MANET Security

Ulrich Herberg
Thomas Clausen
draft-herberg-packetbb-sec-02

- RFC5444 is common building block in MANET protocol
- Proposed I-D is a common extension, intended to be applicable where 5444 is applicable.
- Has been presented and discussed at IETF ‘75
- Simple mechanism for carrying a signature, as address block, message, packet TLV (and multi-value TLV)
Security Threats in MANETs

(for link state protocols such as NHDP/OLSRv2)
Security threats in MANETs

- Identity Spoofing

![Diagram showing an attacker claiming an invalid identity](image-url)
Security threats in MANETs

- Link Spoofing
Security threats in MANETs

- Relaying

- Incorrect control traffic relaying

- Another common attack is relaying control traffic, but not data traffic (out of scope)
Security threats in MANETs

- Replaying

![Diagram showing an attacker replaying recorded control traffic]
Security for NHDP/OLSRv2

- Digitally signed messages may be used to counteract identity spoofing
  - Allows to detect signature == identity

- Digitally signed messages may be used to counteract link spoofing
  - if signed by "both ends of the link"

- Pushes the problem to one of
  i. distributing keys and
  ii. preserving key confidentiality (of shared or private key)

- Does not preclude relay or replay attacks
Security for NHDP/OLSRv2

- draft-herberg-packetbb-sec: common format for RFC5444-based protocols
  - does not mandate or suggest crypto-mechanism (notably symmetric, asymmetric, id-based, etc.)
NHDP Security
draft-herberg-nhdp-sec-threats-00

- Analysis of security threats to NHDP
- Analysis of security threats to protocols using NHDP for neighborhood discovery
In NHDP: “an implementation may recognize additional reasons for identifying that a message is malformed”

This is what draft-herberg-nhdp-sec does, by specifying the process of digitally signing and validating messages in NHDP
Sender: Signing a HELLO message

1. **Message is to be sent**
2. **Add Timestamp TLV**
3. **Temporarily remove all Signature TLVs**
4. **Calculate signature**
5. **Add Signature TLV**
6. **Send message**
7. **Restore Signature TLVs**

* As defined in draft-herberg-packetbb-sec
Recipient: Recognizing a signed HELLO message as correct

Message arrives

- contains `<msg-orig-addr>` and `<msg-seq-num>`?
  - no → Discard message
  - yes → contains Timestamp TLV?
    - no → time differs more than MAX_TIME?
      - no → Restores Signature TLVs and recalculate size
      - yes → Recalculate message size
    - yes → contains any recognized Signature TLVs?
      - no → Read next recognized signature
      - yes → Message valid

Message valid

- does signature correspond to message?
  - yes → Remove all Signature TLVs from message
  - no → no
Summary of NHDP security

- NHDP allows to reject messages for external reasons
- Based on draft-herberg-packetbb-sec
- draft-herberg-nhdp-sec provides a framework for signing and validating messages in NHDP
- Counteracts part of the security threats described in draft-herberg-nhdp-sec-threats
Key distribution and cryptographic algorithms

- No "one-size-fits-all", therefore:
  - Key distribution not addressed (application/deployment specific)
  - Key revocation not addressed (appl./depl. specific)
  - Cryptographic algorithm not suggested (appl./depl. specific)
    - Registries set up by draft-herberg-packetbb-sec for different algorithms
The way ahead

- Evaluate for dymo
  - Verify security considerations for dymo
  - Verify that draft-herberg-packetbb-sec TLV is sufficiently expressive
- Refine, update draft-herberg-packetbb-sec
- Publish draft-herberg-packetbb-sec as RFC?

- Refine NHDP security documents (just submitted)
- Work-in-progress on similar OLSRv2 document, submission shortly after this IETF
  - similar in spirit to the NHDP document
Running code

- draft-herberg-packetbb-sec, draft-herberg-nhdp-sec, as well as the coming draft-herberg-olsrv2-sec are all implemented in "running code"

All routers using valid signed messages

Red router not signing messages