IPsecme
Internet-Draft
Intended status: Informational
Expires: 19 January 2026

M. Chen
L. Su
China Mobile

18 July 2025

IPsec problems when used in NTN network
draft-chen-ipsec-problems-for-ntn-network-01

Abstract

This document describes the problems in the use of IPsec in satellite Internet and NTN network scenarios.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 January 2026.

Table of Contents

1. Introduction 2
2. Terminology 2
2.1. Terms 2
2.2. Requirements Language 3
3. IPsec used in NTN 3
4. Analysis of possible issues with continuing to use IPsec . . 6
4.1. The issues with the IKEv2 handshake protocol when faced with latency and packet loss 6
4.2. The issues with Security Association (SA) and IP Address Binding when the IP address of the satellite is changing 6
4.3. The issues with Zero tolerance for out of order windows 7
4.4. Conflict between Lifetime and Link Interruption 7
5. IANA Considerations 7
6. Security Considerations 7
7. Acknowledgements 7
8. Normative Reference 7
Authors' Addresses 7

1. Introduction

The IPSEC protocol provides end-to-end security for IP networks by authenticating and encrypting IP packets to ensure the confidentiality, integrity, and authenticity of data during transmission. Under satellite Internet and NTN network, IPSEC is still a very important and commonly used security protocol. Due to the dynamic characteristics of satellites, there are also some problems in the use of IPsec.

This document describes the problems in the use of IPsec in satellite Internet and NTN network scenarios.

2. Terminology

2.1. Terms

The following terms are used in this document.

* Non-Terrestrial Network(NTN): using satellites, HAPS, Non ground platforms such as drones serve as communication nodes, forming a three-dimensional communication network together with ground base stations, allows user equipment (UE) to directly access the network through satellites or high-altitude platforms, thereby achieving global communication services.

* gNB: generation NodeB

* base station: a base station is a fixed device in wireless communication networks, used to achieve wireless signal transmission and data exchange between mobile devices and the core network.

* ground gateway station(abbreviated as gateway): a key equipment in satellite communication systems, mainly responsible for data transfer and routing management between satellites and ground networks

* AMF: Access and Mobility Management Function is one of the core functional modules of the core network, defined by the international communication standards organization 3GPP in the technical specification TS 23.501

* UPF: User Plane Function is an independent functional entity responsible for user plane data processing in the 5G core network. As a core component of the 5G SBA (Service Based Architecture) defined by the 3GPP standard, it is mainly responsible for routing and forwarding user data packets, policy execution, and protocol adaptation.

* UE: User Equipment refers to user terminal equipment, which is a collective term for mobile communication devices that can access cellular networks.

* DN: Data network.

2.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. IPsec used in NTN

For NTN network, the wireless access network defined in 3GPP is used with satellite network, UE can access data network via 3GPP wireless network and satellite network. NTN network supports gNB and UPF on satellites, UE connects to the base stations on satellites, and then connect to the core network through ground gateway stations.

The data transmission path between the wireless access network and the core network is called the backhaul link, used to transmit user data, signaling, and control information from the wireless access layer to the core network for processing, forwarding, and storage. When the position of the base station changes, it will affect the security of the return link. This document takes 5G as an example to analyse the use of ipsec problems existed in NTN network.

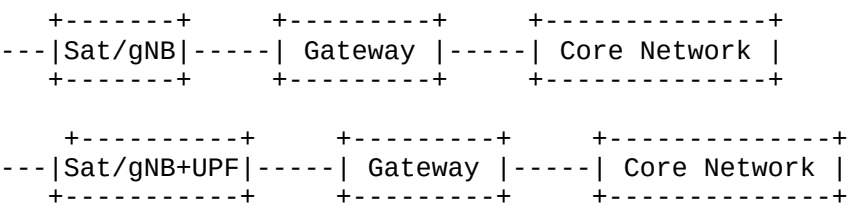

Figure 1: UE access the ground mobile core network through satellite

Multiple security interfaces are involved in this network architecture, and the 3GPP standard(TS33.501) specifies the use of IPsec to solve end-to-end secure transmission issues. The interfaces related to the ipsec protocol are summurised in Table 1.

Interfaces	Usage	Protocol	Description in 3GPP
N2	gNB-AMF	IPsec	In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of the present document. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.(TS 33.501)
N3	UE-UPF	IPsec	In order to protect the traffic on the N3 reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of the present document with

			confidentiality, integrity and replay protection. IPsec is mandatory to implement on the gNB and the ng-eNB.(TS 33.501)
N4	UPF-SMF	IPsec	9.9 Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs Non-SBA interfaces internal to the 5G Core such as N4 and N9 can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, these interfaces shall be confidentiality, integrity, and replay protected. Roaming interfaces between PLMNs except for N32, shall be confidentiality, integrity, and replay protected. Protection for the N32 interface is specified in clauses 13.1 and 13.2..For the protection of the above mentioned internal and roaming interfaces except N32, NDS/IP shall be used as specified in [3], unless security is provided by other means, e.g. physical security. A SEG may be used to terminate the NDS/IP IPsec tunnels.(TS 33.501)
N9	UPF-UPF	IPsec	Same with N4
backhaul	gNB-CN	IPsec	9 Security procedures for non-service based interfaces 9.1 General 9.1.1 Use of NDS/IPThe protection of IP based interfaces for 5GC and 5G-AN according to NDS/IP is specified in TS 33.210 [3]. Traffic on interfaces carrying control plane signalling can be both integrity and

				confidentiality protected according to NDS/IP.

Table 1: Summary of the interfaces related to ipsec in NTN network

From the table, we can see that the security of these interfaces relies entirely on IPsec providing end-to-end transmission security. In NTN networks, there are some issues to use IPsec due to the dynamics of datellites.

4. Analysis of possible issues with continuing to use IPsec

4.1. The issues with the IKEv2 handshake protocol when faced with latency and packet loss

IKEv2 relies on UDP transmission and defined retransmission in RFC 7296. Under long inter satellite link latency, the following issues may be encountered:

* The default initial timeout an easily trigger premature retransmission, leading to a storm of repeated requests. Setting a longer timeout default value during implementation based on transmission latency can solve this problem.

* The loss of a single control message (such as IKE_AUTH) may reach the maximum number of retransmissions, leading to an exponential increase in handshake latency.

Different retransmission rules need to be set according to different environments, especially in the case of satellite networks, then avoid network congestion.

4.2. The issues with Security Association (SA) and IP Address Binding when the IP address of the satellite is changing

The security alliance is uniquely identified by a triplet. This triplet includes: Security Parameter Index (SPI), destination IP address, and Security Protocol Number (AH or ESP). Due to the high-speed movement of the satellite, the overhead time is approximately 5-10 minutes, and at least one end’s IP address is dynamically changing.

SA lacks a IP independent identification mechanism. When the IP changes, the existing SA becomes invalid and the tunnel must be rebuilt. Although MOBIKE supports IP updates, but it cannot solve the problem of simultaneous changes in IP and entity.

4.3. The issues with Zero tolerance for out of order windows

The default anti replay window of IPSec is only 64 packets, relying on strict packet sequences. Due to multi-path routing, QoS scheduling, satellite switching, the probability of out of order arrival in satellite links is extremely high.

The sliding window model will result in he legitimate packet was mistakenly rejected as a replay attack due to out of order, triggering a TCP retransmission storm.

4.4. Conflict between Lifetime and Link Interruption

SA needs to update the key regularly (based on time/traffic), but the inter satellite link is frequently interrupted (obstructed, switched). If the interruption exceeds the survival time of SA, SA will be cleared and a full reconstruction is required for recovery.

It is necessary to set the lifetime of SA based on the worst-case scenario of the satellite network to ensure that SA will not be deleted due to interruption.

5. IANA Considerations

This document does not require actions by IANA.

6. Security Considerations

This document mainly presents issues and does not involve new security considerations at the moment

7. Acknowledgements

Welcome everyone to contribute together

8. Normative Reference

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

Authors' Addresses

Meiling Chen
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing
100053
China
Email: chenmeiling@chinamobile.com

Li Su
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing
100053
China
Email: suli@chinamobile.com