Workgroup: SAVNET Working Group
Internet-Draft: draft-jliu-savi-ipsa-00
Published: 28 February 2024
Intended Status: Informational
Expires: 31 August 2024
Authors: J. Liu
Tsinghua University
H. Li
Tsinghua University
T. Zhang
Tsinghua University
Q. Wu
Tsinghua University

A SAVI Solution for IP based Satellite Access

Abstract

This document presents the source address validation solution for for IP based Satellite Access. This mechanism transfers user states through end network collaboration to solve the impact of dynamic handover of satellite-ground links on native SAVI. This document mainly describes the operations involved in overcoming the dynamics of the access link.

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 31 August 2024.

Table of Contents

1. Introduction

Malicious source address spoofing is an important component of Distributed Denial of Service (DDoS) attacks. Source Address Validation Improvements (SAVI) [RFC7039][RFC7513][RFC8074] is a key technology used in terrestrial Internet to prevent source address spoofing. By listening to the control packets exchanged when the host obtains the IP address, a binding relationship between the IP address and the unforgeable link layer attributes (Anchors) is established for the terminal on the access device. And then source address validation is performed on the IP data packets, Only packets with matching source addresses and bound table entries will be forwarded to ensure the authenticity of the source address of data packets entering the internet. However, in the scenario of satellite access, the high dynamism of Low Earth Orbit (LEO) satellites keeps the anchor away from the user, resulting in the failure of anchor binding information. Each time a handover is made, the satellite

storing binding information will move away from the corresponding user. So the user needs to perform identity authentication and anchor binding again. Frequent execution of this operation by a massive number of global user nodes will generate a signaling storm, leading to a sharp decline in the availability of SAVI.

This document describes the mechanism for the source address validation method for IP based satellite access by end-network collaboration, considering the dynamic characteristics of satellite access scenarios. This technology requires the decomposition of user states in source address validation into collaborative management between the network side and user terminals. When handover occurs, the end-network collaboration completes a low-cost secure transfer of user states, avoiding anchor mobility caused by dynamic handover of satellite-ground links, which leads to a sharp increase in source address validation costs and a decrease in availability. This technology requires only one hop signaling interaction between the user terminal and the access satellite, without involving the ground Network Control Center (NCC) and Inter Satellite Links (ISL) [Starlink-ISL], significantly reducing the rebinding delay caused by handover. In addition, due to the fact that the rebinding process does not occupy any ISL bandwidth, this method has high scalability for satellite access scenarios with a global massive number of users.

2. Terminology

Initial access satellite: the satellite that the user terminal connects to the satellite Internet for the first time.

New access satellite: the user terminal reconnects to the satellite connected to the satellite Internet after handover.

Binding anchor: "binding anchor" is defined as the physical and / or link layer attributes of the additional device, as defined in [RFC7039]. In this document, the binding anchor refers to the communication key of the link layer.

Binding entry: the entry that associates the IP address and MAC address with the binding anchor.

3. The threat of IP source address spoofing in satellite access scenarios

3.1. Characteristics of Satellite Access Scenarios

The satellite access scenario has many new network characteristics, including the use of ISL, the dynamism of the access link (frequent handover between user terminals and LEO satellites will inevitably lead to frequent updates of IP addresses), and the openness of

satellite orbit information (accurate prediction of satellite motion can be achieved through calculation). Due to the global movement of satellites, they are mostly in an uncontrolled environment and face threats from a large number of malicious hosts distributed around the world. In addition, there is a significant performance gap between satellite processors and the ground device, and many terrestrial mature solutions are difficult to implement on satellites.

3.2. source address validation for IP based satellite access scenarios

The use of ISL in satellite access scenarios increases the vulnerability of the network layer. DDoS attack is one of the most common attacks at the network layer. Due to limited computing resources, lack of traceability, and exposure to uncontrolled environments, source address spoofing attacks in satellite access scenarios are more severe than those in terrestrial networks. To defend against such attacks, the most effective technique in terrestrial networks is to filter address spoofing packets and ensure that malicious users in the network are located through traceability of the source address. SAVI and other source address validation technologies have been deployed in terrestrial networks, and their effectiveness has been proven to some extent. However, due to the fragility of satellite constellations described above, SAVI technology cannot be directly applied to satellite access scenarios.

The source address validation scenario for IP based satellite access scenario is shown in Figure 1, which is divided into ground segment and space segment. The ground segment includes user terminals, authentication servers, and ground gateways connected to the Internet. The space segment consists of satellites with access capabilities (using ISL and supporting SAVI).

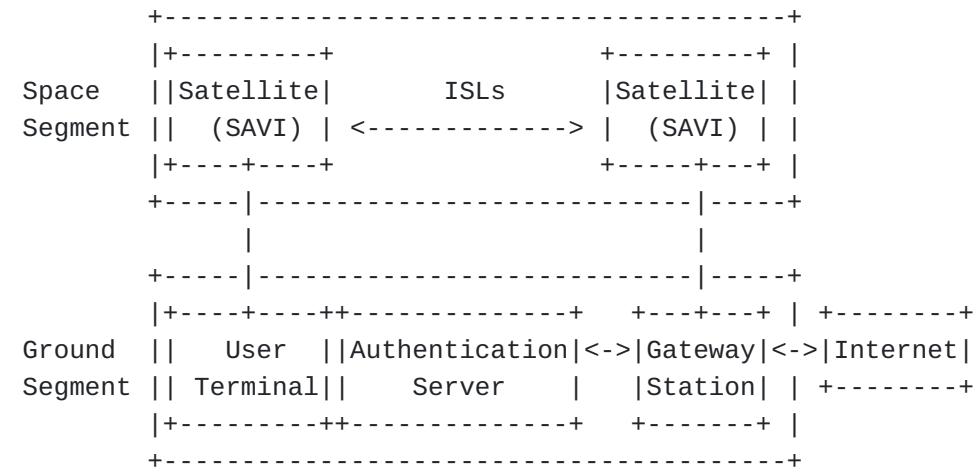


Figure 1: The source address validation for IP based satellite access scenarios.

3.3. Deterioration of existing mobility processing mechanism

A SAVI Solution for WLAN [draft-bi-savi-wlan-24] proposes to extend CAPWAP protocol by introducing host IP message elements. When the mobile host is disconnected from the original access device on the network side, the new access device sends a request to the original access device, and the original access device uses this message to report the MAC address and IP address to the new access device, so as to complete the migration of binding information. Related draft describes that the movement of hosts between APs and ACs can be applied to this extension.

This solution can work effectively in the ground WLAN scenario, but it will fail in ISTN due to the extremely fast relative moving speed (up to 27000km/hour) between the access device (LEO satellite) and the host, and the large moving range (globally). This document refers to the implementation of this solution in ISTN as the anchor request.

Specifically, after the satellite handover, the newly accessed satellite sends the anchor request to the satellite where the anchor binding information is located. After obtaining the anchor binding information, the binding relationship is added in the local data plane, and then the source address validation operation is performed locally. Because the handover frequency of access satellite is minute level and the scale is all users, this method will make the network face massive state migration signaling overhead.

4. Design requirements for source address validation for IP based satellite access

4.1. The ability to effectively resist source address spoofing

The source address validation for IP based satellite access can effectively resist various attacks initiated by malicious users through source address spoofing, such as DDoS. By matching and validating the source address of user data packets with anchor binding information on the access satellite, packets with forged source addresses will be identified and discarded, thus avoiding malicious packets from entering the network.

4.2. Lightweight signaling interaction

The cost of source address validation for IP based satellite access must be within the acceptable range of the devices involved. When satellite handover occurs, the signaling interaction required to handle user state transitions should be sufficiently streamlined to

reduce additional latency and bandwidth waste. In addition, the processing and computational costs of data should also take into account the performance limitations of onboard processing devices.

4.3. High scalability

The source address validation for IP based satellite access should be easy to deploy in a lightweight manner on a large number of globally distributed users and satellites, with performance not deteriorating with the growth of user and satellite scale, and support incremental deployment.

5. Specification of SAVI for for IP based satellite access

5.1. Framework

SAVI for IP based satellite access provides a framework for low-cost migration of anchor binding status information in wide area high-speed dynamic network scenarios represented by IP based satellite access. In the existing SAVI technology, the user state managed only by the network side is decomposed into the collaborative management of the user end and the network side, that is, the satellite sends the user state (such as the user IP address, MAC address and binding anchor) to the user terminal for maintenance, and when the handover occurs, the user terminal and the network side infrastructure linkage complete the user state transfer.

The core workflow of SAVI for based satellite access is briefly described as follows:

a. Tthe orbit deployment stage

The satellite uses encryption methods (such as asymmetric encryption algorithm) to generate key pairs, binds satellite characteristic information (such as satellite ID) with the satellite's own public key to form a public key comparison table, distributes it to other satellites in the constellation through earth stations or GEO satellites, and requests to update the local public key comparison table.

b. The identity authentication stage

The corresponding communication key is obtained after successful authentication through a specific identity authentication mechanism (such as 802.1x).

c. The address allocation stage

This document takes the StateLess Address Autoconfiguration (SLAAC) as an example. The initial access satellite sends the address prefix

and satellite ID to the user terminal through the extended RA message. The user terminal generates a temporary IPv6 address and sends it back to the initial access satellite through the NS message for duplicate address detection (DAD).

d. The initial binding stage

After the initial access satellite completes the duplicate address detection of the temporary address, the communication key is used as the anchor of the source address validation, bound with the user's MAC address and IPv6 address to form the binding information, which is added to the binding state table (BST) of the initial satellite, and the lifetime of this entry is set. After signing the binding information with its own private key, it is sent to the user terminal through the extended Na message.

e. The rebinding stage

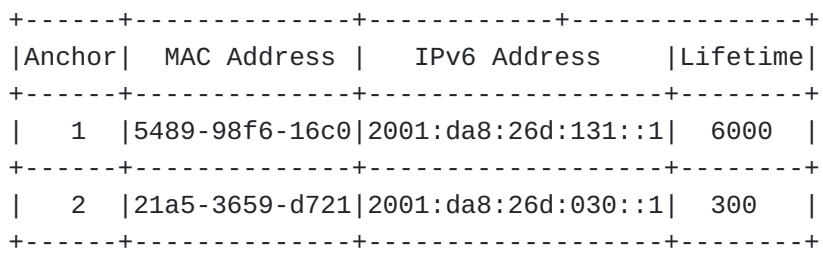
After the user terminal switches the new access satellite, it sends the signed binding information to the new satellite through the extended RS message. The new access satellite queries the initial satellite public key in the local public key comparison table through the initial satellite ID parsed from the user's IPv6 address, obtains the original binding information after verifying the signature of the received information, and then queries the local BST. If the query is successful, Explain that the user terminal has been connected to the satellite, reset the lifetime of the entry. If the query fails, match and verify the binding information with the MAC address and IPv6 address of the current user terminal. If the matching passes, add it as a new entry to the local BST and set the lifetime.

The new access satellite informs the user terminal that the communication key will be used for subsequent data transmission encryption.

5.2. The new binding anchor

Unlike existing SAVI solutions that use Ethernet ports or MAC addresses as anchors, this document proposes to use the communication key of the data link layer as an anchor. The communication key conforms to the characteristic description of the anchor in the SAVI framework. More importantly, the new access satellite can inherit the communication key after completing the migration of the anchor binding state information, so as to avoid reperforming identity authentication and key negotiation to obtain the communication key after handover, so that the user terminal only needs to authenticate when it accesses the IP based satellite access for the first time.

The BST of SAVI for IP based satellite access mainly contains fields, as shown in Figure 1.



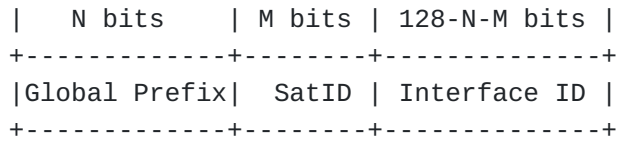
Anchor	MAC Address	IPv6 Address	Lifetime
1	5489-98f6-16c0	2001:da8:26d:131::1	6000
2	21a5-3659-d721	2001:da8:26d:030::1	300

Figure 2: Example Binding State Table for IP based satellite access.

5.3. Semantic extension of IPv6 address based on satellite characteristic

By embedding satellite characteristic information, such as satellite ID, into the IPv6 address, it can be used as the stable identification of the network side state maintenance equipment when the user first accesses. Any new access satellite can resolve the identification from the IP address of the user terminal, so as to query the elements required to decrypt the user state of the corresponding application.

The IPv6 address structure of the SAVI for IP based satellite access embedded with satellite ID is shown in Figure 3.



N bits	M bits	128-N-M bits
Global Prefix	SatID	Interface ID

Figure 3: The structure of IPv6 address expanded.

5.4. Reliable binding migration

Through encryption and decryption technologies such as asymmetric encryption algorithm, the encrypted binding state information is stored in the user terminal, and the terminal sends it to the new access satellite for decryption verification and rebinding after each handover, so as to ensure the security of the user state in the process of transferring from the previous access satellite to the

new access satellite via the user terminal in the clear text communication environment without performing identity authentication.

5.5. Binding clearing

In order to reduce the storage burden of satellite nodes, the entries in the BST will be automatically deleted once the lifetime reaches to zero.

6. Acknowledgements

7. IANA Considerations

This memo includes no request to IANA.

8. References

8.1. Normative References

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <https://www.rfc-editor.org/info/rfc7039>.

[RFC7513] Bi, J., Wu, J., Yao, G., and F. Baker, "Source Address Validation Improvement (SAVI) Solution for DHCP", RFC 7513, DOI 10.17487/RFC7513, May 2015, <https://www.rfc-editor.org/info/rfc7513>.

[RFC8074] Bi, J., Yao, G., Halpern, J., and E. Levy-Abegnoli, Ed., "Source Address Validation Improvement (SAVI) for Mixed Address Assignment Methods Scenario", RFC 8074, DOI 10.17487/RFC8074, February 2017, <https://www.rfc-editor.org/info/rfc8074>.

8.2. Informative References

[draft-bi-savi-wlan-24] Bi, J., "A SAVI Solution for WLAN", 2024, <https://datatracker.ietf.org/doc/draft-bi-savi-wlan/>.

[Starlink-ISL] "Starlink block v1.5", <https://space.skyrocket.de/doc_sdat/starlink-v1-5.html>.

Authors' Addresses

Jun Liu
Tsinghua University
Beijing 100084
China

Email: juneliu@tsinghua.edu.cn

Hewu Li
Tsinghua University
Beijing 100084
China

Email: lihewu@cernet.edu.cn

Tianyu Zhang
Tsinghua University
Beijing 100084
China

Email: ty-zhang20@tsinghua.org.cn

Qian Wu
Tsinghua University
Beijing 100084
China

Email: wuqian@cernet.edu.cn