**3GPP TSG-SA5 Meeting #155 *S5-243296***

Jeju, South Korea, 27 - 31 May 2024

**Source: China Telecom**

**Title: potential solution for Management of connections between UPF on-board satellite and SMF**

**Document for: Approval**

**Agenda Item: 6.19.15**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

[x] 3GPP TS 33.210 Network Domain Security (NDS); IP network layer security

# 3 Rationale

A new use case, potential requirements, and potential solution are added for secure communication between NTN node and SEG.

# 4 Detailed proposal

# 5 Use cases, potential requirements and solutions

## 5.x Management of secure connections in a non-terrestrial network

### 5.x.1 Use case #1: Connectivity between non-terrestrial network node and security gateway

#### 5.x.1.1 Description

In a 3GPP network radio access network (RAN) nodes such as eNodeB and gNodeB are deployed in cell sites which are typically part of an untrusted network domain. By contrast, core network (CN) nodes are deployed in a trusted domain. These two network domains are logically and physically separated by means of security gateways (SEG) as defined in [x]. The communication between the domains, including the network management traffic, must be secured and is carried over a logical connection referred to as the ‘backhaul’.

The backhaul may be secured using security associations between the RAN nodes and a SEG. E.g. Internet Key Exchange (IKE) Version 2 (IKEv2) and IP Security (IPSEC) Security Associations (SAs).

In ground based terrestrial networks the connectivity between RAN nodes and SEG is based on physical connectivity. As a result the underlying IP network design seldom changes, and the logical connectivity between the RAN nodes and SEG remains relatively stable.

However, in airborne non-terrestrial networks (NTN) the connectivity between RAN nodes and SEG is not stable since the RAN nodes are moving. E.g. a satellite in LEO, MEO or GEO orbit. A non-terrestrial node provides a service link and relies on a feeder link to communicate with other nodes comprising the NTN, including the SEG.

As NTN nodes move the availability of terrestrial connectivity is subject to change. This has potential impact to the security associations between the NTN node, SEG and CN.

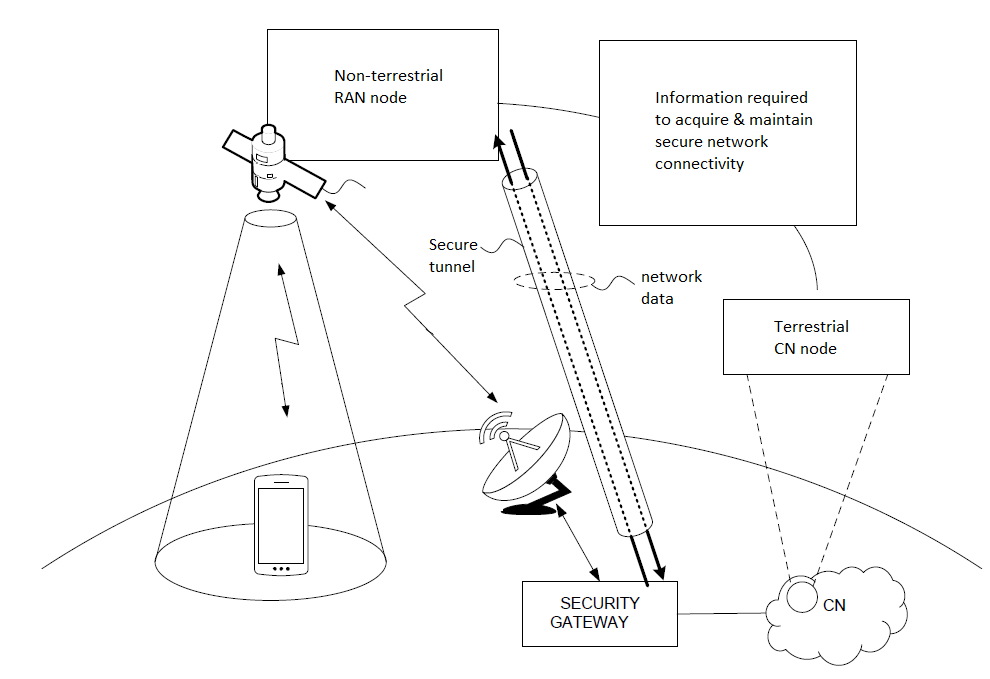


Figure 5.x.1.1-1 Secure connectivity between non-terrestrial RAN node and terrestrial CN node(s)

As NTN nodes move their security associations must be updated subject to the availability of new terrestrial connectivity to a new SEG. In some cases, such SEG transitions may be able to be performed in anticipation of the upcoming feeder link update (i.e. “make then break”) whereas in others the new connectivity may not be available in advance (i.e. “break then make”). Both scenarios must be supported, and different information may be required to setup and maintain the secure associations subject to which security protocols and features are configured.

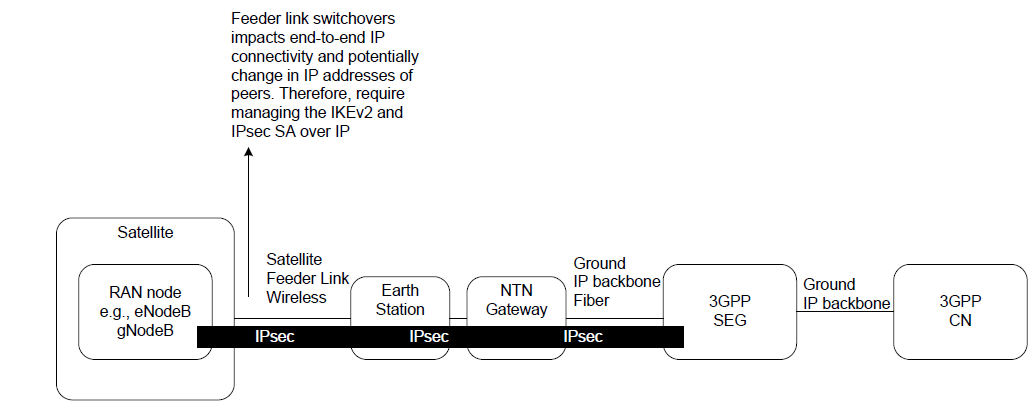


Figure 5.x.1.1-2 Impact of feeder link switchover between NTN node, SEG and CN

The IP configuration requires correlation with the state of connect/disconnect of the IP link itself. For example, for satellite based NTN node the following may need to be considered:

* + satellite may only ever connect to ground stations allowed by policy. As a result, when the satellite moves out of ground station’s catchment location, it loses the ground connectivity via the feeder link and the IP transport during such period, and then reestablishes the IP connectivity.
  + when the satellite orbit is passing over the earth surface (e.g., oceans, mountains, deserts, forests etc.) where there is no ground station and supporting infrastructure, the satellite may by-design route data over to Inter Satellite Link (ISL) to other satellites that may have connectivity with the ground infrastructure over a feeder link, but the ground infrastructure may reside in jurisdiction not permitted by regulations.

To further ensure the security associations are maintained, additional information must also be made available to the NTN node about the anticipated terrestrial connectivity based on criteria such as flight path and/or time windows.

Summary:

Movement of the NTN nodes means the backhaul connection must traverse multiple feeder links and its security associations must be maintained throughout lifecycle phases of IP connectivity. As a result, NTN nodes require information not only to setup the initial secure communications channel, but to maintain such communications as the NTN moves.

#### 5.x.1.2 Potential requirements

**REQ-NTN-PnC-1：**IP configuration data shall be configured for the secure communications channel association between RAN nodes on-board satellite and SEG.

**REQ-NTN-PnC-2：**IP configuration data shall be updated when transitioning between terrestrial networks, to ensure the secure association between NTN node and SEG.

**REQ-NTN-PnC-3：**IP configuration data shall be maintained at NTN node independent of feeder link availability.

#### 5.x.1.3 Potential solutions

##### 5.x.1.3.1 Potential solution #1: Pre-configure security association data in NTN satellite node

Pre-configure the anticipated feeder link switchovers and satellite handovers in advance based on the 'flight path'.

Flight path information can be used as input to the network management system to create configuration data for the RAN nodes hosted on-board satellites. Specifically, time windows can be derived that provide the anticipated connectivity between each NTN node and ground infrastructure via feeder link(s).

Each time window includes start time, end time, and the configuration required to establish/maintain secure communications with SEG during that period. Time windows may overlap in the event multiple connectivity options exist for a given period. Such overlaps can be leveraged to help ensure seamless connectivity.

At least 1 entry needs to be provided to allow each NTN node to perform initial connection to terrestrial network.

Once configured, the appropriate data is applied to its respective NTN node.

Within each NTN node the information is used to define triggers to automate the setup and maintenance of the secure connectivity, including:

* time window start: trigger for IP configuration each time IP connection is available.
* time window end: trigger to anticipate when the IP connection is about to disconnect.
* time window overlaps: trigger to allow configuring the new IP configuration in advance of losing the current connection.
* time window gaps: trigger to adjust secure IP connection configuration before potential disruption to IP connectivity.

Changes to terrestrial network may require the NTN data also be updated. Periodic checks for such changes could also occur as triggered events based on the NTN data, however it may be better to perform such maintenance from the network management system to minimize disruptions to terrestrial connectivity.

#### 5.1.1.4 Evaluation of potential solutions

TBD