able to protect several kinds of attacks. To validate analysis, we have implemented our proposed solution on a network simulator as well as performed simulations of a colluding misrelay attack as a case study. Simulation results show that the attack can bring a devastating impact on the current OLSR. It also shows that the proposed security mechanism provides an effective protection against this kind of attack.

References

[1] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-demand Distance Vector (AODV) Routing,” IETF RFC 3561, July 2003.

[2] D. B. Johnson, D. A. Maltz, and Y-C. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),” IETF Internet Draft, draft-ietf-manet-dsr-09, April 2003.

[3] T. Clausen et. al, “Optimized Link State Routing Protocol,” IETF Internet Draft, draft-ietf-manet-olsr-11.txt, July 2003.

[4] R. Ogier, M. Lewis, and F. Templin, “Topology Dissemination Based on Reverse-Path Forwarding (TBRPF),” IETF Internet Draft, draft-ietf-manet-tbrpf-07.txt, March 2003.

[5] Y-C. Hu, A. Perrig, and D. Johnson, ”Packet Leashes: a Defense against Wormhole Attacks in Wireless Networks,” in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pp.1976-1986, 2003.

[6] D. Dhillon, T.S. Randhawa, M. Wang and L. Lamont, ”Implementing a Fully Distributed Certificate Authority in an OLSR MANET,” IEEE WCNC2004, Atlanta, Georgia USA, March 21-25, 2004.

[7] C. Adjih, D. Raffo, and P. Muhlethaler, ”Attacks Against OLSR: Distributed Key Management for Security,” 2nd OLSR Interop/ Workshop, Palaiseau, France, July 28-29, 2005.

[8] D. Raffo, ”Security Schemes for the OLSR Protocol for Ad Hoc Networks,” Ph.D. thesis, Universite Paris, 2005.

[9] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, ”Analysis of the Node Isolation Attack against OLSR-based Mobile Ad Hoc Network,” 7th International Symposium on Computer Networks (ISCN), pp. 30-35, Istabul, Turkey, Jun. 2006.

[10] D. Dhillon, J. Zhu, J. Richards, T. Randhawa, ”Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs,” in IWCMC 2006.

[11] M. Wang, L. Lamont, P. Mason, M. Gorlatova, ”An effective Intrusion Detection Approach for OLSR MANET Protocol,” 1st IEEE ICNP Workshop on Secure Network Protocols (NPSec 2005).

[12] D. Raffo, C. Adjih, T. Clausen, P. Muhlethaler, ”Securing OLSR Using Node Locations,” in Proceedings of 2005 European Wireless (EW 2005), Nicosia, Cyprus, 2005.

[13] A J. P. Vilela and J. Barros, ”A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks,” Proc. of the 15th IST Mobile and Wireless Communications Summit, Mykonos, Greece, June 2006.

[14] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, ”A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks,” IEEE Global Telecommunications Conference 2006 (Globecom), San Francisco, USA, Nov. 2006.

[15] F. Nait-Abdesselem, J.K. Yoo and B. Bensaou, ”Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol,” IEEE Wireless Communications and Networking Conference (IEEE WCNC), March 2007.

[16] The Vint Project, “The Network Simulator - ns-2,” see http://www.isi.edu/nsnam/ns/index.html/.