

Secure Optimized Link State Routing Protocol (SOLSR)

Amanpreet Kaur

Lecturer

G.N.D.E.C., Ludhiana

Basant Raj Singh Gill

Lecturer G.N.D.E.C., Ludhiana

Gurpreet Kaur Deol

Lecturer G.N.D.E.C., Ludhiana

Abstract-In this paper, the security issues related to the Optimized Link State Routing (OLSR) protocol for Mobile Ad hoc Networks (MANETs) are examined and a new protocol named as Secure OLSR (SOLSR) is proposed by adding security features to the existing OLSR protocol. The security attributes included are based on authentication checks of information injected into the network, adding a digital signature as well as more advanced techniques such as reuse of previous topology information to validate the actual link state and cross check of advertised routing control data with the node's geographical position. The proposed protocol can be applied to any proactive routing protocol for MANETs to provide better security.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services regularly available on the wide-area network to which the hosts may normally be connected.

In Ad hoc networks [5], nodes are wireless and mobile. They don't even have any base station. In such an environment, it may be necessary for one mobile host to solicit the aid of others in forwarding a packet to its destination, due to the limited propagation range of each mobile host's wireless transmissions. Some previous attempts have been made to use conventional routing protocols for routing in Ad hoc networks, treating each a mobile host as a router. The nodes themselves find their routes to other nodes in the network through distributed administration. Each node acts as a router with its own transmitter and receiver antennas and a battery source.

Efficient routing of packets is a primary MANET challenge [20]. Conventional networks typically rely on distance-vector or link-state algorithms, which depend on periodic broadcast

of routing information of all routers to keep routing tables up-to-date. In some cases, MANETs also use these algorithms, which ensure that the route to every host is always known. However, this approach presents several problems.

The routing protocols [3, 6] used in MANETs are generally either table-driven protocols or source-initiated

protocols or hybrid protocols. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. Under this category come the Destination Sequenced Distance Vector Routing (DSDV) Protocol and Optimized Link State Routing (OLSR) Protocol.

A different approach from table-driven routing is source-initiated on demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Under this category comes Dynamic Source Routing (DSR) Protocol and Ad hoc On Demand Routing (AODV) Protocol.

Based on proactive and reactive routing protocols, some hybrid routing protocols are available that combine their advantages. The most typical hybrid one is Zone Routing Protocol (ZRP).

A. Security Issues

The use of wireless links makes MANETs susceptible to attacks. Eavesdroppers can access secret information, thus violating network confidentiality. Hackers can directly attack the network to delete messages, inject erroneous messages, or impersonate a node, which violates availability, integrity, authentication, and nonrepudiation. Compromised nodes also can launch attacks from within a network. Security requirements for Ad hoc routing protocols include [7] certain discovery of paths such that the route should always be found if it exists between two nodes, Isolating misbehaving nodes such that it is made sure that misbehaving nodes are always identified and isolated from routing, and location privacy that gives information about node location and network structure.

Securing MANETs is particularly difficult for many reasons including the vulnerability of channels, vulnerability of nodes, absence of infrastructure and dynamically changing topology.

In this paper, the issues of security in proactive MANET routing protocol OLSR are investigated, especially with emphasis on providing the secure extension to OLSR, and propose a new protocol to overcome some of the security threats.

The rest of the paper is organized as follows: section 2 presents an overview of the OLSR protocol, section 3 describes the vulnerabilities of the OLSR, section 4 provides a detailed description of the proposed solution while section 5 concludes the paper.

II. THE OLSR PROTOCOL

Optimized Link State Routing (OLSR) protocol [9] is a proactive routing protocol where the routes are always immediately available when needed. OLSR is an optimization version of a pure link state protocol in which the topological changes cause the flooding of the topological information to all available hosts in the network.

A. OLSR Control Traffic

Control traffic in OLSR is exchanged through two different types of messages: “HELLO” and “TC” messages. HELLO messages are exchanged periodically among neighbor 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 are emitted periodically by a node, including its own address as well as encoding three lists. The first is a list of neighbors, from which control traffic has been heard but where bi-directionality is not yet confirmed. The second is a list of neighbor nodes, with which bi-directional communication has been established. The third is 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.

TC messages have the purpose to diffuse link state information, and more precisely information about the “last hop”, to the entire network. A TC message contains a set of symmetric neighbors that have at least one symmetrical link with the originator of the TC message. Each one of the links is contained in an Advertised Neighbor Main Address field. TC messages are periodically flooded to the entire network, exploiting the MPR optimization. Only nodes, which have been selected as an MPR, generate and relay TC messages.

MID Messages are emitted only by a node with multiple OLSR interfaces, in order to announce information about its interface configuration to the network. HNA Messages are emitted only by a node with multiple non-MANET interfaces, and have the purpose of providing connectivity from an OLSR network to a non-OLSR network.

B. Multipoint Relay Selection

Multipoint Relays (MPRs) are optimized in OLSR where each node must select MPRs from among its neighbor nodes such that a message emitted by a node and repeated by the MPR nodes will be received by all nodes two hops away. MPR selection is performed through the exchange of HELLO messages a link status of “MPR” specifies that the link between the originator of the HELLO message and the listed address is symmetric and that the node with the included address is selected as MPR by the originator. Thus, each node maintains an MPR selector set, describing the set of nodes which have selected it as MPR. Upon receiving an OLSR control message, a node will consult the MPR selector set for determining if the message is to be retransmitted. If the last-hop of the control message is an MPR selector, then the message is to be retransmitted, otherwise it is not retransmitted.

III. SECURITY WEAKNESSES IN OLSR

Various security weaknesses in proactive routing protocol for Ad hoc networks are what all proactive routing protocols are subject to. One weakness, common for all routing protocols operating a wireless Ad hoc network is that a node generates massive amounts of interfering radio transmissions. This is known as “jamming”, which will prevent legitimate traffic like control traffic for the routing protocol, data traffic on part of a network. Some other vulnerabilities [9] are:

A. Incorrect Control Traffic Generation

OLSR employs two different kinds of control traffic, HELLO messages and TC messages. In general, it is observed that with respect to control traffic generation, a node may misbehave in two different ways: through generating control traffic “pretending” to be another node - known as Identity Spoofing, or through passing incorrect information of links in the control messages - known as Link Spoofing.

B. Incorrect HELLO Messages

A node may send HELLO messages, pretending to have the identity of another node. An example is that node X sends HELLO messages with the originator address set to that of node A. This may result in the network containing conflicting routes to node A.

C. Incorrect TC Messages

A node may send TC messages, pretending to have the identity of another node. In effect, this implies link spoofing since a node assuming the identity of another node effectively passing incorrect links to the network.

D. Incorrect Traffic Relaying

If TC messages or routing protocol control messages are not properly relayed, connectivity loss may result.

IV. ALGORITHMS FOR SECURING THE OLSR PROTOCOL

This section presents a foundation allowing OLSR to resist the various attacks discussed in the previous section. The security architecture proposed is mostly cryptography based in which a few constraints are enforced on the cryptographic system employed to secure the OLSR. Any cryptographic system, satisfying the following two requirements may be employed:

A *signature* for a message can be generated in a node using a function:
 $\text{sign}(\text{nodeid}, \text{key}, \text{message})$,

A *signature* for a message can be verified in a node using a function:
 $\text{verif}(\text{originatorid}, \text{key}, \text{message}, \text{signature})$

A. Securing OLSR using OLSR Signature Message

To prevent malicious nodes from injecting incorrect information into the OLSR network, the originator of each control generates an additional security element called signature message [1,2] and transmitted with the control message. A timestamp is associated with each signature in order to estimate message freshness. Thus, upon receiving the control message, a node can determine if the message originates from a trusted node, or if message integrity is preserved. Signatures are separate entities from OLSR control traffic: while OLSR control messages perform the purpose of acquiring and distributing topological information, signatures serve to validate information origin or integrity.

B. Format of the Signature Message

The SIGNATURE message is encapsulated and transmitted as the data portion of the standard OLSR packet format.

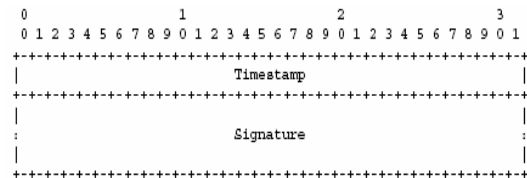


FIG 4.1 SIGNATURE MESSAGE FORMAT

The *Timestamp* field contains the timestamp itself, measured in seconds. This is the timestamp of both the SIGNATURE message and the associated control message.

Timestamps are a commonly used means to prevent replay attacks. They provide the proof of newness so that older pieces of information can be detected and rejected. The criterion to verify whether a timestamp is old is:

$$|\text{Timestamp} - t_0| \leq \Delta t$$

where t_0 is the current time at the receiving node and Δt is the accepted value for discrepancy, including the difference in the synchronization of clocks.

C. Sending a Signed Control Message

To compute a signature corresponding to a control message, the following protocol is used:

1. the node creates the control message;
2. the node retrieves the current time, and writes it in the Timestamp field;
3. the node computes the signature, and writes it in the Signature field;
4. the node puts the SIGNATURE message and the control message in the packet, in this exact order.

Then, the node sends the packet, or repeats the protocol for another control message before sending the packet.

D. Receiving and Checking a Signed Control Message

Upon receiving a control message with its SIGNATURE message, a node processes both. The outline of protocol is given below:

1. the node processes the SIGNATURE message, checking the timestamp, and keeps the SIGNATURE in memory;
2. the node checks the signature of the control message;
3. if the timestamp is fresh and the signature is valid, the control message is accepted and processed according to the standard OLSR specifications for the message type. If not, both the control message and SIGNATURE message are dropped.

CONCLUSIONS

In this paper, an overview of the security problems in wireless networks has been presented, focusing on the routing protocols in Ad hoc networks and contributed with proposing a new algorithm named Secure OLSR, which is a secure form of OLSR protocol.

The first solution is the addition of a digital signature (SIGNATURE) to the control traffic which is mainly used to prevent the injection of incorrect information in the network. For each control message (HELLO, TC, MID or HNA) generated, a corresponding Signatures are used by a receiving node to authenticate the corresponding OLSR control message and every message without a matching, corresponding signature is dropped.

However, the increased security provided by the proposed solutions is at the expense of a greater message overhead, as exchanged control messages have a larger size and involve further computations done by both the originating and the receiving node. These systems are aimed at the protection of network topology information.

The future work can be in adding additional fields in the message to increase security; the overall message overhead and complexity will increase but it adds the security. Another development may be by utilizing better cryptographic algorithms from the point of view of a smaller signature size, reduced computation complexity, and greater speed, which

would increase the suitability of the proposed POLSR security architectures to the actuality of an Ad hoc protocol.

VI. References

- [1] CEDRIC ADJIH, DANIELE RAFFO, PAUL MUHLETHALER, “ATTACKS AGAINST OLSR: DISTRIBUTED KEY MANAGEMENT FOR SECURITY”, INRIA, DOMAINE DE VOLUCEAU, FRANCE.
- [2] CEDRIC ADJIH, THOMAS CLAUSEN, PHILIPPE JACQUET, ANIS LAOUITI, PAUL MUHLETHALER, AND DANIELE RAFFO “SECURING THE OLSR PROTOCOL”, PROCEEDINGS OF THE 2ND IFIP MED-HOC-NET 2003, MAHDIA, TUNISIA, JUNE25-27 2003.
- [3] DANIELE RAFFO, CEDRIC ADJIH, THOMAS CLAUSEN, AND PAUL MUHLETHALER. “OLSR WITH GPS INFORMATION”, PROCEEDINGS OF THE 2004 INTERNET CONFERENCE (IC 2004), TSUKUBA, JAPAN, OCTOBER 28–29 2004.
- [4] DANIELE RAFFO, CEDRIC ADJIH, THOMAS CLAUSEN, AND PAUL MUHLETHALER. “SECURING OLSR USING NODE LOCATIONS”, PROCEEDINGS OF 2005 EUROPEAN WIRELESS (EW 2005), PAGES 437–443, NICOSIA, CYPRUS, APRIL 10–13 2005.
- [5] ELIZABETH ROYER AND C-K TOH, “A REVIEW OF CURRENT ROUTING PROTOCOLS FOR AD-HOC MOBILE WIRELESS NETWORKS”, IEEE PERSONAL COMMUNICATIONS MAGAZINE, APRIL 1999, PP. 46-55.
- [6] HONGBO ZHOU, “A SURVEY ON ROUTING PROTOCOLS IN MANETS” [HTTP://WWW.CSE.OHIO-STATE.EDU/~REDDYV /NETWORKING/ADHOC/AD-ROUTING/SURVEY-RP-MANET.PDF](http://www.cse.ohio-state.edu/~reddyv/networking/adhoc/ad-routing/survey-rp-manet.pdf).
- [7] HUMAYUN BAKHT, “WIRELESS INFRASTRUCTURE- IMPORTANCE OF SECURE ROUTING IN MOBILE AD-HOC NETWORKS”
- [8] NIKOLA MILANOVIC, “ROUTING AND SECURITY IN MOBILE AD-HOC NETWORKS”, FEB 2004, IEEE COMPUTER SOCIETY.
- [9] T. CLAUSEN AND P. JACQUET, “OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR)”, RFC 3626, IETF NETWORK WORKING GROUP, OCTOBER 2003.