Security Changes 802.15.4

Tero Kivinen
INSIDE Secure

What

- In 802.15.4 maintenance work the SC-M takes all 802.15.4 amendments published and rolls them into one 802.15.4 document.
- During this process there is quite a lot of mistakes, errors and omissions noted, which are then fixed during the process.
- Currently in sponsor ballot, you can buy the current version from IEEE.
- Security section snapshot can be found from
  - https://mentor.ieee.org/802.15/dcn/15/15-15-0275-00-0mag-security-functional-description-from-p802-15-4-revc-df5.pdf
  - Mentor is like IEEE version of internet-draft repository. Members can submit stuff, everybody can read and download them.

Corrections

- Fixed incoming state machine to clearly allow mixing secured and not-secured frames.
- Fixed incoming state machine to work with TSCH ASN, i.e. skip the frame counter processing if TSCH is used.
- Properly specified which parts of the 4e new frames are encrypted and which not (i.e. header IEs are not encrypted and Payload IEs can be encrypted).
- Specified that Enh-Acks cannot use the same frame counter as the incoming packet had, they can still use ASN for TSCH.
- Changed the PIB tables to be bit more logical, keeping the same feature set.

Changes / Things removed

- Changed the MAC command identifier to be encrypted for new frame types. It is after the encrypted payload IEs, and you need to decrypt them before you can know where the command identifier is, which would make it very complicated if it was in clear.
- Removed ability have 5-octet frame counter stored in frame, now 5-octet nonce format is only used for TSCH and ASN.
- Removed encrypt only security level (security level 4).
- Removed the short address from the TSCH nonce generation as it is unsafe, and not specified clearly enough (i.e. there cannot really be interoperable implementations done based on the text in 4e).

Additions

- Added ability to specify which IEs the MAC layer will act on, i.e. for each IE there is now ability to specify policy whether it is processed or skipped.
- To make security easier to understand we spitted the incoming state machine to two pieces one for secured frame and another for not-secured frames.
- Provided state machine pictures and security PIB entry pictures.
  - https://mentor.ieee.org/802.15/dcn/15/15-15-0106-05-0mag-security-section-pictures.pdf
  - Not part of base specification, but will be referenced in the bibliography.