



Updates on RFC5444/NHDP Security

Ulrich Herberg
Thomas Clausen

Updates on draft-ietf-manet-packetbb-sec-04

- Went through WG LC, got comments from Christopher Dearlove
- Separated draft into :
 - General framework (TLV format, how to treat msg-hop-count etc.) with TLV type extension 0
 - Specific decomposition of signatures into $\text{crypto}(\text{hash}(\text{content}))$ with type extension 1 (in the appendix)

Next steps for draft-ietf-manet-packetbb-sec

- Include new review from Chris on revision -04
- Rename draft
- Then, WG LC

Updates on draft-herberg-manet-nhdp-sec-02

- Updated reference to packetbb-sec-04
- Uses new structure of packetbb-sec-04, currently with TLV type extension 1 only

Next Steps for draft-herberg-manet-nhdp-sec

- WG adoption of nhdp-sec (?)
- Allow for other signature decompositions (i.e. TLV type extensions) in next revision
- Update to draft-herberg-manet-nhdp-sec-threats