Protecting the OLSR Protocol against Replay Attacks
Eli Winjum, Anne Marie Hegland, Øivind Kure, and Pål Spilling
UniT – University Graduate Center at Kjeller, Norway
Replay attacks

Protection based on timestamps:
  - The Timestamp Exchange Protocol

Protection based on sequence numbers:
  - An alternative scheme

Overhead analysis

Conclusions.
Replay Attacks

- An adversary records a legitimate message in order to replay the message later on.
- The receivers of the replayed message are supposed to handle the message as if it were a fresh one.
- Intension:
  - To burden the receivers with exhaustive computation.
  - To modify and manipulate information by inserting old messages in a planned manner.
- The attacker may become able to control the traffic flow.
How to Detect Replayed Messages

- Assumption: Authentication and data integrity services are available

- A possible way of tricking an authentication service:
  - Replay recorded messages, which are already signed by a legitimate message originator.

- Specific replay protection is needed in addition

- Common mechanisms:
  - Timestamps
  - Sequence numbers
  - Received information is processed only if the time stamp/sequence number is within a specified time/number interval.
- **OLSR: the Optimized Link State Routing Protocol**
- Each node selects Multipoint Relays (MPRs) from its 1-hop neighbors such that all 2-hop neighbors can be reached through at least one of them
- Routing information is exchanged mainly by:
  - **Hello** messages: Broadcast but never forwarded
    - Link sensing, neighbor detection and MPR selection signaling.
  - **Topology Change (TC)** messages: Broadcast and flooded throughout the network
    - Only nodes, which are selected MPR generate and forward TC messages
    - Routing tables are computed from information exchanged through TC messages.
The Timestamp Exchange Protocol

- Each node keeps a clock
- *The Timestamp Exchange (TE) message is proposed*
- Each node broadcasts TE messages periodically. The messages are flooded throughout the network
- Each node performs a timestamp exchange procedure with each of the other network nodes
- Periodical and global dissemination of local time information.
A Basic Message Sequence Number Check

The receiver of a replayed message receives fresh messages from the message originator.

The receiver of a replayed message does not receive fresh messages from the message originator.
The OLSR Link Establishing Procedure

Step 1: Link to B not listed

Step 2: Asymmetric link to A listed

Step 3: Symmetric link to B listed

Information is not used in protocol operations

Information is used in protocol operations
We propose that nodes have to acknowledge the reception of the previous Hello message by returning a receipt.

The receipt is the message sequence number of the most recent Hello message received from the node at the opposite end of the link.

An incoming Hello message is discarded if the receipt is deemed too old.

The receipt is necessary only in case an asymmetric link is advertised.
Evaluation: Replay of Hello Messages

1: Link to B not listed

- A
  - A receipt is not available
- B
  - A previous applicable MSN may be missing

The schemes do not work, but the false information is harmless

2: Asymmetric link to A listed

- A
  - A previous applicable MSN may be missing
- B
  - A receipt is available

A simple MSN check may not work, but the MSN receipt works

3: Symmetric link to B listed

- A
  - A receipt is available
- B
  - A previous applicable MSN exists

The simple MSN check works
Offered OLSR Traffic

![Graph showing Offered OLSR Traffic with lines for Standard OLSR, MSN-Basic, MSN-Receipt, and TEP.]
Offered OLSR Traffic to be Flooded

- Standard OLSR
- MSN-Basic
- MSN-Receipt
- TEP

Number of network nodes

Kbits pr second
Given authentication and data integrity services, the OLSR protocol is rather robust to replay attacks even without particular countermeasures.

A scheme based on a simple message sequence number check may be sufficient, even though nodes are mobile and join and leave the network dynamically.

The shortcomings of the simple message sequence number check will be eliminated if nodes attach a receipt to each asymmetric link they announce in Hello messages.

The proposed scheme scales considerably better than a timestamp exchange protocol based on periodical and global dissemination of local time information.


