Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks

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

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

***Abstract*— Recent advances in wireless networking technologies have made it possible to construct a Mobile Ad hoc Network (MANET) which can be applied in infrastructureless situations. However, due to their inherent characteristics, they are much more vulnerable to malicious attacks than a conventinal wired network. In MANET, routing plays an important role in providing connectivity for mobile nodes who are not within the same radio range. Existing routing protocols in MANET assume a trusted and reliable environment. However, in hostile environment mobile nodes are susceptible to various types of routing attacks. This paper identifies a new routing attack, called Node Isolation attack, against Optimized Link State Routing (OLSR) protocol, one of the four standard routing protocols for MANETs. We analyze in detail and demonstrate the impact of this attack in order to show the necessity for a countermeasure to guard against the attack. As a first step to defend against the attack, we present a simple technique to detect the attack and identify the source of the attack.**

Keywords: ***MANET, Security, OLSR, MPR, Node Isolation Attack***

I. Introduction

With the advent of mobile computing devices and advances in wireless communication technologies, Mobile Ad hoc Networks have been attracting significant attention from the networking research community. A Mobile Ad hoc Network (MANET) is a collection of mobile nodes interconnected by wireless links without the aid of 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 arbitrary 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 [1]. These features make it difficult to deploy security mechanisms similar to that of in wired network. As a result, MANETs are more vulnerable than a conventional wired network and are susceptible to various kinds of attacks including eavesdropping, unauthorized modification, impersonation and routing attack. In MANET security, routing attack is particularly a serious problem.

At present, the Internet Engineering Task Force (IETF) MANET Working Group has selected four standard routing protocols: Ad hoc On Demand Vector (AODV) protocol [2], Dynamic Source Routing (DSR) protocol [3], Optimized Link State Routing (OLSR) protocol [4], and Topology Broadcast based on Reverse-Path Forwarding (TBRPF) protocol [5].

Recently, several research efforts (e.g. ARAN [6], Ariadne [7], SAODV [8], [9], SEAD [10]–[17]) have focused on providing preventive schemes to secure the routing protocol in MANET. Most of these schemes rely on key management or encryption techniques to prevent unauthorized users from joining the network. However, these approaches cannot prevent attacks launched by a compromised node who owns a legitimate key. Therefore, as a second wall of protection, intrusion detection and reaction system appears to be a promising solution. To design an effective and efficient intrusion detection and reaction system, it is crucial to understand on how a compromised node can attack a MANET. In [18], Ning and Sun analyzed and evaluated several possible insider attacks against the AODV protocol including route disruption, node isolation and resource consumption attack. In [19], Hu et al. introduced a rushing attack which result in DoS attack on MANET when AODV protocol is used. The same authors also presented a wormhole attack as well as the countermeasure against the attack [20]. Wang et al. [21] studied and showed that false distance vector and false destination sequence attacks against AODV can lead to a decrease up to 75% in data delivery ratio. In [22] and [23], the influence of resource consumption attack on the performance of AODV protocol has been studied. Kurosawa et al. [24] presented an analysis of blackhole attack on AODV protocol. In [25], several passive attacks model against AODV protocol have been proposed. However, we have not seen any previous study seriously analyzing and evaluating the impact of attacks against OLSR protocol.

In this paper, we identify a new routing attack, called Node

Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN'06)
1-4244-0491-6/06/$20.00 © 2006 IEEE

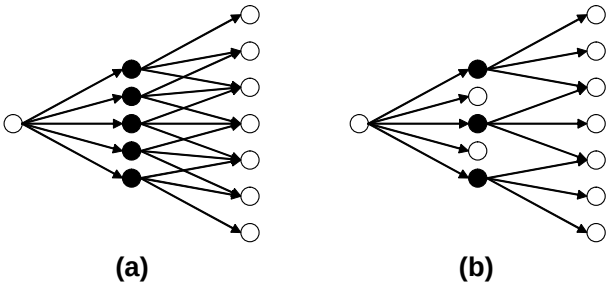


Fig. 1. The broadcast from the leftmost node is retransmitted: (a) by all its neighbors (b) by its MPRs only

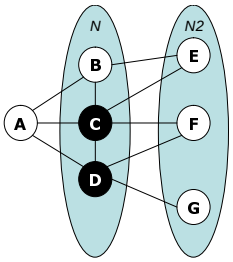


Fig. 2. Node C and D are MPR for A

Isolatin attack, against OLSR-based mobile ad hoc network, analyze the attack in detail, and demonstrate the impact of the attack through simulations. As a first step to guard against the attack, we present a simple technique to detect the attack and identify the source of the attack.

The rest of this paper is organized as follows. Section II describes an overview of the OLSR protocol. Section III introduces the Node Isolation attack. Section IV shows the experimental result. Section V presents a technique to detect the Node Isolation attack. Section VI describes our future works and concludes the paper.

II. The Optimized Link State Routing (OLSR) Protocol

The Optimized Link State Routing (OLSR) protocol is an important proactive routing protocol designed for mobile ad hoc networks. It employs periodic exchange of messages to maintain topology information of the network at each 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 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. Fig. 1 illustrates a node broadcasts its messages throughout the network using standard flooding (Fig. 1 (a)) and MPR flooding (Fig. 1 (b)).

The core functionality of OLSR includes neighbor sensing, multipoint relays selection, topology diffusion and routing table calculation. The followings describe each process.

A. Neighbor Sensing

For neighbor sensing, the HELLO messages are broadcasted periodically. The HELLO messages are broadcasted only one hop away and are not forwarded further.

These messages are used to obtain the information about neighbors. A HELLO message performs the task of neighbor sensing and MPR selection process. 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 choosen it as an MPR.

B. Multipoint Relays Selection

In this subsection, we describe the idea of multipoint relay and algorithm to select MPR [4], [26].

1) Multipoint Relay: The idea of multipoint relays is to minimize the overhead of flooding messages in the network by reducing redundant retransmissions in the same region. Each node in the network selects a set of nodes in its 1-hop neighbors which may forward its messages. This set of selected neighbor nodes is called the "Multipoint Relay" (MPR) set of that node. When a node sends a routing message, only the nodes that are in its MPR set forward its message.

Each node selects its MPR set from among its 1-hop neighbors such that they cover (in term of radio range) all its 2-hop neighbors.

Each node maintains information about the set of neighbors that have selected it as an MPR. This set is called the "Multipoint Relay Selector set" (MPR selector set) of a node. A node obtains this information from periodic HELLO messages received from the neighbors. In OLSR, each node must forward the routing message, intended to be diffused in the whole network, coming from any of its MPR selectors.

2) Multipoint Relays Selection Algorithm: The goal of MPR selection is to construct the MPR set which includes minimum number of the 1-hop neighbors from which it is possible to reach all 2-hop neighbors.

The algorithm for selecting Multipoint Relay set is as follows:

Input : A node's 1-hop neighbor set N and 2-hop neighbor set $N2$.

Output : A node's MPR set M.

(1) For each node in N, calculate the degree, which is the number of nodes in $N2$ that it can reach.
(2) Add to M the nodes in N which are the only nodes to provide reachability to a node in $N2$.
(3) Remove from $N2$ the nodes which are now covered by a node in M.

(4) While there exists nodes in $N2$:
  (4.1) For each node in N, calculate the reachability, which is the number of nodes in $N2$ that it can reach.
  (4.2) Add to M the node that provides the highest reachability. In case of multiple choice choose the node which has the highest degree.
  (4.3) Remove from $N2$ the nodes which are now covered by a node in M.

Fig. 2 shows how a node (say A) selects its MPRs. Initially, Node A's 1-hop neighbor set N is {B,C,D}, 2-hop neighbor set $N2$ is {E,F,G} and its MPR set M is empty. In step (1), the degree of nodes in N is calculated. From the calculation, we obtain the degree of Node B, Node C, Node D as 1, 2, 2, respectively. Next, in step (2), Node D is added to the MPR set M since it is the only node who can reach Node G. In step (3), F and G are removed from $N2$ since it is covered by Node D. Therefore, $N2$ becomes {E}. In step (4.1), the reachability of each node in N is calculated. From this step, we obtain reachability of Node B, C, D as 1, 1, 0, respectively. Next, in step (4.2) Node C is added to MPR set M since it has the highest reachability and highest degree. Therefore, we obtain MPR set M as {C,D}. In step (4.3), E is removed from $N2$ since it is covered by Node C. At this point, since $N2$ is empty, we can obtain the final MPR set as {C,D}. Therefore, Node C and D are the only set of nodes that must forward routing messages, intended to be disseminated to the entire network, coming from Node A.

C. Topology Diffusion

In order to disseminate the topology information, the node that were selected as MPR must generate a topology control (TC) message periodically. MPR nodes must also forward TC message for its MPR selector. The TC messages are the message that are intended to be flooded throughout the network and only MPR are allowed to forward TC messages. A node's TC message contains a list of its MPR selector set. For example, in Fig. 2, Node C and Node D's TC messages must contain the address of Node A who is one of their MPR selectors. Upon receiving TC messages of all MPR nodes in the network, each node learns all node's MPR set and hence obtains knowledge of the whole network topology. Based on these topology, the nodes are able to calculate routing table.

D. Routing Table Calculations

Each node maintains a routing table which allows it to send data to a destination either for itself or for the other nodes in the network.

Each entry in the table contains: destination address, next-hop address, distance, and local interface address. Next-hop address is the address of next hop node in the route to the destination node. Distance is the number of hops to the destination. Local interface address is the node's own address. The routing table calculation is based on Dijkstra's algorithm for finding the shortest path.

The routing table is updated when a change is detected in either the 1-hop neighbor set or the 2-hop neighbor set. More precisely, it is recalculated in case of neighbor appeared or lost, when a 2-hop neighbor is created or removed.

Currently, OLSR does not specify any special security measures. As a result, OLSR is vulnerable to various kinds of attacks. In the next section, we describe a Node Isolation attack which is one of many possible attacks against the OLSR protocol.

III. Node Isolation Attack Model

In this section, we present a Node Isolation attack against the OLSR protocol. As implied by the name, the goal of this attack is to isolate a given node from communicating with other nodes in the network. More specifically this attack prevents a victim node from receiving data packets from other nodes in the network. The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes. This attack can be achieved by exploiting the MPR selection algorithm. The followings are details on how a malicious node can launch the Node Isoaltion attack on a specific node.

Fig. 3 shows a general image of the attack. Let Node T be the target to be attacked and let Node A be an attacker. In the figure, $\{N_1, \ldots, N_i\}$ and A is the subset of set N which is the set of Node T's 1-hop neighbor nodes. $\{U_1, \ldots, U_i\}$ is the subset of set N_2 which is the set of Node T's 2-hop neighbor nodes. $\{V_1, \ldots, V_i\}$ is the subset of set N_j which is the set of nodes whose distance to Node T is further than two hops.

In this attack, attacker A creates virtual links by sending fake HELLO messages including the address list of nodes $\{U_1, \ldots, U_i\}$ who are two hops away from a target node T. According to the protocol, the target node T will select attacker A to be its only MPR. Thus, the only node that must forward and generate TC messages for the target node T is the attacking node A. By dropping TC messages received from the target and not generating TC messages for the target node, the attacker can prevent the link information of target node from being disseminated to the whole network. As a result, other nodes would not be able to receive link information of a target node and will conclude that a target node does not exist in the network. Therefore, a target node's address will be removed from other nodes' routing tables. Since in OLSR, through HELLO messages each node can obtain only information about its 1-hop and 2-hop neighbors, other nodes that are further than two hops away from a target node, i.e, $\{V_1, \ldots, V_i\}$ will not be able to detect the existence of the target node. As a consequence, the target node will be completely prevented from receiving data packets from nodes that are three or more hops away from it.

Fig. 4 (a) shows an example of this attack. In the figure, Node C is the attacking node, and Node B is the target node. Instead of sending correct HELLO message contains {B,F} in neighbor address list, the attacker sends a fake HELLO message contains {B,F,G,Z} which includes the target node's

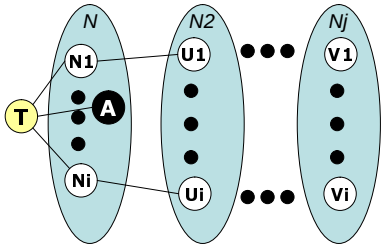
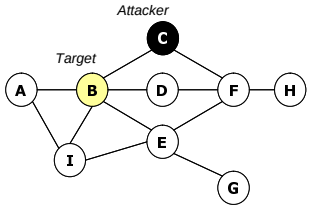
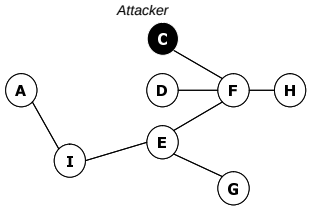


Fig. 3. Attack model



(a) Topology perceived by node H before the attack



(b) Topology perceived by node H after the attack

Fig. 4. Example of the Node Isolation Attack

all 2-hop neighbors {F,G} and one non-existent node {Z}. According to the protocol, the target node B will select the attacker C as its only MPR. Being Node B's the only MPR, attacker refuse to forward and generate TC message for Node B. Since the link information of Node B is not propagated to the entire network, other nodes whose distance to Node B is more than two hops (e.g. Node H) would not be able build route to Node B. As a result, other nodes would not be able to send data to Node B. Despite being existed in the network, the target node B will be isolated from the network (Fig. 4 (b)).

An attacker can launch this attack, as long as the target node is within its transmission range. Although the attack will not hold when the target node moves out of the attacker's transmission range, the attack can become more powerful when multiple attackers present in the network.

IV. Simulation Results of The Node Isolation Attack

To validate our analysis, we have implemented the Node Isolation attack in a simulator and performed series of simulation-based experiment to test its effectiveness. We run simulation on the network simulator NS-2 [27] using OLSR

TABLE I
SIMULATION PARAMETERS

Simulator	NS-2 (ver.2.28)
Simulation time	100 sec
Transmission range	250 m
Link bandwidth	2 Mbps
Traffic type	CBR
Data payload	512 bytes
Packet rate	4 pps
Number of total nodes	15
Number of attackers	4
Number of connections	1

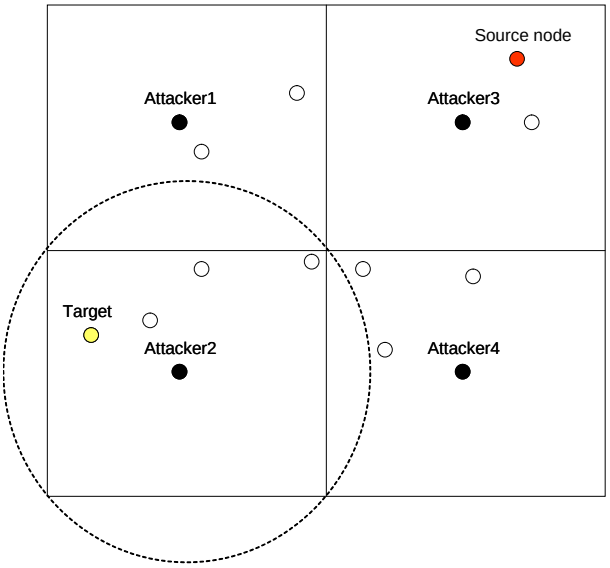


Fig. 5. Example of simulation topology

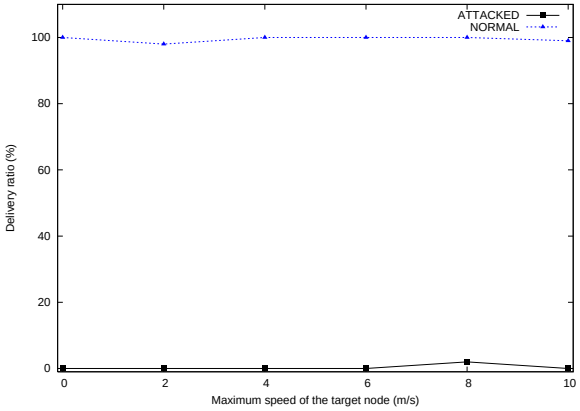


Fig. 6. Delivery ratio for varying maximum speed of a target node

source code from [28]. The parameters used in our simulations are shown in Table I. In the simulation, the radio transmission range for each node is 250 meters and link bandwidth is set to 2 Mbps. The duration of simulation is 100 seconds. We use Constant Bit Rate (CBR) as the traffic source. The size of data payload is 512 bytes transmitted at the rate of 4 packets/s.

We simulated scenarios consisted of 15 wireless nodes including 4 attackers and 1 target node on the 1000 meters by 1000 meters area. The target node moves according to random waypoint model [29], i.e, after it arrives at a random location, it stays there for pause time seconds before moving to the next random destination and repeating the same process. Here we set the pause time to be 2 seconds. Attackers are placed such that their transmission range cover all area of target's movement. Fig. 5 shows an example of topology used in our simulations.

To test the feasibility 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.

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. We vary the maximum speed of the target node from $0m/s$ to $10m/s$ in $2m/s$ increments and observe the packet delivery ratio to a target node from a source node who is further than two hops away for each scenario.

The simulation results are shown in Fig. 6. As expected, when there is an attack, the delivery ratio drops almost to 0%, while in normal situation the target node can almost receive all generated data packets from the source node.

From these experiments, it is easy to see that attacker(s) can effectively prevent a target node from receiving data packets from other nodes whose distance to a target node is more than two hops. This implies that, the Node Isolation Attack can result in DoS attack to the target node.

V. Detecting the Node Isolation Attack

In this section, we propose a simple technique to detect the node isolation attack. Fig. 7 shows the idea on how to detect the attack. In MANET, a node, say Node T can hear a transmission from its MPR due to the nature of broadcast channel in wireless network. By hearing its own MPR's transmission, Node T can find out whether its MPR is malicious or not. In OLSR protocol, as a rule each node must broadcast HELLO message to indicate its existent periodically, say, every *HELLO_INTERVAL* period. Nodes who are MPR for other nodes must also broadcast TC messages periodically, say, every *TC_INTERVAL* period to advertise link information for its MPR selector. However, during the Node Isolation attack, attacker who is an MPR does not follow the above mentioned rule by broadcasting only HELLO message and not generating TC message in order to isolate a node who is its MPR selector. Therefore, only HELLO message will be heard while TC message which include Node T's address will not be observed

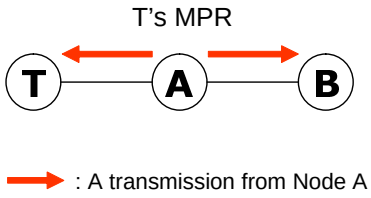


Fig. 7. Basic idea in detecting the Node Isolatin attack (Node T can hear a transmission from its MPR)

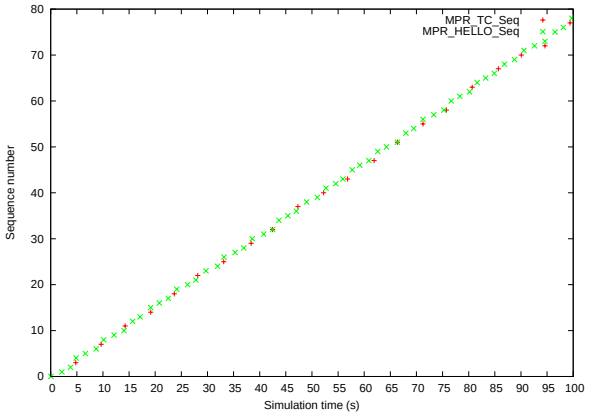


Fig. 8. Sequence number of observed HELLO and TC message generated by target node's MPR during the normal operation

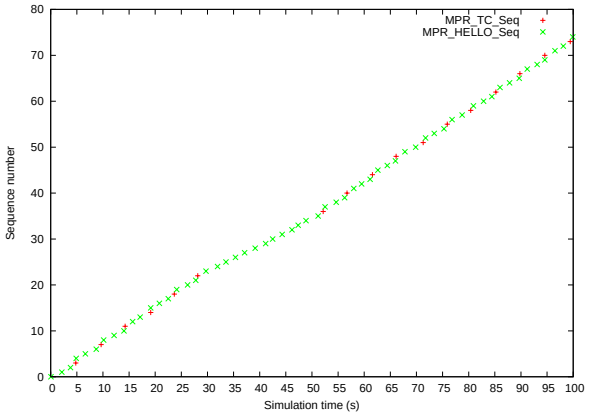


Fig. 9. Sequence number of observed HELLO and TC message generated by target node's MPR under when attack is launched from $30s$ to $50s$

during the attack period. Based on this observation, we can effectively detect the anomaly due to the attack.

To confirm this we ran the simulation using the same topology with previous simulation with attack launched from $30sec$ to $50sec$ as well as without attack. We observed the sequence number of TC message and HELLO message generated by MPR of the target node.

The results of this observation when there is no attack and when there is attack is shown in Fig. 8 and Fig. 9, respectively. From the results we can see that when there is no attack the TC message and HELLO message has been observed periodically (Fig. 8). However, when there is attack only HELLO message has been observed from $30s$ to $50s$ (Fig. 9). This is bescause during the attack a malicious node did not generate any TC

message. In this way, if a node has detected that its MPR fails to generate TC message, a node can judge that its MPR is trying to isolate it.

Using the above technique a node can effectively identify the source of the attack. However, one limitation of this approach is that it might not detect the attack which is launched by two consecutive nodes who work in collusion. For example, in Fig. 7 although Node A generates TC message advertise link information for Node T, Node B who is Node A's partner drops this link information. In this case it will be very difficult to detect the attack and therefore needs a new technique to detect and take countermeasure against the attack.

VI. Conclusions and Future Works

Recently, MANETs are receiving a tremendous attentions from the networking research community due to their flexibility and their easy deployment. MANET uses routing protocol to provide connectivity between nodes who are not within the same radio range. Existing MANET routing protocols assume a trusted and cooperative environment. However, in hostile environment MANET are susceptible to various kinds of attacks which is more serious than conventional wired network. In MANET, routing attack is particularly a major concern. In this paper, we have presented a new routing attack, called Node Isolatin attack, against OLSR-based mobile ad hoc network. This attack allows attacker(s) to isolate a specific node or a group of nodes from receiving data packets from other nodes who is further than two hops. We demonstrated the impact of this attack through simulations. After analyzed the Node Isolation Attack in detail, we have presented a simple technique to detect the attack as the first step to defend against the attack.

One shortcoming of the proposed solution is that it might not detect the attack in which two consecutive nodes work in collusion. Currently, we are seriously working on this issue. Our future work will also be focused on investigating other sophisticated attacks which have not been well studied as well as studying the possible countermeasure against such attacks.

References

[1] S. Corson, and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," IETF RFC 2501, January 1999.

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

[3] 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.

[4] Th. Clausen et. al, "Optimized Link State Routing Protocol," IETF Internet Draft, draft-ietf-manet-olsr-11.txt, July 2003.

[5] 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.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. BeldingRoyer, "A Secure Routing Protocol for Ad Hoc Networks," In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002.

[7] Y-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," in Proceedings of the MobiCom 2002, Atlanta, Georgia, USA, September 23-28, 2002.

[8] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector Routing," ACM Mobile Computing and Communications Review (MC2R), Vol. 6, No. 3, pp. 106-107, July 2002.

[9] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," In Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pp. 1-10, September 2002.

[10] Y-C. Hu, D. B. Johnson, and A. Perrig "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

[11] P. Papadimitratos, and Z. Haas, "Secure routing for mobile ad hoc networks," in Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, January 27-31, 2002.

[12] S. Capkun, L. Nuttyan, and J. Hubaux, "Self-organized public-key Management for mobile ad hoc networks," IEEE Transactions on mobile computing, Vol. 2, No. 1, January-March, 2003.

[13] L. Zhou, and Z. J. Haas, "Securing ad hoc networks," IEEE Networks Special Issue on Network Security November/December, 1999.

[14] C. Adjih, Th. Clausen, Ph. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR protocol," In Proceedings of Med-Hoc-Net, Mahdia, Tunisia, June 25 2003.

[15] 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.

[16] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An Advanced Signature System for OLSR," in Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 04), Washington, DC, USA, October 25 2004.

[17] 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.

[18] P. Ning, and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," Tech. Rep. TR-2003-07, North Carolina State University, Department of Computer Science, February 2003.

[19] Y-C. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," ACM Workshop on Wireless Security (WiSe 2003) Westin Horton Plaza Hotel, San Diego, California, U.S.A, September 19, 2003.

[20] 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.

[21] B. B. W. Wang, and Y. Lu, "On Vulnerability and protection of ad hoc on-demand distance vector protocol," In International Conference on Telecommunication, France, Paris, 2003.

[22] P. Yi, Zh. Dai, Sh. Zhang, and Y. Zhong, "A New Routing Attack in Mobile Ad Hoc Networks," International Journal of Information Technology, Vol. 11, No. 2, 2005.

[23] S. Desilva and R.V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proceeding of IEEE Wireless Communication and Networking Conference 2005, New Orleans, Lucian, USA.

[24] S. Kurosawa, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," In proceeding of International Journal of Network Security, 2006

[25] X. Hong, J. Kong, and M. Gerla, "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks," in Proceedings of IEEE Military Communications Conference (MILCOM'03), Boston, MA, October 13-16, 2003.

[26] J. Leguay, V. Conan, and T. Friedman, "QoS Routing in OLSR with Several Classes of Service," IEEE PerCom Workshop on Pervasive Wireless Networking (PWN06) Pisa, Italy, March, 2006.

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

[28] F. J. Ro, "UM-OLSR Documentation," University of Murcia, March 2005, see http://masimum.dif.um.es/um-olsr/html/index.html

[29] C. Bettstetter, G. Resta, and P. santi, "The Node Distribution of the Random Waypoint Mobiligy Model for Wireless Ad Hoc Networks," IEEE Transanction on Mobile Computing, Vol.2, No. 3, pp. 257-269, July/september, 2003.