NHDP/OLSRv2 Security

Ulrich Herberg
Thomas Clausen
Reminder draft-herberg-manet-packetbb-sec

- Proposed I-D is a common extension to RFC5444, intended to be applicable where RFC5444 is applicable.

- Simple mechanism for carrying a signature, as address block, message, packet TLV

Reminder draft-herberg-manet-nhdp-sec

- Add signature TLV to messages with value:
  - `<sign-tlv> := <hash-fkt><sign_algo><sign>`

- Signing messages: `sign = sign_algo(hash-fkt(message))`

- Validating messages: `verified = verif(message, <sign-tlv>)`
Updates from packetbb-sec-02 to -03

- Editorial changes
- Introduced Address Block TLVs for signatures and timestamp
  - fine-grained security (i.e. sign “both ends of a link”)
Fine-grained security in NHDP/OLSRv2

- Problem when using signed control messages as in draft-herberg-manet-nhdp-sec and draft-herberg-manet-olsrv2-sec:
  
  Required trust in links advertised by a router

- Possible solution: sign each address in an address block
Fine-grained security in NHDP/OLSRv2

- Additional security when chain of trust cannot be assumed
- Message size grows significantly (linearly with density)
- Will be included in next revision of nhdp-sec draft
Security Vulnerability Analysis of NHDP/OLSRv2

(complete analysis in http://hal.archives-ouvertes.fr/inria-00456376/en/)

Analysis will be integrated into draft-herberg-manet-nhdp-sec-threats and draft-herberg-manet-olsrv2-sec-threats
Proper functioning of OLSRv2 assumes that

- each router can acquire and maintain an accurate topology map, and
- that the network converges.

OLSRv2 networks can be disturbed by breaking either of these assumptions:

- routers may be prevented from acquiring a topology map, or
- routers may acquire a wrong topology map, or
- routers may acquire inconsistent topology maps.
Topology Map Acquisition

- Flooding disruption by identity spoofing

- $a$ can select $b$ or $d$ as MPR
- if it selects $b$, $X$ can disrupt flooding by not forwarding traffic ($c$ is unreachable by flooded traffic)

- $b$ can select $a$ or $c$ as MPR
- if it selects $a$, $x$ (white) is unreachable by flooded traffic
Topography Map Acquisition

- Flooding disruption by link spoofing

- X spoofs links to c and w
- a will select X as MPR
- flooding is disrupted (routers “left” of b are unreachable by flooded traffic)
Topology Map Acquisition

- Radio Jamming
  - Interfaces on a “jammed” channel are unable to receive HELLOs or TCs
  - Depending on the L2, transmission of control traffic may still be possible
  - Some inherent protection of NHDP by ignoring unidirectional links
Topology Map Acquisition

- Hop Limit
  - decreasing hop limit reduces scope of TC message
Topology Map Acquisition

- **Hop Count**
  - When set to 255, TC messages will not be forwarded
  - When value is reduced, validity time may be affected when using distance-dependent validity times (RFC5497)
Effective Topology

- Incorrect forwarding (data traffic)
  - No influence on routing protocol, but discrepancy between effective and perceived topology

- Wormholes
  - Traffic is recorded and tunneled through an “out-of-band” channel
  - Harmfulness depends on characteristics of the wormhole, and how paths are calculated
Effective Topology

- Sequence number attack
  - Denial-of-service attack using message sequence numbers or ANSN

- Message timing attacks
  - Decreasing validity time
  - Decreasing interval time when using link quality
Effective Topology

- Indirect jamming (neighborhood discovery)
- Switching between SYM and LOST status of an advertised link
- Leads to in-router resource exhaustion (MPR recalculation)
- Possibly triggers HELLOs/TCs
Effective Topology

- Indirect jamming (link state advertisement)
- Switching between MPR and LOST status
- Leads to in-router resource exhaustion (routing set recalculation of other routers)
- Possibly triggers TCs
Inconsistent Topology

- Inconsistent Topology Maps due to Neighborhood Discovery

- X does not participate in link state advertisement procedure
- Traffic transiting d will be forwarded to X rather than to the intended destination
- Traffic transiting c with b as destination, will be delivered to the intended b
- Traffic transiting c with a as destination may be delivered to the intended a via b or to the malicious router via d
Inconsistent Topology

- Inconsistent Topology Maps due to link state advertisement

- $f$ selects $X$ as MPR
- $b$ and $c$ will route traffic towards $a$ to the intended destination
- $e$ and $f$ route traffic towards $a$ to $X$
Inconsistent Topology

- Routing Loops
  - $g$ ignores TCs originating from itself

- Perceived Topology in $f$

- Perceived Topology in $g$
References

- U. Herberg, T. Clausen, “MANET Cryptographical Signature TLV Definition”, draft-herberg-manet-packetbb-sec-03
- U. Herberg, T. Clausen, “Cryptographical Signatures in NHDP”, draft-herberg-manet-nhdp-sec-00