Security for Satellite Access and NTN

Xiaomi

Satellite/NTN related work in 3GPP

Unique ID	*Title*	*Nature of Relationship*
770002	Study on using Satellite Access in 5G	SA1 study item (Rel-16) on use cases and requirements for satellite access in 5G
800048	Stage 1 of 5GSAT	SA1 work item (Rel-17) on service requirements of satellite access in 5G
860010	Guidelines for Extra-territorial 5G Systems	SA1 study item (Rel-18) on new regulatory requirements
890022	Study on vehicle-mounted relays	SA1 study item (Rel-18) containing service requirements related to satellite access
800026	Study on architecture aspects for using satellite access in 5G	SA2 study item (Rel-17) on architecture aspects for using satellite access in 5G
860005	(Stage 2 of) Integration of satellite components in the 5G architecture	SA2 work item (Rel-17) for integrating satellite systems in 5G architecture
940074	Study on satellite access Phase 2	SA2 study item (Rel-18) on 5GC enhancement for satellite access Phase 2
941006	NR NTN (Non-Terrestrial Networks) enhancements	RAN work item (Rel-18) on NR enhancements for satellite access

SA2 R18 SID (SP-211651)

- Study on 5GC enhancement for satellite access Phase 2
  - *Architectural enhancements to support discontinuous coverage for mobility enhancement (e.g. paging enhancement)*
  - *Architectural enhancements considering prediction, awareness & notification of UE wake-up time, power saving optimizations*
- Security considerations
  - How to protect the potential new procedures/messages for mobility enhancement supporting discontinuous coverage? With existing security mechanisms or new security mechanisms?
  - How to handle the security context in the UE (regarding its validity) when it is not staying awake for the sake of power efficiency?
  - How to handle the security context in the UE (regarding its validity) when it is temporarily out of coverage?
  - How to protect the data stored and/or forwarded for UEs temporarily out of coverage?

RAN R18 WID (RP-213690)

- NR NTN (Non-Terrestrial Networks) Enhancements
  - *4.1.3 Network verified UE location*
    - *Study and evaluate, if needed, solutions for network to verify UE reported location information*
- Security considerations
  - UE location verification at the network is to ensure:
    - Authentic UE location information is not tampered by attackers during transmission
    - Original information for positioning is not fabricated by a misbehaving UE
    - The UE fabricating its information for positioning cannot repudiate its misbehavior

→ UE position info is to be protected during transmission from the UE to the network

→ Is there a need for non-repudiation of the original position info from the UE?

Privacy Specific Issues

- Multiple LSs received from RAN1 and RAN2 with privacy concern
  - *R1-2106332: concerning privacy issue of the gNB/NTN-GW*
    → In the regions prohibiting broadcasting NTN-GW/gNB location, there is privacy concerns.
  - *R2-2106543: concerning privacy issue of the UE*
    → If a permanent/temporary ID (e.g. SUPI/IMSI, 5G GUTI) is sent together with UE location information, there could be a privacy issue
  - *R2-2109199: concerning user consent for UE privacy*
    → an NTN specific user consent may be needed before gNB can configure the UE to report its location information

Proposals in SA3

- Identify security key issues and study security solutions for enhanced architecture supporting discontinuous coverage with satellite access
- Identify security key issues and study security solutions for network verification of UE location information reported with satellite access
- Analyze privacy issues and study protection mechanisms (if needed) for potential RAN solutions utilizing the location of the gNB/NTN-GW or the UE