MAC CE Security Analysis

Nokia

Security types needed for MAC CEs

- Classification of UL/DL MAC CEs based on security and privacy need
  - The threats may depend on the purpose of MAC CE, so the necessary protection could vary – based on SA3 analysis, RAN2 defines signaling to determine MAC CE protection
- Security need based on the nature of threat/vulnerability of the MAC CE:
  - Passive Eavesdropping &Privacy: Encryption
  - Location Tracking & Fingerprinting: Encryption
  - Message Injection/spoofing to cause Denial of Service: Integrity protection
  - Jamming: Neither may help - robustness in PHY in required instead (not strictly in scope of SA3)
  - Cross-Layer Exploits: Encryption (potentially integrity protection depending on use case)
- Proposal: SA3 to identify need for MAC CE protection + potential mechanism
  - Methodology: Identification of the type of security (encryption/integrity) needed for each MAC CE. Consider impacts to both UE (UL) and network (DL).

Questions to RAN2

- If MAC CEs would be protected in similar way as PDCP packets, what would be the impact from the security protection (e.g. adding integrity signature such as MAC-I to the MAC CEs could increase the total MAC CE size)?
- What is the allowed or expected processing impact for the security protection? That is, when a MAC CE is sent by the UE/BS, are there requirements on how fast the processing should be done and does the sender expect a response or behavior change from the receiver (i.e. are there requirements for processing the MAC CEs that could be impacted by the time taken by the procedures for encryption/decryption or integrity protection/verification)?
- Would there be issue if the MAC CEs the received processes the MAC CEs in different order than the transmitter sent them (i.e. is there some “stateful” behavior where several MAC CEs need to be received in a particular order)?
- Are the MAC CEs sent individually or can they be grouped to provide a bigger payload? (i.e. what should be assumed regarding the size of the payload to be protected)