Improved Routing for Protection against Denial of Service Attack in Ad Hoc Networks

M. Dhivya
ME-CSE
Kongunadu College Of Engineering & Tech
Trichy.

A. Kanimozhi,
ME,Assistant Professor,
Kongunadu College Of Engineering & Tech
Trichy.

Abstract--**In MANETs, applications are mostly involved with sensitive and secret information. It assumes a trusted environment for routing, security is major issues. Here analyze the vulnerabilities of a pro-active routing protocol called optimized link state routing (OLSR) against node isolation attack and colluding attack can be easily launched. The OLSR protocol is secured by Enhanced OLSR (EOLSR) mechanism, which is a trust based technique to secure the EOLSR nodes against the attack. This technique is capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus detecting node isolation attacks called Denial-of-service (DOS) attack. The colluding attack can be injected nodes will work together to generate a severe attack in the network, which aims to create a collision at an arbitrary node, we present a collusion attack model against optimized Link State Routing (OLSR) Protocol. to detect the attack by utilizing information of two hops neighbors. The experiment results show that our protocol is able to achieve routing security with increase in packet delivery ratio and reduction in packet loss rate when compared to standard OLSR under node isolation attack and colluding attack.**

Index Terms*— *Ad hoc networks, denial-of-service (DOS) attack, node isolation attack, colluding attack, optimized link state routing (OLSR), protocols.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices which are connected by wireless links without the use of any fixed infrastructures or centralized access points. In MANET, each node acts not only as a host but also as a router to forward messages for other nodes that are not within the same direct wireless transmission range. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. MANETs are much more vulnerable and are susceptible to various kinds of security attacks because of its cooperating environment. In the absence of a fixed infrastructure that establishes a line of defence by identifying and isolating non-trusted nodes, it is possible that the control messages generated by the routing protocols are corrupted or compromised thus affecting the performance of the network. Routing protocols in MANET can be classified into two categories: reactive protocol and proactive protocol. In proactive routing protocols, all nodes need to maintain a consistent view of the network topology. When a network topology changes, respective updates must be propagated throughout the network to notify the change. In reactive routing protocols for mobile ad hoc networks, which are also called "on-demand" routing protocols, routing paths are Searched for, when needed. Even though many research works had been carried out for routing attacks in MANET,**.** most of it concentrated mainly on reactive routing protocols. Optimized link state routing (OLSR) routing protocol which is a proactive routing protocol offers promising performance in terms of bandwidth and traffic overhead but it does not incorporate any security measures. As a result, OLSR is vulnerable to various kinds of attacks such as flooding attack; link withholding attack, replay attack, denial-of-service (DOS) attack and colluding injected attack.

In this paper, we analyze a node isolation attack and colluding attack propose a solution for it. Node isolation attack can be easilylaunched on OLSR after observing the network activity for a period of time. We propose a solution called enhanced OLSR (EOLSR) that is based on verifying the hello packets coming from the node before selecting it as a multipoint relay (MPR) node for forwarding packets. Another work, we propose an active attack scheme named Colluding Injected Attack (CIA) in MANET. These injected nodes will work together to generate a severe attack in the network, which aims to prevent a specific node from receiving any packet. This proposed attack will make use of the hidden terminal problem and create a collision at an arbitrary node, which in turn will result in making the attacked node unable to receive or relay any packet. Also the CIA attack in a neighborhood aims to mislead the watchdogs' nodes (nodes that used to monitor the behaviors of other nodes in a neighborhood) in wrongly reporting the attacked node (the legitimate node) as behaving maliciously in this neighborhood.

II. THE ENHANCED OPTIMIZED LINK STATE ROUTING (EOLSR) PROTOCOL

Enhanced Optimized link state routing (EOLSR) [2], [5] is one of the most important proactive routing protocols designed for MANET. It employs periodic exchange of messages to maintain topology information of the network at each node. The key concept of OLSR is the use of multipoint relay (MPR) to provide efficient flooding mechanism by reducing the number of transmissions required. Each node selects a set of its neighbor nodes as MPR. Only nodes selected as MPR nodes are responsible for advertising as well as forwarding topology information into the network.

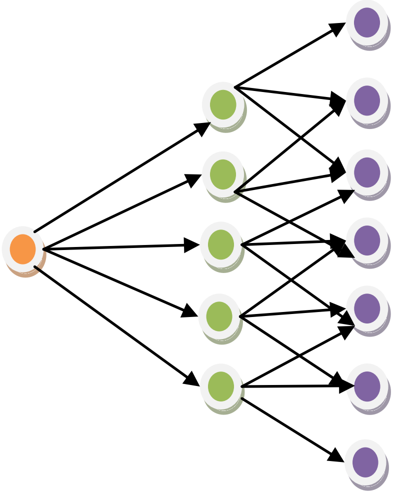
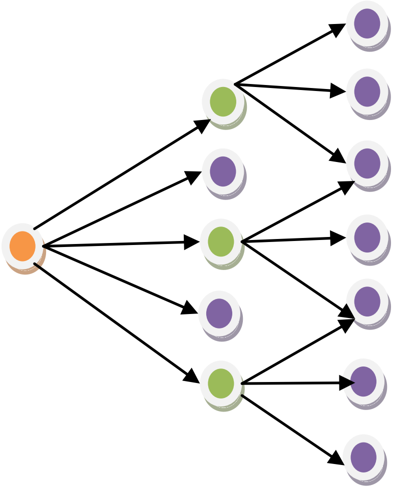


Fig 2.1.The broadcast from the leftmost node is retransmitted:

(a) by all its neighbors

The protocol is best suitable for large and dense network as the technique of MPRs works well in this context. A node selects MPRs from among its one hop neighbors with "symmetric", i.e., bi- Fig. 1 illustrates a node broadcast its messages throughout the network using standard flooding where all neighbors relay message transmitted by the leftmost node and MPR flooding where only MPR nodes relay the message. directional, links. Therefore, selecting the route through MPRs automatically avoids the problems associated with data packet transfer over uni-directional links. In OLSR protocol, two types of routing message are used, namely, HELLO message and TC message. A HELLO message is the message that is used for neighbor sensing and MPR selection.



(b) by its MPRs only.

A. *Network Model*

We assume a large mobile ad-hoc network (MANET) that consists of a number of wireless nodes with moving ability (each node is free to move in any direction). Each node has the ability to store, process and relay packets to other nodes if it receives packets that are not for its own use.

B. *Neighbourhood Discovery*

Control traffic in OLSR is exchanged through two different types of messages: "HELLO" and "TC" messages. HELLO messages are exchanged periodically among neighbour nodes, in order to detect links to neighbors, to detect the identity of neighbors and to signal MPR selection. TC messages are periodically flooded to the entire network, in order to signal link state information to all nodes.

- *HELLO messages*

HELLO messages are emitted periodically by a node, including its own address as well as encoding three lists: a list of neighbors, from which control traffic has been heard (but where bi-directionality is not yet confirmed), a list of neighbor nodes, with which bidirectional communication has been established, and a list of neighbor nodes, which have been selected to act as MPR for the originator of the HELLO message. HELLO messages are exchanged between neighbor nodes only.

Upon receiving a HELLO message, a node examines the lists of addresses. If its own address is included, it is confirmed that bi-directional communication is possible between the originator and the recipient of the HELLO message. When a link is confirmed as bi-directional, this is advertised periodically by a node with a corresponding link status of "symmetric". In addition to information about neighbor nodes, periodic exchange of HELLO messages allows each node to maintain information describing the links between neighbor nodes and nodes which are two hops away. This information is recorded in a nodes 2-hop neighbor set and is explicitly utilized for the MPR optimization the core optimization of OLSR.

- *TC messages*

Like HELLO messages, TC messages are emitted periodically by a node. The purpose of a TC message is to diffuse topological information to the entire network. Thus, TC message contains a set of bi-directional links between a node and a subset of its neighbors. For a discussion on the selection of which neighbors to include in the TC messages to provide sufficient topology information, TC messages are diffused to the entire network, employing the MPR optimization

C. *Multipoint Relays Selection*

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 constructs the MPR set which includes the minimum number of its 1-hop neighbors which it is possible to reach the node's all 2-hop neighbors. Each node also maintains information about the set of neighbors that have selected it as a 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.

D. *Topology Diffusion*

In order to disseminate the topology information, the nodes that were selected as MPR must send the topology control (TC) message. The TC messages are the messages 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 nodes' MPR set and hence obtains knowledge of the whole network topology. Based on these topology, the nodes are able to calculate routing table.

III. ROUTING ATTACKS

In MANETs every node participates in the routing process. Hence, it is possible for attackers to launch attacks against the routing protocol by sending false routing information. The possibility of such attacks was already mentioned in. In these attacks against the routing protocol are referred to as routing disruption attacks. By sending false routing information, an attacker may try to dispose other nodes to make him a part of their routes. This is often referred to as 'route attraction'. If an attacker succeeds in attracting routes, he may perform several attacks including

- Node isolation attack
- Colluding attack
- Collusion attack
- Launching a denial-of-service (DOS) attack

A. *Node Isolation Attack*

Here we present a Node Isolation attack which can result in denial-of-service against OLSR protocol. The goal of this attack is to isolate a 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.

In this attack, attacker creates virtual links by sending fake HELLO messages including the address list of target node's 2-hop neighbors, (the attacker can learn its 2-hop neighbors by analyzing TC message of its 1-hop neighbors). According to the protocol, the target node will select attacker to be its only MPR. Thus, the only node that must forward and generate TC messages for the target node is the attacking node. 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 more than two hops away from a target node 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.

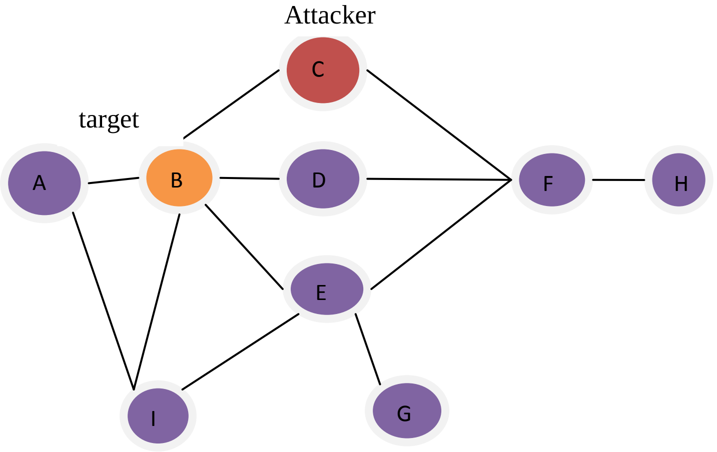


Fig 3.1 Node Isolation attack (a) topology perceived by Node H before the attack

In the figure 3.1 (a) Node C is the attacking node, and Node B is the target node. Instead of sending correct HELLO message that contain {B, F} in neighbor address list, the attacker sends a fake HELLO message that contains {B,F,G,Z} which includes the target node's 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 onl

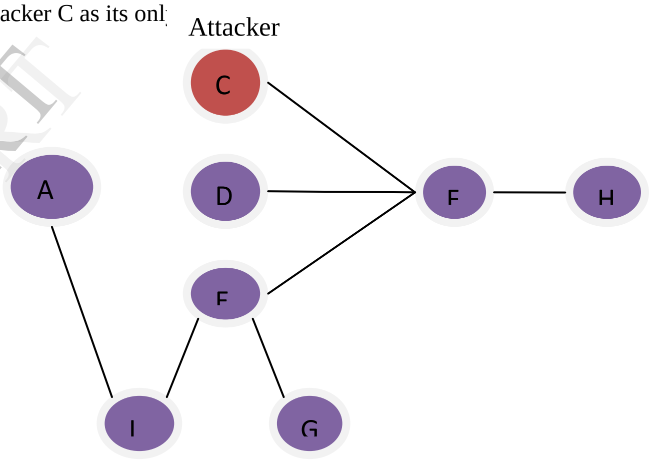


Fig 3.1 (b) Topology perceived by Node H after the attack.

Being Node B's the only MPR, the attacker refuses 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 to build route to Node B. As a result, other nodes would not be able to send data to Node B. Despite being in the network, the target node B will be isolated from the network. An attacker can launch this attack, as long as the target node is within its transmission range.

B. *Colluding Injected Attack*

Colluding injected attack (CIA) works in MANET. CIA attack is launched after finishing two consecutive phases. First is, the node replication phase, in which the adversary will compromise an arbitrary node and then inject a replication node of the compromised node in the network. The second phase is the node injection phase, in which the adversary will inject another node that will work with the injected replicated node to restrict an arbitrary node's ability of receiving and relaying any packet. By doing this, a legitimate node (the attacked node) might be reported as being malicious by any watchdog node if they existed in the neighborhood, since they will not hear any forwards from the attacked node.

Moreover, in reliable networks, (where the source node needs a conformation ACK packet from the destination to make sure that it receives the packet), if the attacked node is a destination node of an arbitrary communication, due to its inability of receiving any packet, the source node might timeout before receiving any ACK from the destination node, thus may conclude that this destination node in unreachable.

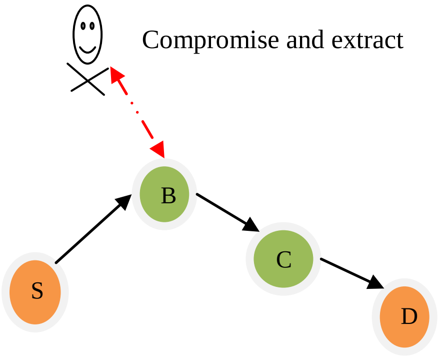


Fig 3.2 (a) The adversary compromised a node

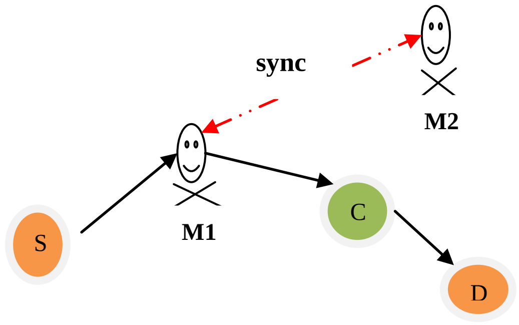


Fig 3.2 (b) Node injection phase

C. *Collusion Attack Against EOLSR Protocol*

Collusion Attack is an attack against Mobile Ad Hoc Networks and is based on Optimized Link State Routing (OLSR) Protocol. In this attack, two attacking nodes collude to prevent routes to a target node from being established in the network.

Topology information from TC messages is stored and processed by nodes to build routes to destinations that are more than 2-hops away from it [2]. In the collusion attack, the misbehaving nodes do not forward topology information related to the target node. This prevents routes to the target node from being established. As already stated, OLSR specifies that topology information (TC messages) is to be forwarded only by MPR nodes. Thus the necessary condition for the attack is that misbehaving nodes be MPR nodes.

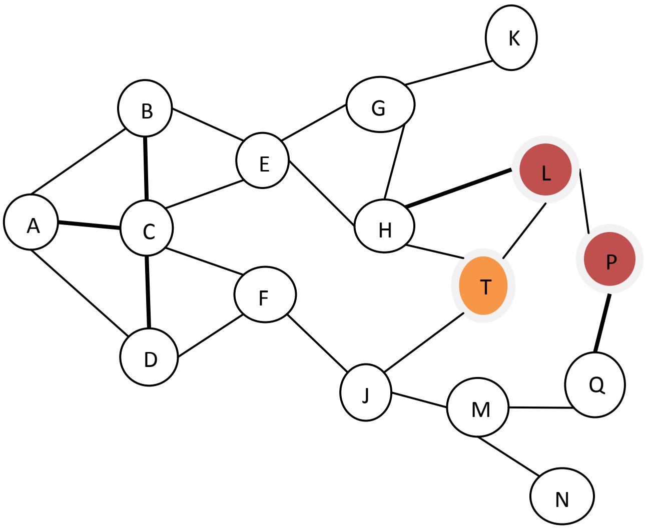


Fig 3.3 (a) A sample MANET. Node T is the target. Nodes L and P are colluding attackers

The network in Figure 3.3 (a). Let the misbehaving nodes (attackers) be *L* and *P* and let *T* be the target node. In this attack, the first attacker, node *L*, uses a HELLO message to announce symmetric 1-hop links to all the 2-hop neighbours of the target node *T*. As per the MPR Computation algorithm, *T* selects *L* as its MPR node. After being selected as an MPR node for T, the first attacker *L* chooses *P* as its own MPR node. This implies that all the TC messages generated by *L* are to be forwarded only by *P*. TC messages generated by *L* listing *T* as its MPR selector are dropped by *P*, the second attacker. No TC messages with information about the target node *T* are disseminated into the network. The result is that no node in the network will contain any topology tuple with information regarding *T*. Routes to *T* cannot be established by nodes more than 2-hops away from *T*. The effect of the attack is shown in Figure 3.3 (b).

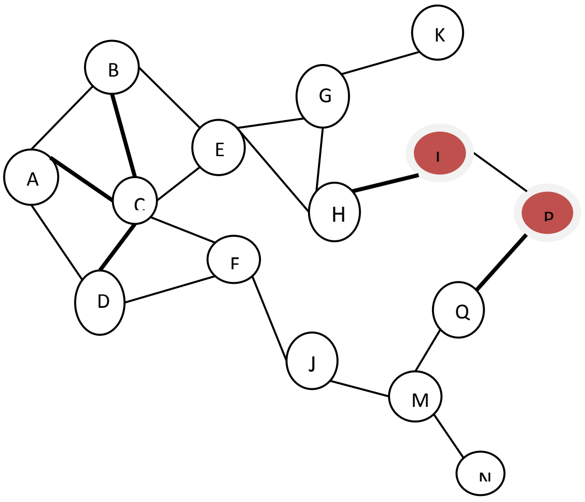


Fig 3.3 (b) Network Topology as seen by nodes beyond 2-hops distance from T, namely, A, B, C, D, E, F, G, K, Q, N

The authors propose to detect Collusion Attack by including a node’s 2-hop neighbourhood information in HELLO messages. This allows a node to have knowledge of its 3-hop neighbors’ without the need of TC messages and to verify information sent by neighbors. Though the proposed method detects an attack, it cannot differentiate between mobility induced topology changes and the collusion attack. This result in a significant amount of false positives. The authors in

[3] propose incorporation of an information theoretic trust framework in OLSR to detect and act against Collusion Attack. Nodes cooperate to calculate trust values of other nodes, which leads to a blacklisting process after a certain threshold. This method involves maintaining extra data structures for storing the trust values at each node. Furthermore, the method requires cooperation of neigh boring nodes to arrive at correct results.

IV. RELATED WORK

In [4], the authors address the problem of Collusion attack in OLSR using an acknowledgement (ACK) based mechanism to detect malicious nodes, so that they are excluded from the forwarding process. This scheme has a considerable overhead induced by the extra control messages. In [5], the authors provide an analysis of the Node Isolation Attack, a version of Collusion Attack involving a single attacker. In the detection phase of the proposed countermeasure [5], the target observes its MPR node to check if it is generating TC messages.

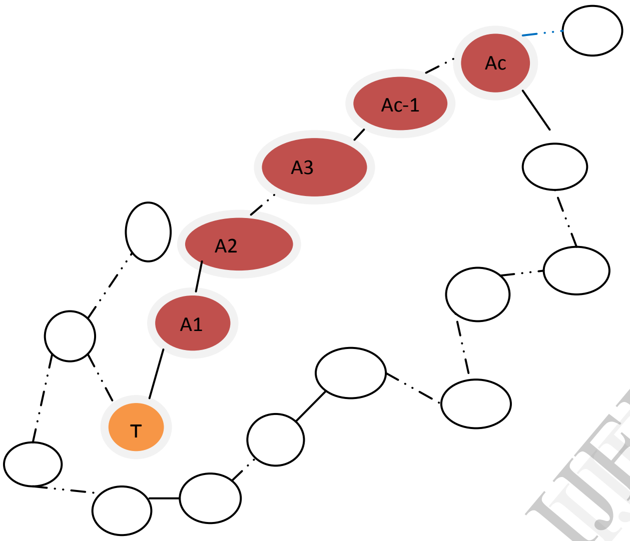


Fig 5. Collusion attack chain A1 to Ac targeting T

This approach fails against the Collusion Attack because it is the second attacker that drops packets and this attacker may be outside the target's range. The example of collusion attack extended upto any number of colluding attackers.

V. CONCLUSION

This paper proposes a solution for node isolation attack and colluding attack launched against OLSR routing protocol. Here, we have discussed through an attack model, that it is easy for a malicious node to launch the node isolation attack to isolate an OLSR MANET node. This attack allows at least one attacker to prevent a specific node from receiving data packets from other nodes that are more than two hops away. The proposed solution called EOLSR, which is based on OLSR, uses a simple verification scheme of hello packets coming from neighbor nodes to detect the malicious nodes in the network. Colluding injected attack CIA) will work together to launch a colluding attack to create collusion an arbitrary node in the network, to restrict its ability of receiving any packet, or relaying any packet. Collusion attack in which the first attacker creates fake link to make packets route to itself while letting the second attacker to misuse the packet. The simulation result showed that the attack can have a devastating impact on the OLSR MANET. After analyzed the attack, we have presented a simple mechanism to detect the attack by adding the address of 2-hop neighbors in HELLO message. Our future work will be focused on implementing the proposed mechanism and evaluating its effectiveness as well as finding an efficient solution to avoid the attack. Moreover, cooperative or colluding attack can be launched, because our technique doesn't employ any promiscuous listening of neighbor nodes for detecting the attackers.

REFERENCES

1. B. Kannhavong, H. Nakayama, and A. Jamal pour, "A survey of routing at- tacks in mobile ad hoc networks," IEEE trans. Wireless Commun., vol. 14, no. 5, pp. 85–91, Oct. 2007.
2. T. Clausen and P. Jacquet, "IETF RFC3626: Optimized link state routing protocol (OLSR)," Experimental,2003.
3. T.Clausen and U.Herberg, "Security issues in the optimized link state routing protocol version 2(OLSRv2)," Int. J. Netw. Security Appl., 2010.
4. B.Kannhavong, H. Nakayama and A. Jamal pour, "A study of routing attack in OLSR-based mobile ad hoc networks," Int. J. Commun. Syst., 2007.
5. B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against OLSR-based mobile ad hoc network," in Proc. ISCN, 2006, pp. 30–35.
6. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Securing the OLSR protocol," in Proc. Ad-Hoc-Net, 2003.
7. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An advanced signa- ture system for OLSR," in Proc. ACM SASN, 2004.
8. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for security," in Proc. OLSR Interop and Workshop, 2005.
9. C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, and D. Raffo, "Secur- ing the OLSR routing protocol with or without compromised nodes in the network," HIPERCOM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494, Feb. 2005.
10. D. Dhillon, T. S. Randhawa, M. Wang, and L. Lamont, "Implementing a fully distributed certificate autority in an OLSR MANET," in Proc. IEEE WCNC, 2004.
11. D. Dhillon, J. Zhu, J. Richards, and T. Randhawa,"Implementation &evaluation of an IDS to safeguard OLSR integrity in MANETs," in Proc. IWCMC, 2006.
12. A. J. P. Vilela and J. Barros, "A cooperative security scheme for optimized link state routing in mobile ad-hoc networks," in Proc. IST MWCS, 2006.
13. A. Adnane, R. de Sousa, C. Bidan, and L. Mé, "Analysis of the implicit trust within the OLSR protocol," in Proc. IFIP, 2007.
14. X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A library for parallel simulation of large-scale wireless networks," in Proc. PADS, 1998.
15. D. Raffo, "Security schemes fo the OLSR protocol for ad hoc networks," Ph.D. dissertation,
Univ. Paris, 2005
16. M. Mohanapriya and S. Urmila, "A novel technique for defending routing attacks in OLSR MANET,"
in Proc. IEEE ICCIC, 2010.