Proceedings published by International Journal of Computer Applications® (IJCA)
International Conference on Computer Communication and Networks CSI- COMNET-2011

Vulnerabilities, Attacks and their Detection Techniques in Ad hoc Network

Rauki Yadav
Department of Computer Science, Suresh Gyan Vihar University, Rajasthan, India

Naveen Hemrajani
Department of Computer Science, Suresh Gyan Vihar University, Rajasthan, India

Dinesh Goyal,Savita Shiwani
Department of Computer Science, Suresh Gyan Vihar University, Rajasthan, India

ABSTRACT
The aim of this Paper is to study the performance of the OLSR protocol. This paper is about security issues in OLSR. There are many ways a malicious node can exploit the vulnerabilities to launch attack on network. OLSR is a proactive routing protocol, Control packets has been send by OLSR to build and update the topology. As a part of this paper I have simulated a new attack method against OLSR based ad-hoc networks named as detour attack. Initially the attack is simulated with one attacker then with multiple attacks and the overall performance of network is observed under attack as well as normal conditions .The observations are made with different set of topologies and for different positions of attacking nodes. Finally a detection technique is proposed to detect the presence of an attacker node carrying out Detour attack.

Keywords
Wireless networks, Routing Protocol, Ad hoc network, multi point relay, Security, Attacks.

1. INTRODUCTION
The most common applications of wireless networks are Group Standard for Mobile communications(GSM) and Wireless Local Area Network(WLAN). Nodes are not arranged in any particular fashion in such networks.So to ensure better communication in between nodes, some routing protocols has been developed for such networks. These protocols also help to utilize the resources optimally. Optimized Link State Routing (OLSR) protocol is one example of such protocols. There are some vulnerabilities in OLSR,. In this Paper a study of attack against OLSR have been presented. I have simulated detour attack and have observed the impact with different simulation parameters.

1.1 Ad hoc Network
An ad hoc network is basically a collection of wireless nodes not having a permanent network. They are without any fixed infrastructure like access points or base stations. In ad hoc networks every node is willing to forward data for other nodes, and which nodes forward data is decided dynamically based on the network connectivity. The term 'ad hoc' implies that the network is structured for a special, sometimes exclusive service designed for specific applications (eg, disaster recovery, battlefield).In ad hoc networks the communication is organized completely decentralized. To regulate or control the traffic there is no central authority. A node can be receiving and origination network traffic, also forwarding traffic on behalf of other nodes. And this kind of act can be performed by all nodes at the same time. The environment may change dynamically and the application can me mobile as well,so it is so obvious that topology also keeps on changing. Due to their flexibility and special nature, ad hoc networks are advantageous in different environments [3]. An example ad hoc network is shown in the figure 1 shown below:

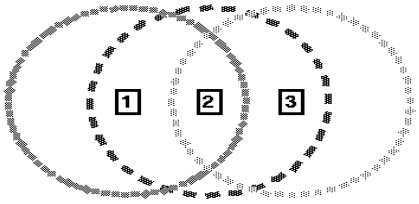

Figure 1: Ad hoc network of three wireless mobile hosts.

1.1.1 Attacks in Ad Hoc Networks
The quality of connection becomes poor which results in decrease in network performance.

- A malicious node sends false route updates due to that route failures occur frequently and hence network performance degrades.
- A malicious node captures a packet and reduces its time-to-live (TTL) so that it gets dropped before its destination.
- A node can redirect the traffic by sending false route information which may lead to poor resource consumption and finally degraded performance.
- A malicious node isolates a particular node form other nodes present in the network. The key concept is to prevent a node's information to be spread into the network. So other nodes will not be aware of presence of that node and hence won t be able to send data to this node

2. ROUTING IN AD HOC NETWORKS

The few categories for ad hoc routing protocols are shown in Figure 2.

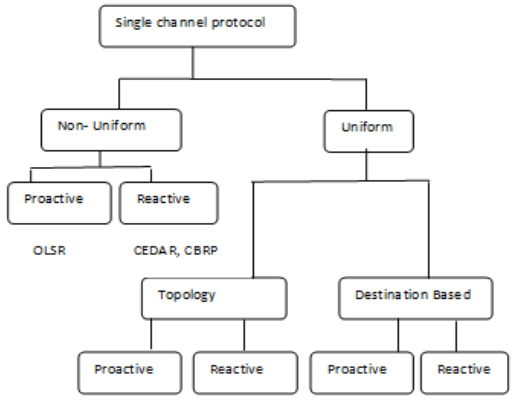

Figure 2: Classification of ad hoc routing protocols.

2.1 Scheduling Based Routing Protocols

On the basis of scheduling, routing protocols can be divided into two parts: Reactive protocols and Proactive protocols.

2.1.1 Reactive Protocols

Reactive protocols determine the route to a destination on demand. If a communication is about to be set up and no route to the destination is already known, route discovery process is initialized. A route request packet is usually flooded through the network. When this packet either reaches a node with a route to the destination or the destination itself, a route reply is sent back to the source node either by link reversal or through flooding of the route reply packet. Routing occurs either in form of source routing or hop by hop.

2.1.2 Proactive Routing

Proactive Routing uses a table driven approach. Each node maintains routing information about other nodes present in the network. This information is usually stored in a number of different tables. These tables are updated periodically or whenever there is a change detected in the network. What information is to be kept and how it is to be exchanged depends upon the used routing protocols.

3. OLSR DESCRIPTION

The Optimized Link State Routing Protocol (OLSR) is an optimized version of the pure link state protocol. The main focus is at the IP layer functions. OLSR is designed for MANETs. It is a proactive protocol which is table driven. In this protocol, a node exchanges the information about network topology from other nodes at regular intervals. The MPR nodes announce this information periodically in topology control (TC) messages. In this way, a node tells the network, that it has connectivity with the nodes which have selected it as an MPR. MPRs is route calculation to form the route from a given source node to any destination node in the network. The MPRs are used by the protocol to ensure efficient flooding of control messages within the network. In wireless ad hoc networks, we use different notion of a link,packets can go out the same interface; therefore, a different approach is required to optimize the flooding process. At each node, the OLSR protocol discovers 2-hop neighbor information by using Hello messages. Then a set of MPRs (Multipoint relays) is elected. The MPRs are selected in by any node such a way that there exists a path between the selecting node and each of its 2-hop neighbors through the selected MPR. Now TC messages are forwarded by these MPRs which contain the information about MPR selectors. All these functioning of MPRs makes OLSR stand away from other link state routing protocols in following ways: All nodes do not share the TC message forwarding path, it varies depending on the source.

4. RELATED WORK

4.1 Attacks Against Ad Hoc Networks

In [6] describes Denials of Service (DoS) attacks on Wireless ad hoc networks. Also the authors propose possible solutions for the attacks. Both the routing layer and MAC layer vulnerabilities are discussed. The attacks discussed are periodic drop, route failure and replay attack.In [9] authors has proposed a security mechanism against Byzantine attack and wormhole attack on MANETs. In [16]Authors has pointed out the main areas where ad hoc networks lack in security mechanism. A simulation based study is presented for the attacks.[17] divides DoS attacks in two major categories: routing disruption attack and resource consumption attack. Further they classify routing disruption attacks in three classes which are outsider attacks, insider attacks and protocolcompliant attacks.

4.2 Attacks Against OLSR Protocol

In [14],[20] the authors has discussed about the security issues in routing protocols.They talk about possibilities of different types of attacks on ad hoc routing protocols. They have classified the threats as modification, impersonation, and fabrication exploits. The vulnerabilities of such protocols are discussed, possible attacks and then a mechanism is proposed to make the routing protocol secure.In [7],[19] authors say that OLSR is vulnerable to attacks as security aspects has not been designed for OLSR. however there is still requirement of strong and efficient mechanism for detection and response against inside intruders. They have designed an intrusion detection system for OLSR which prevent the inside authorized nodes from compromising the security of MANETs.In [18] author propose a intrusion detection system based version of OLSR called as CCIDS OLSR which can detect link spoofing, link deletion.

5. OLSR VULNERABILITY

OLSR is responsible for suggesting routes to forward traffic. And this task is performed using Multi Point Relay (MPR). MPRs are selected for every node and control messages are broadcast using these MPRs. Using control messages network topology information is spread to each node across the network. Thus each node comes to know about network topology information. At each node a topology table is maintained to keep track of the route to be taken in order to forward data/control packets. In wired networks, at various layers, security systems have already been implemented. In ad hoc networks, where medium is wireless, every node work as a router. Since data passes through nodes, any node can tamper the control packet or data packet. Thus a node is capable of changing route information contained in control messages as well as deleting or modifying data packets. So we need to have security mechanism .Routing protocols in ad hoc networks are vulnerable . And

presence of a mis-behaving/malicious node is difficult to detect as ad hoc networks are distributed, dynamic in nature and they are not centralized. This leaves ad hoc networks open for attackers to attack.

6. DETOUR ATTACK AND DETECTION

6.1 Proposed Attack Methodology

In this attack method a malicious node first collects information about network. Then it updates its own link table with wrong information about its neighbours. All nodes which receive this information, update their routing tables according to the false information sent by the malicious node. Now incorrect routes are selected to forward data packet, which result in packets being dropped.

6.1.1 Gathering Network Information

In OLSR, at every node several repositories are maintained to provide information about the network topology. Every node maintains a routing table using which routes to other nodes present in topology are decided. Similarly there are repositories which keep information about 1-hop and 2-hop neighbors of a node.In order to launch detour attack a malicious node collects the following information about network from various repositories:

1. Total number of nodes present in topology.

2. Information about all its 1-hop neighbors.

3. All its 2-hop neighbors.

4. Status of links with its neighbor nodes.

6.1.2 Updating Own Topology Information

A grid topology having 25 nodes is shown in figure 3. Here assume attacker node is N 13.Thus N8, N12,N14,N18 are 1 hop neighbors of the attacking node and N3, N7,N9, N11, N15, N17, N19,N23 are 2 hop neighbour.Similarly if attacker node is N14, then 1 hop neighbor is N9, N13, N15,N19 and 2 hop neighbors are N4, N8, N10, N12, N18, N20, N24. It is clear that none of the 2-hop neighbors of N13 is a 2-hop neighbor of N14.

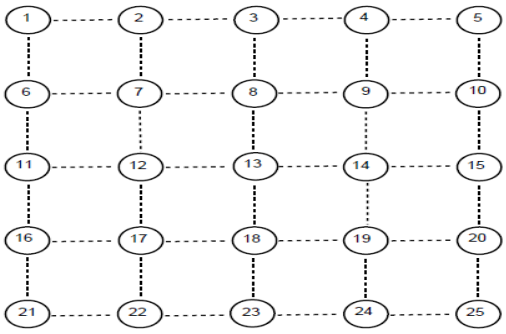

Figure 3. A grid topology having 25 nodes(5*5)

6.1.3 Broadcast Wrong Topology Information

The malicious node has updates its own link tuple with wrong information, this wrong information is broadcast to its 1-hop neighbor nodes. These nodes update their repositories with wrong information. Since according to the new information all their 2-hop neighbors are covered by the malicious node, they are forced to choose the malicious node as its MPR according to OLSR conventions. Once a malicious node becomes MPR, it is ensured that most of the traffic is forwarded via this node.

6.1.4 Effect on Network

When malicious node has become MPR, most of the traffic will be forwarded through this node only. And since it has updates its own link table with fake network information, every time a route is required, the link table is referred, most of the times it returns the destined node present at 1-hop distance only .Eventually the drop in data packets gets increased significantly which decreases network performance.

7. SIMULATION PARAMETERS AND SCENARIOS

We conducted our simulation using NS-2 simulator, a scalable simulation environment for wireless network systems .In my simulation the convergence time is taken as 30 seconds, so that each node is aware of all of its neighbors. Number of nodes are between 16 to 49 for simulated network. The attacker node waits for its information repositories to be filled with network information. Once all the repositories are full, it starts filling its own repositories with fake information about its 1-hop neighbors.. As a result incorrect information is spread into the network and malicious node is selected as MPR by all its 1-hop neighbors.. After 30 seconds data packets are send from source to sink. Because of incorrect routing information , once a data packet reaches to attacker node, it gets dropped due to unavailability of physical link between attacker and the sink. Table 7.1 shows the simulation parameter.

Table 7.1 simulation parameter

Simulation	NS 2
Topology	Grid(n* n)
Packet size	1024 byte
Protocol	OLSR
Packet generation rate	2^4 packet per minute
Medium	wireless
Distance between nodes	50 meters
Convergence time	30 sec
Channel capacity	1 Gbps

In Figure 4 we shows the scenario of number of packets delivered to sink in normal as well as attack condition. The occurrence of a data packet at sink for no attack is shown by vertical linespots with dotted line, while that of under attack condition is represented by vertical bars. Time is taken on X-axis while on Y-axis, a 0 means packet drop and 1 means packet received. One can observe from the graph that in normal condition all the packets were delivered to sink, while in attack condition only a small fraction of total packets sent reached the sink.Figure 5 shows the impact of attack with different number of nodes in the network. As discussed above the effect of attack reduces with increase in the topology size, which can be observed form the figure as well. It is clear that as we increase the topology size, the number of packets dropped decrease.

It is clear from the graphs that in no attack situation, all the packets are received by the sink normally. Under attack circumstances, the number of packets received by the sink

decreases by a huge difference.This scenario is for single attacker as in shown in figure5.

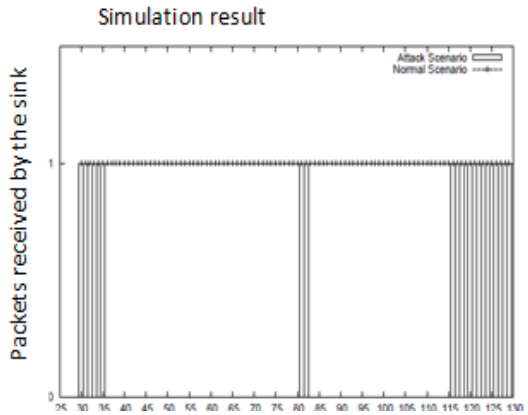

Figure-4 Packets Received by sink in both attack and no attack situations.

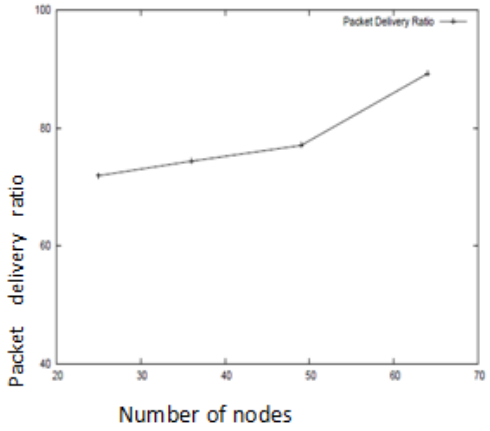

Figure 5 Packet Delivery Ratio with different topologies.

For 2 attacker node, we chose a node as source node while 2 attacker nodes were chosen. From source node 100 packets were sent to each remaining node present in the network in normal condition as well as under attack condition. The attack was simulated in 2 conditions with 2 attackers. In first condition both the attackers are taken at a minimum distance of 4 hopes from each other. In second situation both the attackers were placed at a distance of 2 hops from each other.For small topology the impact of attack is same as in the case of both the attackers were distant from each other. But for larger topology size such as for large topology it seems that the attack works as if there was only one attacker. For more comparative study let us have a look at the graph (Figure 6).

In both the cases, when attacker nodes are close to each other and when they are distant to each other. Its understood from graph that for small topology, both the attack simulations produce somehow similar impact. In case of large topology, close attacking positions of attackers makes the attack as if only 1 attacker was present, while in case of distant attackers there a large drop in PDR as shown in graph.Further the same attack was carried out in the presence of 3 attacker nodes. In case of 3 attack it was observed that the attack makes much more impact on PDR in case of larger topologies also. In previous cases we observed that attack was more effective for smaller topologies than for larger topologies, whereas with 3 attacker nodes the attack is equally effective and severe in case of large topologies as well as smaller topologies.

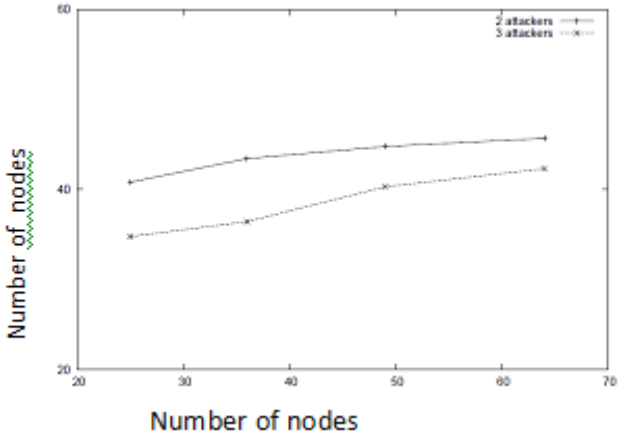

Figure 6: PDR comparison with 1 attacker and 2 attackers (Close to each other).

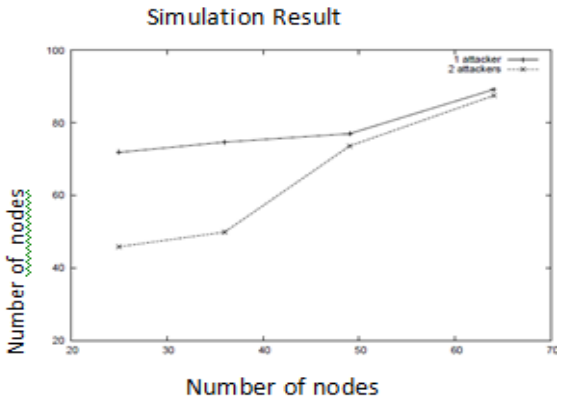

Figure 7: Comparison of PDR in case of 2 attackers (having different distances).

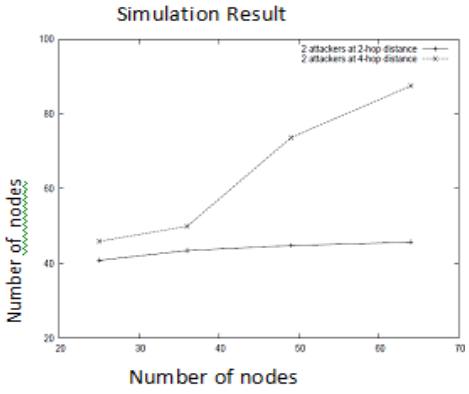

Figure 8: PDR comparison in presence of 2 attackers & 3 attackers.

8. PROPOSED DETECTION TECHNIQUE

In order to detect the presence of a malicious node in the network, the set of MPRs is observed for every node. This observation is carried out every 5 seconds as new TC messages are generated and broadcast after every such interval. Now if for a particular node, if a node is becoming its MPR almost all the times, while remaining MPR set keeps on changing, then this MPR node can be an attacker. We maintain a count of occurrence of that node being selected as MPR. If the count exceeds a threshold value within a finite period of time, this node is an attacker which is performing malicious activities.

9. CONCLUSION AND FUTURE WORK

OLSR is vulnerable to attacks. Specially it is prone to routing misbehavior attacks. As we see that in networks based on OLSR an insider node can easily be compromised and many kind of attacks can easily be launched. Though many secure versions have been proposed at time to time, but only few threats were considered each time. So a secure version of OLSR is still needed which can detect and remove at least a certain class of attacks. As far as the proposed attack (Detour attack) is concerned, a counter-measure is to be designed to remove the attack completely. However routing misbehaviour attacks have been carried out in past as well and some detection techniques as well as counter measures are also present, but in detour attack the method is slightly different, so there has to be some different countermeasure. Like wise some new attack methodology can be designed to carry out attack on OLSR, so that detection and countermeasure techniques can be designed in order to make OLSR a more secure routing protocol.

10. REFERENCES

[1] nS3: http://www.nsnam.org/, 2011.

[2] I. Aad, J.-P. Hubaux, and E.W. Knightly. Impact of denial of service attacks on ad hoc networks. Networking, IEEE/ACM Transactions on, 16(4):791 –802, aug. 2008.

[3] M.S. Corson and J.P. Macker. Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations, 1998.

[4] S. Deering and R. Hinden. Rfc2460 - internet protocol, version 6 (ipv6) specification, standards track edition, 1998.

[5] Paul Muhlethaler Adjih Cedric, Daniele Raffo. Attack against olsr: Distributed key management for security.

[6] V. Gupta, S. Krishnamurthy, and M. Faloutsos. Denial of service attacks at the mac layer in wireless ad hoc networks. In MILCOM 2002. Proceedings,volume 2, pages 1118 – 1123 vol.2.

[7] M. Wang, L. Lamont, P. Mason, and M. Gorlatova. An effective intrusion detection approach for olsr manet protocol. In Secure Network Protocols, 2005. (NPSec). 1st IEEE ICNP Workshop on, pages 55 – 60, nov. 2005.

[8] P. Jacquet and T. Clausen. Optimized link state routing protocol (olsr), rfc 3626, 2003.

[9] John S. Baras, Svetlana Radosavac, George Theodorakopoulos, Dan Sterne, Peter Budulas, and Richard Gopaul. Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in olsr. In Military Communications Conference, 2007. MILCOM 2007. IEEE, pages 1 –7, oct. 2007.

[10] Thomas Clausen and Ulrich Herberg. Vulnerability analysis of the optimized link state routing protocol version 2 (olsrv2). In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on, pages 628 –633, june 2010.

[11] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks. In MultiTopic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, pages 62 – 68, 2001.

[12] W.W. Brown, IV Marano, V., W.H. MacCorkell, and T. Krout. Future combat system-scalable mobile network demonstration performance and validation results. In Military Communications Conference, 2003. MILCOM 2003.IEEE, volume 2, pages 1286 – 1291 Vol.2, oct. 2003.

[13] F. Templin, R. Ogier, and M. Lewis. tbrpf rfc3684, experimental edition,February 2004.

[14] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. A secure routing protocol for ad hoc networks. In Network Protocols, 2002.Proceedings. 10th IEEE International Conference on, pages 78 – 87, nov.2002.

[15] University of Southern California Information Sciences Institute. Rfc791 internet protocol, 1981.

[16] Hoang Lan Nguyen and Uyen Trang Nguyen. Study of different types of attacks on multicast in mobile ad hoc networks. In Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on, page 149, april 2006.

[17] Ruiliang Chen, M. Snow, Jung-Min Park, M.T. Refaei, and M. Eltoweissy Nis02-3: Defense against routing disruption attacks in mobile ad hoc networks. In Global Telecommunications Conference, 2006. GLOBECOM '06.IEEE, pages 1 –5, 27 2006-dec. 1 2006.

[18] Da Zhang and Chai Kiat Yeo. A novel architecture of intrusion detection system. In Consumer Communications and Networking Conference (CCNC),2010 7th IEEE, pages 1 –5, jan. 2010.

[19] J. Orset and A. Cavalli. A security model for olsr manet protocol. In Mobile Data Management, 2006. MDM 2006. 7th International Conference on, page 122, may 2006.

[20] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour. Analysis of the node isolation attack against olsr-based mobile ad hoc networks. In Computer Networks, 2006 International Symposium on, pages 30–35.