Proposed methodology for MAC CE security

Qualcomm Incorporated

Discussion on proposal

- Not feasible to analyse all MAC CEs – as needs to be done both individually and in groups (attack may use multiple MAC CEs)
    - There are over 60 individual MAC CEs
- Any such analysis may end up being re-considered in a later release resulting in requiring protection of a previously unprotected MAC CE
    - This will add a lot of implementation complexity
- Need to get to the solution discussion stage to be able to give RAN2 a reasonable estimate for security overhead
    - Important not to spend time on over-detailed security analysis to be able to share information with RAN2 by their requested checkpoint

Methodology proposal

- Determine if protection of any MAC CEs is required
  - This can be captured in the Annex on MAC CE security
- If so, agree a Key Issue to study possible solution to provide this security
  - Ideally this would be agreed in February meeting
- Once above agreed, work on suitable solutions for MAC CE security
  - Progress these in April and May meeting with the hope of tentative overhead impact by May meeting
- Liaise with RAN2 on impact of such processing and overhead
  - E.g. request feedback on issues applying security to all MAC CEs after security is established
  - Note: Some MAC CEs may be need before security can be set up (e.g. before AS SMC can be sent at idle to active)
- If MAC CEs are added in later releases, then by default they are always sent protected
  - If necessary, RAN2 needs to provide SA3 with information why a new MAC CE needs to be sent unprotected, e.g. similar to cleartext IEs in initial NAS security in 5G.

RAN2 queries

- None as some SA3 progress needed before it is clear what information is needed from/relevant to RAN2