A Study on Security Vulnerabilities in Non-Terrestrial Networks

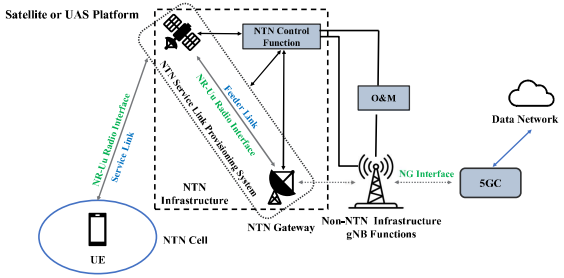
Rahul Varma Chintalapati, Nishith Tripathi, Jeffrey Reed
Commonwealth Cyber Initiative, Virginia Tech

Motivation

Problem Statement and Research Goals

1. Investigate security vulnerabilities of wireline and wireless interfaces in NTNs.
2. Carry out quantitative analysis of Service Link and Feeder Link interfaces of an NTN to determine vulnerability to jamming attacks.
3. Propose security mechanisms for NTNs and describe how the present 5G security framework can be extended to secure an NTN.

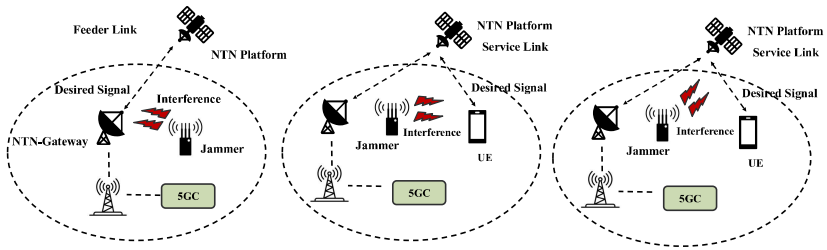
Background



The Transparent Payload Architecture

A 5G NTN-based system with a transparent NTN payload consists of NTN capable UEs, transparent NTN payloads residing on NTN platforms (e.g., satellites or HAPSs), terrestrial NTN-Gateways, non-NTN infrastructure gNBs on the ground, the 5G Core Network, and the Data Network.

Jamming Scenarios

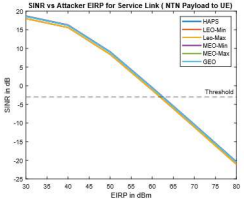


The attacker tries to cause interference to the feeder link from the NTN payload to the NTN-GW.

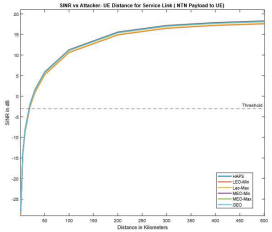
The attacker tries to cause interference in the service link from the NTN platform to the UE.

The attacker tries to cause interference in the uplink service link from the UE to the NTN payload.

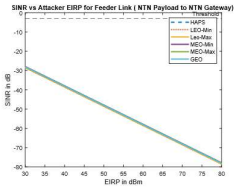
Discussion and Results



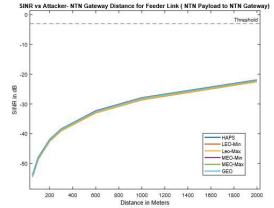
This graph depicts the trends in the SINR at the UE receiver as the EIRP of the attacker varies and the distance between the attacker and the UE remains constant.



This graph describes the SINR trends, as the distance between the UE and the attacker varies when the attacker EIRP remains constant at 50 dBm.

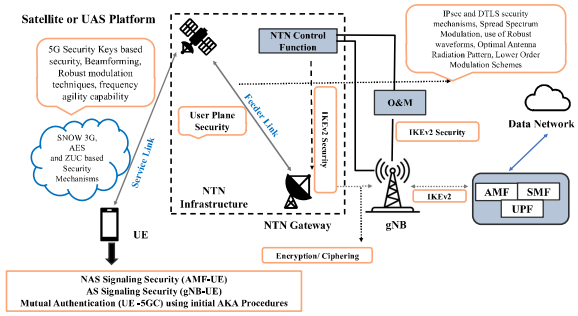


This graph shows the trends in the SINR at the NTN-Gateway receiver as the EIRP of the attacker varies at constant distance (100 m).



The graph shows the SINR trends as the distance between the NTN-Gateway and the attacker varies.

Proposed NTN Security Mechanisms



Wireline Centric NTN Security.

Security mechanisms for wireline interfaces in 5GC are classified into service-based wireline interfaces (NRF-NF mutual authentication) and non-service-based wireline interfaces (IKEv2, IPsec).

Node-centric NTN Security.

Due to the wireless interfaces between various NTN nodes or Network Functions, the TN-like security level does not exist inherently. To prevent node-based attacks, the 3GPP-defined intra-network security mechanisms can be used to ensure the validity of the nodes.

Interface-centric NTN Security.

Interface-centric security aims to establish a secure connection between two NTN nodes for communication.

Conclusion and Future Work

Conclusion.

5G has a comprehensive security framework, including security for service-based and non- service-based interfaces and integrity protection and ciphering for both the Access Stratum and Non-Access Stratum signaling. 5G also supports integrity protection and ciphering for the User Plane to protect user traffic.

This poster describes how 5G security framework can be applied to secure an NTN.

The poster also analyzes various jamming scenarios, and the impact of jamming attacks on the Uplink and Downlink of Service and Feeder Links in an NTN System.

Future Work.

This proof of Concept of NTN security can be extended to defining security practices for the O-RAN Architecture.

The preliminary quantitative jamming analysis can be used to develop an x-app to detect jamming attacks using the knowledge of impact of jamming attacks on performance metrics like SINR, SNR, I/N among others.

References

[1]. Luiz A. DaSilva, Jeffrey H. Reed, *"Securing 6G: Securing NTN"*, IEEE-Wiley., 2024.

[2]. Rahul Varma Chintalapati, "*Network Slicing for Smart Traffic Intersections and Secure Non-Terrestrial Networks and Terrestrial Networks*", Masters Thesis (Unpublished).

[3]. Rahul Chintalapati, Nishith Tripathi, Manoj Kumar, Jeffrey Reed, "*Feasibility Analysis of Isolation-Based Spectrum Sharing Between Terrestrial and Non-Terrestrial Networks*", IEEE Texas Symposium, April 2024.

Acknowledgements : This research was sponsored in part by the CCI Project Grant, the NSF SpaceNet Project Grant (CNS 22535139) and the NSF OAIC Project Grant (CNS 2120411)

cyberinitiative.org