International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013
ISSN 2229-5518

Vulnerability Discovery and Mitigation in OLSR of Mobile Ad-hoc networks

Sd Salman Ali[1], Dr. G. Manoj Someswar[2]

[1] PhD Scholar, Pacific Academy of Higher Education and Research University, Udaipur. India.
E-mail: ssali.508@gmail.com.
[2] Principal and Professor in CSED, Anwarul- uloom College of Engineering and Technology, Hyderabad. India.
E-mail: manojgelli@yahoo.co.in.

Abstract: Mobile ad hoc networks (MANET) are formed by a group of mobile nodes connected by using wireless networks without the need of a fixed infrastructure. They can communicate to each other by direct peer-to-peer wireless communication when they are close to each other or otherwise they user multi-hop paths. Due to its, node mobility support, decentralized architecture and dynamic routing capabilities MANETs are envisioned to become a stand-alone network for a group of mobile users. Although several routing protocols have been introduced in MANET's for efficient routing and scalable performance, Optimized Link State Routing (OLSR)received particular attention recently. In order to reduce the traffic messages flood in MANET's, OLSR uses Multipoint Relays (MPRs) as an internal mechanism. A lot of research on OLSR reveals various vulnerabilities and security issues. In this paper we are introducing some secure and robust methodologies to mitigate security attacks on OLSR and its MPR's. To overcome control traffic attacks and to reduce the overhead generated by redundant control messages we implemented k-robust-MPR selection process. Experimental simulation shows that our methodologies are useful and approach is very secure, robust and scalable for routing in mobile ad hoc networks.

Keywords: MANET's, Link State Routing, Multipoint Relays, Routing, k-Robust-MPR selection

I. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing - catering to both nomadic and fixed users, anytime and anywhere. Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure.

In a Mobile Ad Hoc Network (MANET),the network topology may change dynamically since nodes can move in an unpredictable manner [9,3]. Nodes are free to move at any speed in any direction and join or leave the network at any time. Nodes with heterogeneous capabilities (e.g., transmission range) can coexist. In [3] a MANET as an autonomous system of nodes or Mobile Stations (MSs) connected by a wireless medium. This network maybe modeled in the form of an arbitrary communication graph. In a MANET, every node is able to communicate directly with other nodes within its range. Nodes with direct communication are called neighbors. Any pair of nodes not directly connected, can communicate through a path formed by other nodes. MANETs are basically peer-to-peer, multi hop wireless networks [4]. The established links can be either symmetric or asymmetric. Information packets are transmitted in a store-and-forward manner by intermediate nodes, i.e., every node acts as a router. In a MANET, every node configures its network address and can resolve the way to reach any destination..Fig. 1, shows an example of a network in ad hoc mode.

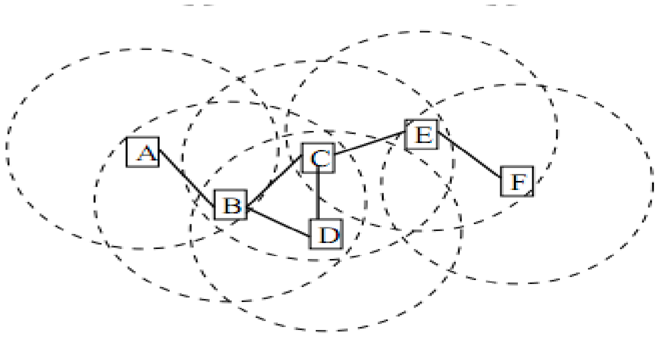


Fig.1.Example of Ad-hoc Multi hop

Routing is an important issue in MANETs. Efficient resources utilization is necessary due to the restricted capabilities of nodes. In a MANET, route computation must be distributed, as centralized routing in a dynamic network is not possible. Nodes only have a local knowledge of the network. An efficient and reliable routing strategy must consider the limited resources and being adaptable to the network conditions such as mobility, network size or traffic density. In Link State Routings (LSR) every node floods the network with the link-state information of its neighboring nodes. The OLSR protocol has received particular attention recently by research people because of its flexibility and adoptability. OLSR is defined in RFC 3626 [4].As many other routing protocols for MANETs, OLSR is not secure by design. The selection of the MPRs and exchange of topology control information are important vulnerability targets. Therefore, we use OLSR to show vulnerabilities in link-state routing protocols for MANETs and to implement our proposed countermeasures. This security risks and proposed solution [7] can be adapted to other proactive (or reactive) routing protocols for MANETs.

In this paper our contribution deals with the effect of control traffic attacks in OLSR networks and the selection of MPR sets with additional coverage to mitigate their effect [3]. The MPR selection with additional coverage is presented in RFC 3626 [6]; we name it k-Covered-MPR selection. However, additional coverage reduces the performance of the network due to additional control traffic information, i.e., Topology Control (TC) messages. We propose a k-Robust-MPR selection. In a k-Robust-MPR selection a node selects, when possible, k + 1 disjoint MPR sets to guarantee that even if k of the selected MPR sets become invalid, the remaining set is still a valid MPR set. Our proposed MPR selection offers equivalent protection against control traffic attacks also reducing the overhead generated by additional control traffic information.

II . Related Work

Several authors have contributed with cryptographic mechanisms to secure OLSR. Cryptographic mechanisms are proposed to enforce: integrity, authentication and confidentiality. Thus, public-key encryption is used for confidentiality, digital signature for integrity of the messages and digital certificates for authentication. However, the implementation of a Public Key Infrastructure (PKI) in MANETs is difficult due to the lack of a central authority (CA). Additionally, the efficient distribution of public and private keys is a challenging problem.

Optimized Link State Routing Protocol

The Optimized Link State Routing Protocol (OLSR) is developed for mobile ad hoc networks. The protocol is documented in the experimental Request for Comment (RFC) 3626. OLSR is table-driven and pro-active and utilizes an optimization called Multipoint Relaying for control traffic flooding.RFC3626 modularizes OLSR into core functionality, which is always required for the protocol to operate, and a set of auxiliary functions. OLSR uses an IP address as the unique identifier of nodes in the network. As OLSR is designed to be able to operate on nodes using multiple communication interfaces, every node must choose one IP address that is set to be its main address. OLSR can be used both with IP version 4(IPv4)[44] and version 6(IPv6)[28]. In an OLSR context the differences between IPv4 and IPv6 is the size of the IP addresses transmitted in control messages, the minimum size of messages and the address to use as destination for control traffic.

All OLSR control traffic is to be transmitted over UDP on port 698. This port is assigned to OLSR by the Internet Assigned Numbers Authority(IANA). The RFC states that this traffic is to be broadcasted when using IPv4, but no broadcast address is specified. When using IPv6 broadcast addresses does not exist, so even though it is not specified in the RFC, it is implicit understood that one must use a multicast address in this case. However, the OLSR protocol packet format allows for a wide variety of custom packets to be transmitted and flooded to the needs of the designer. OLSR will forward unknown packet types according to the default forwarding rule. The MPR optimization used in OLSR makes this possibility for message flooding a great asset to anyone in need of net-wide broadcasting of traffic in the ad-hoc network.

Multipoint Relaying

OLSR uses flooding of packets to diffuse topology information throughout the network. Flooding, in its simplest form, means that all nodes retransmit received packets. To avoid loops, a sequence number is usually carried in such packets. This sequence number is registered by receiving nodes to assure that a packet is only retransmitted once. If a node receives a packet with a sequence number lower or equal to the last registered retransmitted packet from the sender, the packet is not retransmitted. On wired networks other optimizations are usually added such as no retransmission on the interface on which a packet arrived. On a wireless multi-hop network however, it is essential that nodes retransmits packets on the same interface that it arrived, since this is the very nature of wireless multi-hop networks. This again causes every re-transmitter to actually receive a duplicate packet from every symmetric neighbor that re-transmits the packet. The concept of multipoint relaying is to reduce the number of duplicate retransmissions while forwarding a broadcast packet. This technique restricts the set of nodes retransmitting a packet from all nodes, to a subset of all nodes. The size of this subset depends on the topology of the network. This is achieved by selecting neighbors as Multipoint relays(MPRs). Every node calculates its own set of MPRs as a subset of its symmetric neighbor nodes chosen so that all 2 hop neighbors can be reached through a MPR. This means that for every node n in the network that can be reached from the local node by at minimum two symmetric hops, there must exist a MPR m so that n has a symmetric link to m and m is a symmetric neighbor of the local node.

III. VULNERABILITY DISCOVERY and MITIGATION in OLSR

Now a day’s OLSR become a popular routing protocol for MANET’s. In OLSR protocol in order to reflect the network topology efficiently every node should get and maintain the routing table at their level. All the nodes of network must contain the identical topology map for routing table construction. Therefore, the target of a misbehaving node may be that the nodes in the network (a) build inconsistent routing tables that do not reflect the accurate network topology, or (b) acquire an incomplete topology map. Attackers will found these existed intrusions information by using various Intrusion detection mechanisms and launch various attacks like Identity Spoofing, Link Spoofing, Reply Attack, Wormhole Attack and various Flooding Attacks on network topology. In Identity Spoofing the misbehaving node may generate false Hello or TC messages pretending to be a different node. In Link Spoofing a misbehaving node may generate Hello or TC messages including false links to other nodes in the network. In Reply Attacks a misbehaving node resends old valid TC or Hello messages. In Wormhole Attack an inexistent link can be created by one or more nodes by tunneling valid Hello messages without following the rules of the protocol.

Most of the previous researches [4,8,9] on OLSR given some better solutions to all above problems, but they failed to introduce a complete solution to overcome the most dangerous attacks under Flood Disruption Attacks. In link state routing protocols for MANETs, some attacks can be launched even in networks with either cryptographic capabilities or Vulnerability Discovery Systems (VDS). For example in OLSR exchange of control traffic information and the MPR selection process are important areas for attackers to attack.

3.1 Vulnerability Discovery in OLSR : In this paper we focused on Flood Disruption Attacks, which are the main target of an attacker is to disrupt the topology map acquisition process by disturbing the flooding of valid control traffic information. We are using Vulnerability Discovery Systems (VDS) in this research is WATCHERS (Watching for Anomalies in Transit Conservation: a Heuristic for Ensuring Router Security). When the VDS detects a malicious behavior, needs to notify other nodes in the network about the misbehaving node. Therefore some VDS protocols have been designed exclusively for MANETs. We classified the flooding attacks into two categories are i) incorrect MPR selection and ii) incorrect relaying process.

3.1.1 Incorrect MPR Selection: in this category, the malicious node either selects an in complete MPR set or forces other nodes to compute an incorrect MPR set. To launch the attack, the malicious node may either generate control traffic information with a false identity (i.e., identity spoofing) or report inexistent links to other nodes (i.e., link spoofing). As a consequence, the affected node computes an invalid MPR set,i.e., some of its two-hop neighbors are not covered through at least one node in its MPR set. Fig 2.a represents flooding disruption attack due to link spoofing, where node x spoofs links to nodes e and c. Node x sends Hello messages and looks like the best option to be selected as an MPR for node a. Node a receives the Hello messages from node x and computes incorrectly its MPR set by selecting node x as the only element to reach nodes e and c. Thus, all routing information do not reach nodes two hops away from node a. Fig 2.b represents flooding disruption attack due to the malicious node, where node a is forced to select node x as an MPR because is the only node to reach the inexistent node w. In the second case, a malicious node may disrupt the flooding of topology control information by misbehaving during the MPR selection process. Node x wants to be selected as the only MPR of node a. Then, it spoofs a link to node g and generates Hello messages announcing node g as a one-hop neighbor and its only MPR. From the perspective of node a, nodes c and g can be reached through node x. Then, node x is the best candidate to be selected as an MPR for node a. Thus, node x receives and forwards TC messages from node a. This attack exploits the source dependent requirement in OLSR to forward control traffic information. In this case, for nodes a, b, c and e, node x is not included in their selector table and they never forward any message from node x.

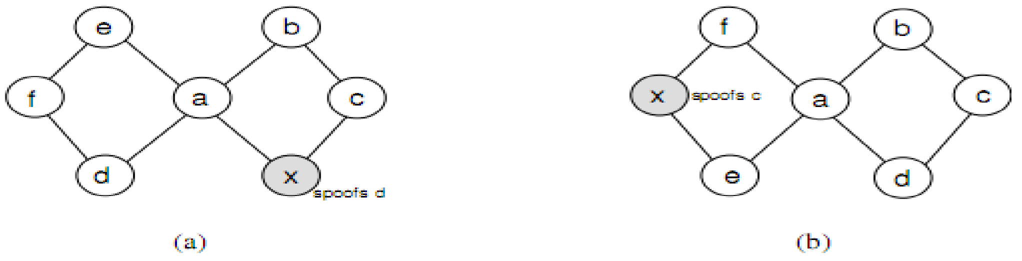


Fig 2.(a) flooding disruption attack due to link spoofing and (b) flooding disruption attack due to the malicious node.

3.1.2 Incorrect Relaying: In this attack a misbehaving node can disrupt the integrity of the network by either incorrectly generating or relaying control traffic information on behalf of other nodes. Consider x in Fig. 3(a) as a misbehaving node. Node x wants to be selected as the only MPR of node a. Then, it spoofs a link to node g and generates Hello messages announcing node g as a one-hop neighbor. From the perspective of node a, nodes c and g can be reached through node x. Thus, node x is selected by node as its only MPR and might perform the following incorrect behaviors: Selfish behavior or Slanderer behavior. In selfish behavior the attack is performed by a node that misbehaves and neither generates nor forwards TC messages. To increase the effectiveness of the attack, the malicious node might establish false links to other nodes in the network and force its one-hop neighbors to select it as their MPR. In fig3.(b) the node x has been selected by node a as an MPR but it does not relay control traffic on behalf of other nodes. As a result, node d does not receive control traffic information from node a. In slanderer behavior due to message size limitations, an MPR may report only a partial list of elements in its selector set. A receiver cannot know if an MPR reports its entire selector set in more than one TC message. The information gathered from the TC messages is accumulated in its topology table and is only eliminated when the validity time has expired.

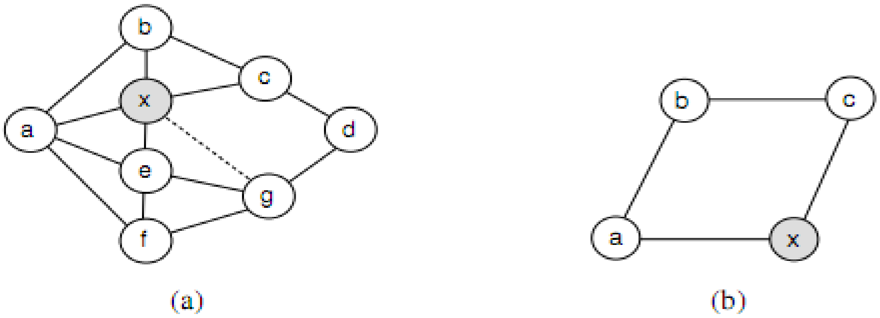


Fig.3. (a) Selfish behavior and and(b) slanderer behavior in Incorrect Relaying.

3.2 Vulnerability Mitigation in OLSR

The Optimized Link State Routing (OLSR) [4] did not include security constrains in its original design. The selected MPRs are responsible of generating and forwarding control traffic messages and used to form optimal routes from a given node to any destination in the network. If an MPR fails or misbehaves sending or forwarding control traffic information, the connectivity of the network is compromised. To overcome this problem, we proposed function k-robust-MPR, in order to improve the selection of MPRs with additional coverage. Thus every node selects, when it is possible, k + 1 disjoint MPRs sets. The union of the k + 1 disjoint sets is a k-robust-MPR set, if we remove a maximum of k elements from the MPR set of a given node n, all nodes two hops away from node n are still covered by the remaining elements in the k-robust-MPR set. We tested functions k-robust-MPR and k-covered-MPR with the presence of two types of misbehaving nodes. One adversary interrupts the proper flooding of the control traffic messages, and the second one, generates them incorrectly.

The control messages flood the network to allow every node to create optimal paths to any destination in the network. If a node misbehaves by generating or forwarding incorrect control traffic information the integrity of the network is compromised. During the execution of the protocol, each node broadcasts Hello messages to advertise their presence among their one-hop neighbors, to learn about their two-hop neighbors and to select its MPRs. The MPRs generate and retransmit Topology Control(TC) Messages. The information from Hello and TC messages allows every node to construct their routing tables. Thus, in an OLSR network, the nodes have two principal tasks to perform: i) to generate correctly routing information, and ii) to correctly relay traffic on behalf of other nodes in the network.

3.2.1 k-robust-MPR process in OLSR : our proposed function k-robust-MPR choosing disjoint groups of MPRs. In [7], additional coverage is defined as the ability of a node to select redundant MPRs. The selection of MPRs must be as small as possible to reduce the overhead due to flooding the network with TC messages like in [10]. Nevertheless, additional coverage allows a node to advertise its presence to more nodes in the network. In this manner, extra coverage helps to maintain the integrity of the network in spite of the presence of misbehaving nodes during the execution of the OLSR protocol. Function k-covered-MPR describes the MPR selection with coverage k as shown later. In our function

d(n; u): number of hops between nodes n and u.

N1(n) := {n1 : d(n, n1) <= 1}.

$N_{<=2(n)}$:= {n2 : d(n, n2) <= 2g}.

N2(n) := $N_{<=2}$(n) \ N1(n).

Function k-covered-MPR, with respect to a given node n works as follows :

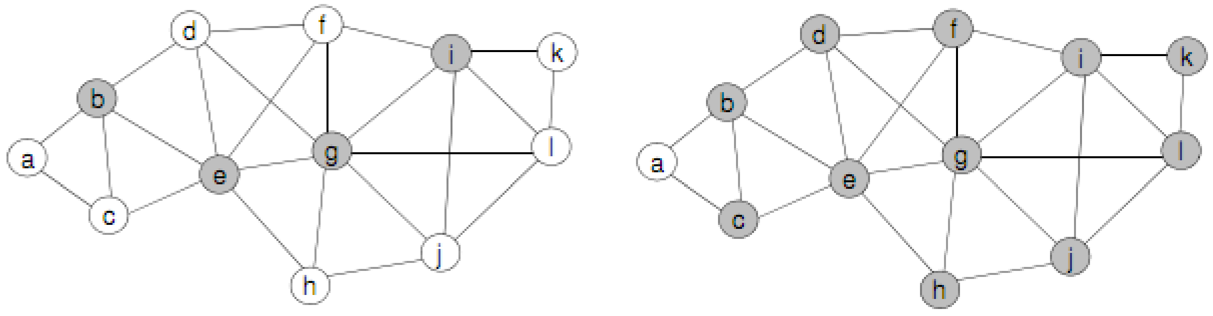
1. First, we obtain the poorly covered nodes in N2(n). Then, we include in the MPR set M, the nodes in N1(n) that poorly cover nodes in N2(n).

2. We remove the poorly covered nodes from N2(n).

3. While there exist nodes in N2(n) not yet covered by at least k nodes in the MPR set:

• We add to M the node n1 in N1(n) not in the MPR set, that provides the largest reachability(n; n1;M) and degree(n,n1).

• We eliminate all the nodes in N2(n) now covered by at least, k nodes in theMPR set.



(a) MPR selection without additional coverage. (b) *k*-Covered-MPR selection *k* equal to two.

Fig.4. MPR selection in an OLSR network with and without K-covered-MPR selection

Due to the additional MPRs selection, the number of TC messages increases considerably the amount of traffic in the network. In the sequel, we describe an improved function to select MPR sets with extra coverage that presents a balanced trade-off between additional coverage and traffic overhead.

IV. EXPERIMENTS

We conducted simulations on [9] to confirm that our k-robust-MPR set selection allows to minimize the effect of misbehaving nodes and helps to reduce the overhead generated by the k-covered-MPR function proposed in the standard OLSR protocol. To measure the effectiveness of our proposal, we count the number of nodes that were able to find a path to all nodes in the network after executing the two different MPR selection methods, for a certain period of time. Additionally, we take into account, the number of retransmissions during the simulations. For our experiments, we assume that all the nodes have the same characteristics, every node has just one interface and all the links between the nodes are bidirectional. Additionally, all the nodes have the same willingness to carry and forward traffic on behalf of other nodes, except for those that have been selected as misbehaving nodes. Our experiments confirmed that k-robust-MPR function mitigates the effect of misbehaving nodes with a better performance than the k-covered-MPR.

V. CONCLUSION

In this paper, we proposed an improved MPR selection with k-covered-MPR to mitigate control traffic attacks in an OLSR network. Our goal is to provide service availability and security. In our proposal, every node selects, if it is possible, k+1 disjoint MPR sets. As a result, we obtain a k-robust-MPR set. The number of topology control messages increases considerably reducing the performance of the network. We compared functions k-covered-MPR and k-robust-MPR in the presence of misbehaving nodes. We measured the number of nodes with complete routing tables after the execution of the OLSR protocol. Our experiments show that our function k-robust-MPR reduces the amount of traffic generated by function k-covered-MPR, and offers equivalent protection against control traffic attacks.

VI. REFERENCES

[1] R. Abdellaoui and J.-M. Robert. SU-OLSR: A new solution to thwart attacks against the OLSR protocol. In 4th Conference on Security in Network Architectures and Information Systems (SAR-SSI), Luchon, France, June, 22 - 26 2009.

[2] M. Abolhasan, T. Wysocki, and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, 2(1):1–22, January 2008.

[3] H. Badis and K. Al Agha. QOLSR multi-path routing for mobile ad hoc networks based on multiple metrics: bandwidth and delay. In Vehicular Technology Conference, IEEE, volume 4, pages 2181 – 2184, May 2004.

[4] K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Olsson. Detecting disruptive routers: a distributed network monitoring approach. IEEE Network, 12(5):50 –60, September 2008.

[5] G. Cervera, M. Barbeau, J. Garcia-Alfaro, and E. Kranakis. Mitigation of topology control attacks in OLSR networks. In 5th International Conference on Risks and Security of Internet and Systems (CRISIS), Jean-Marc Robert, editor, pages 81–88,Montreal, Canada, October 10 - 13, 2010.

[6] G. Cervera, M. Barbeau, J. Garcia-Alfaro, and E. Kranakis. Preventing the Cluster Formation Attack Against the Hierarchical OLSR Protocol: Invited Talk. In 4thCanada-France MITACS Workshop on Foundations & Practice of Security (FPS),Paris, France, May 12 - 13 2011.

[7] T. Clausen and U. Herberg. Security Issues in the Optimized Link State Routing Protocol version 2 (OLSRv2). Research Report RR-7218, INRIA, France, March2010.

[8] J.F.Ch. Joseph, A. Das, and B-S. Lee. Security threats in ad hoc routing protocols. In Guide to Wireless Ad Hoc Networks, Computer Communications and Networks, pages 1–18.Springer London, 2009.

[9] T. Henderson et. al. The NS-3 network simulator. Software package retrieved fromhttp://www.nsnam.org/, 2011.

[10] S. Rana and A. Kapil. Defending against node misbehavior to discover secure route in olsr.In Information Processing and Management, Springer Berlin Heidelberg, 2010.