Collusion Attack Resistance Through Forced MPR Switching in OLSR
Wireless Days 2010, Venice, Italy

Lalith Suresh P., Rajbir Kaur, M.S. Gaur, V. Laxmi

Department of Computer Engineering
Malaviya National Institute of Technology
Jaipur, India

October 17, 2010
Overview

- Optimised Link State Routing (OLSR)
- Collusion Attack Against OLSR
- Collusion Attack Convergence
- FMS-OLSR
- Simulation Results
Optimised Link State Routing (OLSR)

- Proactive routing protocol developed for MANETs.
- Uses Multi Point Relays (MPR) for reducing control message flooding overhead.
- HELLO messages for link sensing.
- TC messages for relaying topology information beyond 3 hops.
HELLO messages allow nodes to build their one-hop neighbour sets.

It subsequently allows nodes to build a two-hop neighbour set and an MPR set.
MPR set is the smallest set of one-hop neighbours required by a node to contact all its symmetric two hop neighbours.

In the above, A's MPR set would be \{D,C\}.
MPR nodes (\{C,D\}) announce their 'MPR Selectors' to the rest of the network using TC messages. Thus the green nodes become aware of node A.

Nodes that receive TC messages update their Topology Set. Routing table is computed using information (topology tuples) from the Topology Set.

This is the critical point of the routing protocol’s convergence.
Topology tuple removal

- Topology Tuples generated from a particular node A’s TC messages can either be:
  - Removed from a node’s topology set when more recent TC Messages are received from A. (Cancellation of Topology Tuples)
  - Removed from a node’s topology set after the validity time has expired. (Expiration of Topology Tuples)
- TC message generation time is called TC-Interval (usually 5 seconds).
- Topology tuple expiration time is typically 3 * TC-Interval.
Let $T$ be the target. $L$ and $P$ are the attackers.
Node $L$ generates a fake HELLO message announcing one-hop connectivity to all of node $L$'s symmetric two hop neighbours. $T$ chooses $L$ as its only MPR node. $L$ is thus fully responsible for forwarding any control messages from $T$.
$L$ then chooses $P$ as it’s only MPR node. Thus, $P$ becomes fully responsible for forwarding control messages from $L$.
Nodes from $T$’s former MPR set remove $T$ from their MPR Selector sets.
This is the view that nodes outside 3 hops of $T$ have of the network after the attack converges.

$T$ is thus knocked out of the network.
The attack can have a convergence delay of either:

- Short Convergence Delay, or
- Long Convergence Delay.
Short Convergence Delay

- If after the attack, the former MPR nodes of the target have non-empty MPR Selector sets, they will generate TC messages (which won’t announce the target).
- These TC messages will cancel out all Topology Tuples related to the target.
- Time required for this to happen is the time between two TC messages, the *TC-Interval*. 
Long Convergence Delay

- If after the attack, all the former MPR nodes of the target have empty MPR Selector sets, they will no longer generate TC messages.
- All Topology Tuples generated by these nodes will expire.
- The time required for this to happen is the $3 \times TC-Interval$. 
Every node has an \textit{AvoidanceSet}.

for \textit{AvoidanceDelay} duration, 
\hspace{1cm} \text{if } ((|\text{MPRset}| == 1) \text{ and } (|N1| > 1))\{
\hspace{1cm} \text{AvoidanceSet.add(Lone_MPR_node).}
\}

Nodes in the \textit{AvoidanceSet} are not included in the MPR computation process.

Remove nodes from \textit{AvoidanceSet} after \textit{AvoidanceHold} duration.
Act before the attack converges!
Choosing AvoidanceDelay

- Target is attacked
- Take corrective measures by this point to avoid damage
- HELLO Interval
- HELLO Interval
- TC Interval
- Short convergence Delay

- $\text{AvDelay} + \text{HelloInterval} < \text{ConvergenceTime}$
Choosing AvoidanceHold

- **AvDelay** + **HelloInterval** + **AvHold** > **ConvergenceTime**
Collusion attack extended up to 'c' attackers.
FMS-OLSR works for $c = 1$ as well.
Key aspect is to steer away from the head of the chain.
Experimental Setup

- Network Simulator 3.
- 36 nodes, random direction mobility model.
- Speeds varied across experiments.
- Hello Interval $= 2$ seconds.
- TC Interval $= 5$ seconds.
- One pair of attackers, targeting a single node.
- UDP traffic sent to the target before the attack commences.
Simulation Results

Packet Delivery Ratio vs. Speed of each node in m/s

Avoidance Delay = 2
Avoidance Delay = 3
Avoidance Delay = 5
Avoidance Delay = 10
Avoidance Delay = 15
Avoidance Delay = 20
Simulation Results

Packet Delivery Ratio vs Speed of each node in m/s

- Collusion Attack + FMS-OLSR
- Collusion Attack + OLSR
- No Collusion Attack + FMS-OLSR
- No Collusion Attack + OLSR
Simulation Results

![Graph showing the number of control packets generated vs. speed of each node in m/s for different scenarios: Collusion Attack + FMS-OLSR, No Collusion Attack + FMS-OLSR, and No Collusion Attack + OLSR. The graph demonstrates a decrease in the number of control packets as the speed increases for all scenarios.]
Conclusion

- FMS-OLSR is effective against tackling the Collusion Attack.
- Does not introduce new packet formats.
- Does not increase network overhead.
- Is simple to implement.
Questions?
Thank You!

Lalith Suresh  
<lalith@mnit.ac.in>

Rajbir Kaur  
<rajbir@mnit.ac.in>

M.S. Gaur  
<gaurms@mnit.ac.in>

V. Laxmi  
<vlaxmi@mnit.ac.in>