Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 75 (2014) 27726-27729

ISSN: 2229-712X

Flooding attacks using packet dropper method in Optimized Link State Routing (OLSR)

Akshat Khaskalam* and Sandeep Sahu
Shri Ram Institute of Technology, Jabalpur, India.

ARTICLE INFO

Article history:
Received: 7 March 2013;
Received in revised form:
20 September 2014;
Accepted: 18 October 2014;

Keywords
OLSR,
Security,
Flooding mechanisms,
MPR.

ABSTRACT

Mobile Ad-hoc Networks (MANET) is the self organizing collection of mobile nodes. The Optimized Link State Routing (OLSR) protocol was designed to improve scalability of Mobile Ad-Hoc Networks (MANETs). OLSR protocol implements Multipoint Relay (MPR) nodes as a flooding mechanism for distributing control information. Nevertheless, OLSR was designed without security measures. There-fore, a misbehaving node can affect the topology map acquisition process by interrupting the flooding of control information or disturbing the MPR selection process.

Introduction

Mobile Ad-hoc Networks (MANET) also called infrastructure less networks are complex distributed systems consist of wireless links between the nodes and each node also works as a router to for-wards the data on behalf of other nodes. The nodes join or leave the network on their own will. The routing protocols in MANET may generally be categorized as: table-driven/proactive and source-initiated (demand-driven)/ reactive. In our paper, we gives some issues regarding OLSR protocol which is proactive routing protocols, which is based on periodic exchange of topology information. In OLSR, each node periodically broadcasts its HELLO messages. These are received by all one-hop neighbors but are not relayed. HELLO messages provide each node with knowledge about one and two-hop neighbors. Using the information from HELLOs each node performs the selection of their MPR set. The selected MPRs are declared in subsequent HELLO messages. Using this information, each node can construct its MPR selector table with the nodes that selected it as a multipoint relay. A TC message is sent periodically by each node and flooded in the network, declaring its MPR selector set. Using the information of the various TC messages received, each node maintains a topology table which consists of entries with an identifier of a possible destination (a MPR selector in the TC message), an identifier of a last-hop node to that destination (the originator of the TC message) and a MPR selector set sequence number. The topology table is then used by the routing table calculation algorithm to calculate the routing table at each node.

Related work

OLSR is a proactive routing protocol designed exclusively for MANETs. The core of the protocol is the selection, by every node, of Multipoint Relay (MPR) sets among their one-hop symmetric neighbors as a mechanism to flood the network with partial link-state information. OLSR offers, in fact, more than a pure link state protocol, because it provides the features which are minimization of flooding by using only a set of selected nodes, called multipoint relays (MPRs), to diffuse its messages to the network and reduction of the size of control packets by declaring only a subset of links with its neighbors who are its multipoint relay selectors (MPR selectors) and allows to construct optimal routes to every destination in the network. The link-state information is constructed by every node and involves periodically sending Hello and TC messages. HELLO Messages are used for searching the information about the link status and the neighbors nodes. With the Hello message the MPR Selector set is constructed which describes which neighbors has selected this nodes to play as MPR and from this information the nodes can calculate its own set of the MPRs. Whereas, Topology Control(TC) messages are used for broadcasting information about own advertised neighbors which includes at least the MPR elector list.

Security Issues in OLSR:

In this section, we review vulnerabilities in OLSR and proposed countermeasures. According to Herberg and Clausen [1], in OLSR every node must acquire and maintain a routing table that effectively reflects the network topology. The routing tables constructed by every node must converge, i.e., all nodes must have an identical topology map. 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. In the former case, the attacker may launch several types of attacks to accomplish its goal, for example:

Identity spoofing:

A misbehaving node may generate false Hello or TC messages pretending to be a different node. The attack can be launched as follows:

– A misbehaving node generates a Hello messages with a false identity. For instance, in Fig. 1(a), node M1 may generate Hello messages pretending to be node e. As a result, the MPRs of M1 will present themselves as the last hop to reach node e.

– A misbehaving generates TC messages with a false identity. For instance, M1 may generate a TC message pretending to be node f advertising node i as part of its Selector

Tele:
E-mail addresses: akshat2382@gmail.com

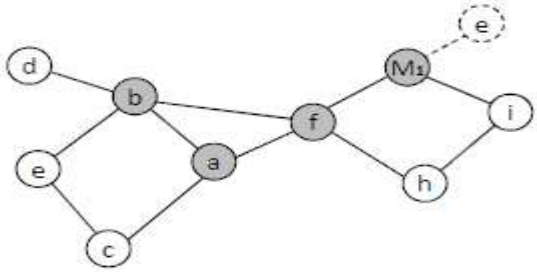
Set. As a consequence, node f appears to be the last hop to reach node i.

Link spoofing:

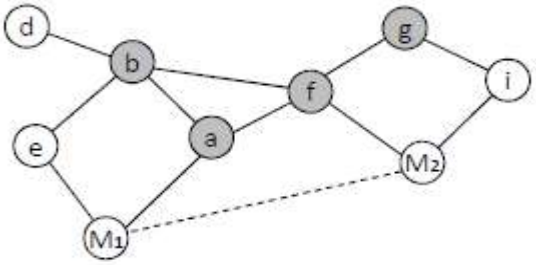
A misbehaving node may generate Hello or TC messages including false links to other nodes in the network. The attack can be launched as follows:

– In Figure 1(a), nodeM1 generates an incorrect Hello message announcing node e as its one-hop neighbor. As a result, nodes i and f include node e in their two-hop neighbor table.

– In Figure 1(b), node M1 may also generate TC messages announcing node e as part of its Selector Set. As a consequence, node M1 appears to be the last hop to reach node e.



(a)



(b)

Figure 1. Example of an OLSR-based network with misbehaving nodes M1 and M2

Replay attack:

In this attack, a misbehaving node resends old valid TC or Hello messages. For instance, suppose that in Fig. 3.1(a), nodeM1 had a valid link to node e. Node M1 may resend an outdated Hello message announcing node e as its one hop neighbor even if node e has moved and is not part of its one-hop neighborhood anymore. As a result, the network is flooded with stale information.

Wormhole attack:

In a 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. For instance, in Fig. 3.1(b), node M1 retransmits Hello messages between nodes a and e. Thus, node e and a exchange Hello messages and establish an incorrect bidirectional link. A larger wormhole can be mounted when two misbehaving nodes collude. For instance, in Fig. 3.1(b), there exists a link between nodes M1 and M2 that is never reported. Nodes e and i exchange Hello messages through the tunnel created by nodesM1 andM2. As a result, nodes e and i establish an incorrect link. In both cases, once the incorrect link has been established, other control traffic messages (i.e., TC, MID or HNA) can be tunneled.

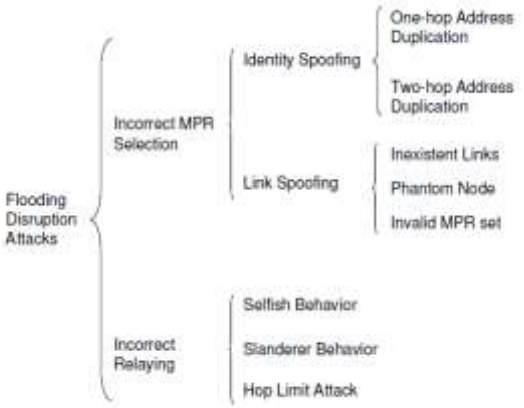


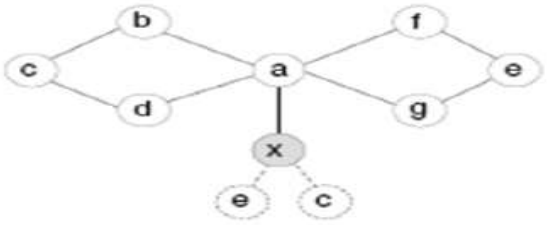
Figure 2. Taxonomy of flooding disruption attacks [2]

Flooding Disruption Attacks in OLSR:

The flooding mechanism for control traffic information in an HOLSR network is based on the correct selection of the MPRs. Control traffic messages (i.e., TC and HTC messages) are for-warded exclusively by the MPRs. An attacker seeking to interrupt the control traffic flooding can either (a) manipulate the information about the one and two-hop neighbors of a given node to cause the MPR selection to fail, or (b) misbehave during the generation and forwarding processes. Thus, a node will receive incomplete information about other nodes in its cluster or in lower level clusters. The attack has a cross layer impact if the affected node is a cluster head with an interface to an upper level. In this case, nodes in the upper level will fail to compute a route to nodes in lower levels of the network. For instance, consider in Fig. 3.1 that node E2 selects node H2 as its MPR, nonetheless H2 misbehaves and does not retransmit any control traffic message. In consequence, node F2 and nodes in cluster C3.B will not be aware of nodes within cluster C1.E. Following subsections present various attacks in detail.

Link Spoofing:

The link spoofing attack [3] is performed by a malicious node that reports an inexistent link to other nodes in the network. The objective of the attacker is to manipulate the information about the nodes one or two hops away and be selected as part of the MPR set. Once the malicious node has been selected as an MPR, it neither generates nor forwards control traffic information. The flooding disruption attack due to link spoofing is illustrated in Fig. 4.2.1(a). In this example, 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 will not reach nodes two hops away from node a. A variant of the attack can be performed by reporting a link to an inexistent node.

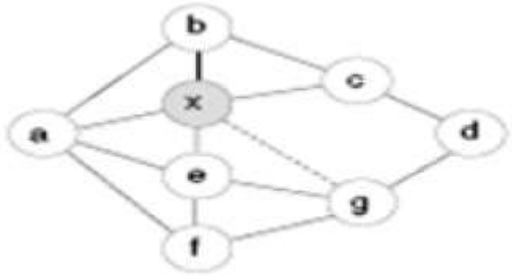


(a) Node x spoofs links to nodes e and c

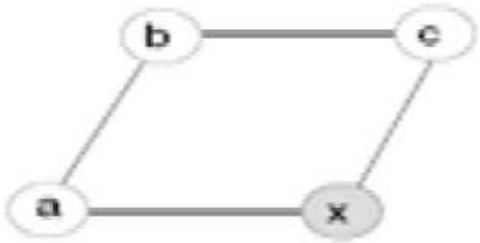
Figure 3. Flooding disruption due to link spoofing attacks

Invalid MPR Set:

In this attack, a malicious node disrupts the flooding of topology control information by misbehaving during the MPR selection pro-cess. Figure 4.3.1(a) illustrates the attack. 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 or HTC messages from node a. However, those messages never reach node d because any one-hop neighbor of node x retransmits the messages. 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 will never forward any message from node x.



(a) Node x never selects a valid MPR set.



(b) Node x modifies and forwards incorrectly TC and HTC messages.

Figure 4. Flooding disruption due to protocol disobedience

Cooperation Aspects:

Beyond the cryptographic schemes, current proposals for secure routing include cooperation enforcement mechanisms, which can be divided in two categories: currency-based mechanisms and reputation based mechanisms. Currency-based mechanisms are based either on the ex-change of virtual currency between nodes [4] or on the availability of a service which trades credits by receipts retrieved from messages in transit in the network [5]. In terms of reputation-based solutions, they are typically composed by three distinct mecha-nisms: (1) a local monitoring mechanism to observe the behavior of network nodes and determine their trustworthiness, (2) a repu-tation dissemination mechanism to convey other nodes with the results from the observations performed by the previous mechanism, and (3) a punishment/isolation mechanism to protect the network from misbehavior. Nuglets are a virtual currency used to pay for packet forwarding services [4]. In the Packet Purse Model, the source node loads nuglets in the packet before sending it and each forwarding node acquires some of these nuglets as payment. In the Packet Trade Model each forwarding node buys the packet from the previous node by some nuglets and sells it to the following node for more nuglets. Both approaches rely on a tam-per proof security module. The authors recognize that it is difficult to estimate the number of nuglets to send in the packet in order for it to get to the destination in the Packet Purse Model, and the Packet Trade Model allows overloading of the network because the sources are not bound to pay for sending packets. The estimation of the amount of nuglets to send by using a counting technique where each node holds a nuglet counter that is decreased when a node sends an own packet and increased when he forwards packets on behalf of other nodes. CORE is a Collaborative Reputation mech-anism [6] to enforce node cooperation in MANETs.

Introduced Algorithm:

Algorithm 1 Feedback message processing

1: SRs ← secondary rating of the node under analysis, *S*
2: PRs ← primary rating of the node under analysis, *S*
3: **if** mechanism for detection of false HELLO or false TC genera-tion has identified *S* as misbehaving node
then
4: PRS ← PV
5: **else**
6: **if** SRS < PRS **then**
7: SRS ← SRS + SRV
8: **else**
9: PRS← PRs + PRV
10: **end if**
11: **end if**

Simulation Results and Discussion:

Our approach is influenced but little bit different, for better approximation of dropping node we have choose following metrics to conjunction with authors [1] threshold metrics [€, α, β, μ], they are listed below-

1. Packet Delivery Ratio (pd)
2. Packet Modification Ratio (pm)
3. Packet miss routed ratio (pm_r)
4. Residual Energy (re)

Now authors [1] metric will be modified and calculated using above metrics (assuming A, and C is MANET Node)-

€ ⟶ f(pd, pm, pm_r, re)

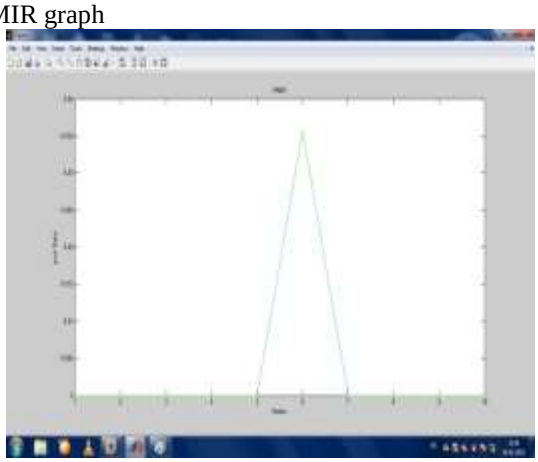
and same for other metrics α, β, μ.

Fundamentally there are two types of packet dropper node selfish and misbehaving. To detect all two nodes following calculation has been made-

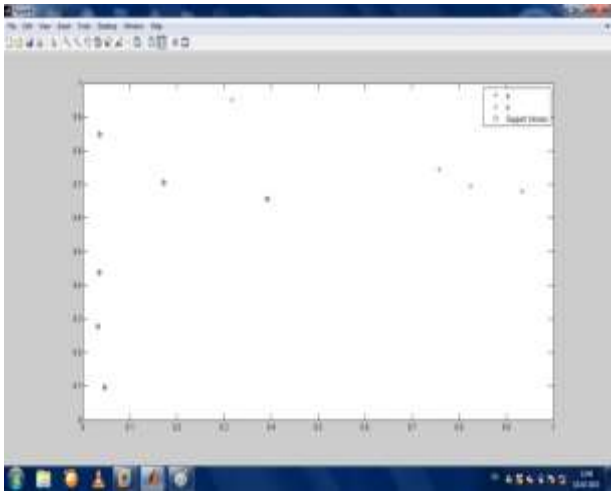
1. **Selfish node** detection via the metrics [€, α, β, μ] with conjunction
f(pd,re)
2. **Misbehaving Node** detection via the metrics [€, α, β, μ] with conjunction
f(pd,pm,pm_r)

Following are the simulation result on NS-3 Simulator

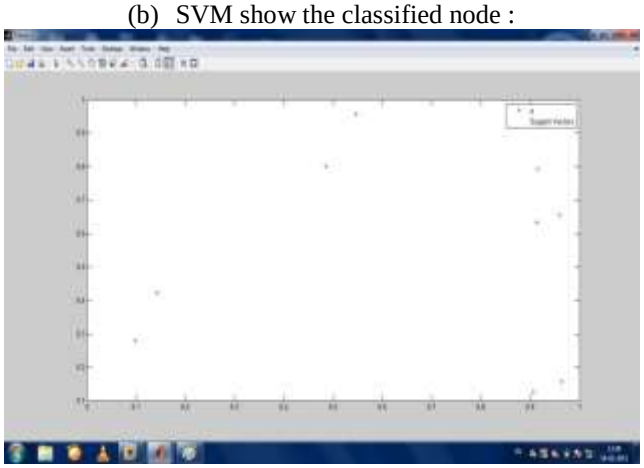
(a) PMIR graph



(c)Result graph shows the number of node which drop the packets and nodes have not dropped the packets:



(b) SVM show the classified node :



Conclusion:

This study tested the suggested Feedback Reputation Mechanism for OLSR protocol proposed in [7]. It identified the effect of modify-ing the neighboring set of nodes through the transmission range, to the punishment of the malicious and non-malicious nodes and to the recovery rate of the malicious node. The limits of the neigh-boring set are presented to be used as a heuristic for applicable environments. Descriptions of these environment are suggested, that this mechanism could be applied with the proven limitations, and also environments that should not be applied exactly due to these limitations. It has also discussed ways to tackle the identified problem through timeout mechanisms, logging of rating history and exploitation of the signal strength of the links between nodes. The result of implantation is discus in this paper simulation topic. All implantation are in NS-3[8].

References:

[1] T. Clausen and U. Herberg. Security Issues in the Optimized Link State Routing Protocol version 2 (OLSRv2). Research Report RR-7218, INRIA, France, March 2010.

[2] G. Cervera, M. Barbeau, J. Garcia-Alfaro, and E. Kranakis. Mitigation of flooding disruption attacks in HOLSR networks. In 9th Annual Conference on Communication Networks and Services Research Conference (CNSR), Ottawa, ON, Canada, May 2 - 5 2011.edition, 2006.

[3] H. Aiache, F. Haettel, L. Lebrun, and C. Tavernier. Improving security and performance of an ad hoc network through a multipath routing strategy. Journal of Computer Virology, 4:267–278, 2008.

[4] Butty´an L. and Hubaux J.P. (2000) *The 1st ACM international symposium on mobile ad hoc networking & computing*, 87-96.

[5] Zhong S., Chen J. and Yang Y.R. (2003) *INFOCOM*.

[6] Michiardi P. and Molva R. (2002) *The IFIP-Communication and Multimedia Security Conference*.

[7] Jacquet P., Muhlethaler P., Clausen T., Laouiti A., Qayyum A. and Vennot L.(2001) *IEEE International Multitopic Conference*.

[8]The ns-3 network simulator. http://www.nsnam.org, July 2009.