Vulnerability modelling of ad hoc routing protocols – a comparison of OLSR and DSR

Mikael Fredin - Ericsson Microwave Systems, Sweden
Leif Axelsson - Ericsson Microwave Systems, Sweden
Andrew McCabe – BAE SYSTEMS ATC, UK
Alan Cullen - BAE SYSTEMS ATC, UK

The authors gratefully acknowledge the support of their colleagues in BAE SYSTEMS plc, Ericsson Microwave Systems AB and Ericsson Telebit A/S, and the support from the UK, Swedish and Danish MoDs under the EUCLID/Eurofinder programme, Project RTP6.22 (B2NCW).
Contents

• Goals
• OLSR/DSR Recap (key points)
• Modelling Overview
  – Node Model
  – Simulation Scenarios
  – Radio model
  – Jamming model
• Simulation results
• Visualisation of jamming
• Additional investigations / protocol optimisations
• Conclusions
Goals

• To carry out vulnerability modelling of two contrasting ad hoc routing protocols, one reactive (DSR), and one proactive (OLSR)

• In particular, to investigate the effect a jammer has on a network of static sensors in the following scenarios:
  – Different network sizes: 30 nodes and 70 nodes
  – Different jamming powers and duty cycles
  – Different jammer positions (Central and corner locations)
  – Medium radio transmit power (~10% packet lost at 250 units)
OLSR Refresher (key points)

- OLSR is a proactive protocol:
  - Routing messages are sent at ‘regular’ intervals, regardless of user traffic:
    - All nodes broadcast HELLO messages.
    - Only a subset of the nodes (the MPR nodes) flood TC messages.
- Only the MPR nodes may relay user traffic.
- Different message periods may be used
  => trade-off between responsiveness and overheads.
- Option to use link quality information (link layer notifications) from the lower layer, to prevent the use of poor quality links.
- Routing messages may be brought forward (sent immediately) when topology change is detected (e.g. due to mobility, or during startup)
DSR Refresher (key points)

• Reactive (on-demand) routing protocol
  – Routing information only exchanged when data is sent
  – Main mechanisms: route discovery and route maintenance

• Known routes are cached locally in each node (route cache).
  – If a valid route does not exist in the local cache, a route discovery packet is flooded across the network. Wait for route reply.

• User packets include source route and maintenance overheads
  – All user packets carry a full source route as overhead.
  – Optionally route maintenance can be applied to each packet.

• Route maintenance detects broken links
  – If a packet cannot be forwarded (broken route) a route error packet is sent back to the packet source node.
  – Node that detects the broken link tries to salvage the packet.
OLSR & DSR: OPNET Implementation

• Results produced using OPNET Modeller environment

• OLSR
  – Proprietary implementation (platform independent C++ code)
    • Interfaced to OPNET 10.5A (PL3) via a custom ‘wrapper’ process
    • Fully compatible with RFC 3626
    • Includes an implementation option to enforce a minimal intervals between successive messages.

• DSR
  – Using the standard DSR model supplied with OPNET 10.5A (PL1)
    (this model not 100% compliant with DSR draft 9)
Modelling Overview

- Ad-hoc Nodes contain:
  - Ad Hoc Routing protocol (OLSR or DSR)
  - Application process (source/sink of user traffic)
  - IP stack
  - Radio communications

- Jammer Node contains:
  - Packet generator
  - Radio transmitter

- Statistics collected on:
  - The percentage of user packets sent by each node that are successfully delivered to their intended destination
  - Average hop counts for delivered user packets
  - Routing overhead transmitted onto the network
Modelled Scenarios:

- Ad hoc nodes, randomly positioned within 500 x 500 world
  - multiple simulation runs: different node positions and user traffic
- Number of nodes: 30, 70
- No mobility (nodes assumed stationary)
- ‘Medium’ radio power used for ad-hoc transmissions
- Jammer node placed at:
  - centre of world
  - one corner of world
- 3 different jammer power used
  - 10%, 100%, 1000% (relative to ad hoc node transmit power)
- Various jammer pulse lengths and duty cycles
- User Traffic: Each node sends one 1024-bit user packet per sec to a random destination
  - Used only to monitor traffic route-ability/connection
  - Not concerned with collision/congestion etc (implementation-specific)
Propagation Model

- SNR-based propagation model
- Packet reception probability depends on:
  - Distance of transmitter from receiver
  - Distance of jammer from receiver

\[
PathLoss = \left\{ \frac{\lambda^2}{16\pi^2 D^2} \right\}
\]

\[
R_{xPower} = T_{xPower} \times T_{xAGain} \times PathLoss \times R_{xAGain} \times \left( \frac{BandwidthOverlap}{T_{xBandwidth}} \right)
\]

\[
SNR = 10\log_{10} \left( \frac{R_{xSignalPower}}{InterferenceNoise + BackgroundNoise} \right)
\]

\[
BER = \text{Function of \{modulation type, SNR\}}
\]

\[
\text{Packet Loss Rate} = \text{Function of \{BER, no of bits\}}
\]

Expected Packet Loss Rate
Medium Power - No Jamming

- 1384 bits
- 584 bits
- Old Model

© BAE Systems and Ericsson 2005. All rights reserved
• Simulation Results:
  – User Traffic: Percentage successfully delivered
  – User Traffic: Average hop count
  – Routing overhead: Messages transmitted per node
  – OLSR, DSR, Comparisons
  – Jammer Effectiveness / Figure of Merit

• Visualisation of jamming

• Additional investigations / optimisations:

• Summary / Conclusions
User Packets delivered: 30 Nodes, Centre Jammer

User data delivered successfully
(30 nodes, jammer in centre)

Proportion delivered

- 10% DSR
- 100% DSR
- 10% OLSR
- 100% OLSR
- DSR baseline
- 10% OLSR
- 100% OLSR
- OLSR baseline

Burst type

- 50us / 500us
- 50us / 5ms
- 50us / 50ms
- 5ms / 50ms
- 5ms / 500ms
- 5ms / 5s
- 0.5s / 5s
- 0.5s / 50s
- 0.5s / 500s
- Continuous
User Packet Hop Counts (30 Nodes, Centre Jammer)

Hop counts (30 nodes, jammer in centre)

- 10% DSR
- 100% DSR
- 1000% DSR
- DSR baseline
- 10% OLSR
- 100% OLSR
- 1000% OLSR
- OLSR baseline

Burst type:
- [10% 1% 0.1%]
- [10% 1% 0.1%]
- [10% 1% 0.1%]
- [100%]
Routing Messages Transmitted (30 Nodes, Centre Jammer)

Routing Messages Transmitted
(30 Nodes, jammer in centre)

- Messages transmitted per node per sec
- Burst type
- [10% DSR] [100% DSR] [1000% DSR] [DSR baseline]
- [10% OLSR] [100% OLSR] [1000% OLSR] [OLSR baseline]
Jammer Effectiveness (30 Nodes, Centre Jammer)

Jammer Effectiveness
30 Nodes : Central Jammer

user packets delivered

<table>
<thead>
<tr>
<th></th>
<th>OLSR</th>
<th>DSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>NoJamming</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>50us / 50ms</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>5s / 5s</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>50us / 50ms</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>5s / 5s</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>50us / 50ms</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>5s / 5s</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>50us / 50ms</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>5s / 5s</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Continuous</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>
Jammer Figure of Merit (30 Nodes, Centre Jammer)

This Figure of Merit emphasises packets lost per unit of jamming power.
• Simulation Results:
  – Traffic delivered
  – Hop count
  – Routing messages transmitted
  – Comparisons / Figure of Merit

• Visualisation of jamming

• Additional investigations / optimisations:

• Summary / Conclusions
Probability of packet loss under Jamming

<table>
<thead>
<tr>
<th>Jammer Distance</th>
<th>Node Separation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td>500</td>
<td>500</td>
</tr>
</tbody>
</table>

Probability of packet loss: Packet Size: 1384 bits; Jammer Power 100%

- Probability of packet loss: Packet Size: 1384 bits; Jammer Power 100%
- Probability of packet loss: Packet Size: 1384 bits; Jammer Power 10%

- Dependents: Jammer Tx Power (relative to ad-hoc node transmit power)
  - Relative distance of jammer and source node from the receiving node (key factor)
  - Packet size (weak dependence).
- Note the narrow transition region - due to the rapid BER vs SNR falloff
Visualisation of Jamming in a 30 node Network

Green links: (good) have better than 50% success in both directions.

Red Links: (asymmetric) have better than 50% success in only one direction, worse than 50% success in other direction.

Yellow Links: (bad) worse than 50% delivered in both directions

* Only showing LLN links here *
(not so easy to draw for non-LLN case)
• Simulation Results:
  – Traffic delivered
  – Hop count
  – Routing messages transmitted
  – Comparisons / Figure of Merit

• Visualisation of jamming

• Additional investigations / optimisations:

• Summary / Conclusions
Additional investigations / optimisations

• 70 node networks
  – Jammer in corner/centre

• OLSR minimal intervals
  – Pulsed jamming can lead to significant increases in the OLSR routing overhead transmitted onto the network.
  – This can be countered by enforcing a minimum interval between successive OLSR transmissions.
  – Minimum intervals up to the default message intervals have little adverse effect on user traffic delivery.

• OLSR Link Layer Notification
  – Hop counts higher when LLNs used
  – User packet delivery better when LLNs are used
  – Routing overhead higher when LLNs are used (more MPRs, more hops)

• DSR Route Maintenance, salvaging and retransmissions
  – User packet delivery better when salvaging is used
  – User packet delivery also better when retransmissions are used
  – Routing overhead higher when salvaging and/or retransmission are used
  – Route maintenance increases the routing overhead but also increases user packet delivery
• Simulation Results:
  – Traffic delivered
  – Hop count
  – Routing messages transmitted
  – Comparisons / Figure of Merit

• Visualisation of jamming

• Additional investigations / optimisations:

• Summary / Conclusions
Summary & Conclusions: Generalities

• Long distance links are more susceptible to jamming than short links.
  – During jamming, an ideal routing protocol would aim to use a route with many short hops in preference to a route with a few long hops.
  – Both protocols tended to use shorter hops when the jamming was continuous (i.e. when it was clear that certain links were non-operational)
  – Neither protocol succeeded in converging towards shorter hops in the presence of pulsed jamming

• In general, OLSR packet delivery rates were better than DSR
  – Mainly due to OLSR’s use of Link Layer Notifications (LLNs)
    • OLSR selected shorter hops which are more robust to jamming
  – However DSR has salvaging
    • No benefits over OLSR under severe jamming, where frequently no alternative route would be available.
    • Succeeded in a few cases of less severe jamming.
Summary & Conclusions: Routing Overhead

• OLSR
  – With OLSR’s responsiveness to topology changes constrained by enforcing minimum intervals between successive transmissions:
    • The overhead increase during jamming is relatively small (typically <30%).
    • During severe jamming, the overhead falls due to network fragmentation.
  – When shorter OLSR minimum intervals were used
    • The routing overhead increased significantly (by OOM for fast pulsed jamming)
    • Little change in user traffic delivery performance.

• DSR
  – Under some jamming conditions there were repeated unsuccessful searches for unreachable destinations - this causing up to a factor of 10 increase in overhead
    • Familiar weakness with reactive protocols
    • Serious problem due to additional network load and power consumption
Summary & Conclusions (cont)

• Hop counts
  – Higher for OLSR than DSR during jamming
    • Mainly due to OLSR’s use of LLNs, resulting in OLSR using shorter links but needing more hops.

• Jammer duty cycles
  – Matching the jamming cycles to the OLSR “HELLO” or “TC” default message intervals did not provide any additional jammer advantage.
    • OLSR’s message ‘jitter’ helps to mitigate against this type of attack
    • Synchronising jamming to actual OLSR emissions would most likely provide a jammer advantage - not tested as part of this work
  – DSR does not emit routing messages to a fixed cycle time and is therefore not additionally susceptible to any specific cycle.
Summary & Conclusions (cont)

• A possible enhancement to DSR is to flood the “route error” message locally, rather than sending it right back to the source, so that nodes around a failing link are notified sooner.

• Jammer planning
  – A jammer placed at the geographical centre is more disruptive than a jammer placed at the corner of the network (as expected).
  – Using multiple low power jammers is more a power efficient way of disrupting a network than using a single high power jammer.