Internet Area Working Group
Internet-Draft
Intended status: Informational
Expires: 4 December 2023

J. Liu
H. Li
T. Zhang
Q. Wu
Tsinghua University

2 June 2023

Problems and Requirements of Source Address Spoofing in Integrated Space and Terrestrial Networks

draft-jliu-istn-savi-requirement-02

Abstract

This document presents the detailed analysis about the problems and requirements of dealing with the threat of source address spoofing in Integrated Space and Terrestrial Networks (ISTN). First, characteristics of ISTN that cause DDos are identified. Secondly, it analyzes the major reasons why existing terrestrial source address validation mechanism does not fit well for ISTN. Then, it outlines the major requirements for improvement on source address validation mechanism for ISTN.

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 4 December 2023.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document.

Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Mega-constellations of low-earth-orbit (LEO) satellites, such as Starlink [Starlink], Kuiper [Kuiper] and OneWeb [OneWeb] serve the area that the terrestrial networks cannot reach [Networking-in-Heaven]. LEO satellites have advantage of wide coverage [ITU-6G][Surrey-6G][Nttdocomo-6G] and low delay [Low-Latency-in-Space].

LEO mega-constellations have Inter Satellite Links (ISLs) ,which enable traditional attacks extend from one-hop in satellite communication environment to the whole satellite networks. Also,

LEO’s attributes, such as open access environment, limited Resources and dynamic topology, enable severe security threats. These security threats yield diverse challenges on existing network security design.

By analyzing security events occurred recently, we realized that typical LEO threats are Source Address Spoofing. This memo outlines the major problems and requirements for improvement on source address validation mechanism in ISTN.

2. Terminology

LEO: Low Earth Orbit

GEO: Geostationary Earth Orbit

LSN: LEO Satellite Networks

ISL: Inter-satellite Links

GS: Ground Station

SAVA: Source Address Validation Architecture

SAVI: Source Address Validation Improvements

DHCP: Dynamic Host Configure Protocol

SLACC: Stateless Address Autoconfiguration

DNS: Domain Name System

DDoS: Distributed Denial-of-Service Attacks

CDN: Content Delivery Network

3. Vulnerable Characteristics of ISTN

A satellite constellation is composed of one or more satellite shells. Each shell is organized by a large number of satellites distributed around the earth according to certain design strategies to ensure cooperative performance. Kepler elements can be used to describe the orbit of a satellite. Usually, satellites with an orbital altitude of 400-2000 km are called LEO satellites, and satellites with an orbital altitude of 2000-36000 km are MEO satellites. GEO is a satellite in geosynchronous orbit, with an altitude of about 36000 km from the earth. Satellites in different orbits have their own characteristics [LEO-MEO-GEO]. Table 1 exemplifies typical mega constellations in operation.

Constellation	Altitude (km)	Number of orbits	Number of satellite per orbit
Starlink	550	72	22
	1110	32	50
	1130	8	50
	1275	5	75
	1325	6	75
Kuiper	590	28	28
	610	36	36
	630	34	34
Telesat	1015	27	13
	1325	40	33

Table 1: Typical-mega-constellations.

3.1. Inter-Satellite Links (ISLs)

Comparing with previous satellite communication systems,ene of the most obvious feature of the mega constellation is the use of inter-satellite links. ISL can reduce the delay of satellite network and improve network capacity by avoiding the ping-pong phenomenon and reducing the occupation of the link between the ground station (GS) and the satellite. Although ISL is not used in the initial stage of Starlink deployment, it is still an important part of the future satellite network. Since the launch on September 14, 2021, the satellite version of Starlink has been upgraded to V1.5, and the load of inter satellite laser link is increased [STARLINK-ISL]. As of April 22, 2022, V1.5 satellites have been launched 13 times in total, and the proportion of in orbit Starlink satellites supporting ISL is rising rapidly. The performance of trans-oceanic routes in networks with and without ISL is discussed in [Ground-Relays]. The conclusion is that ISL always have lower delay than ground relay. The most typical configuration is to equip each satellite with four ISLs, which are respectively used to link the front and rear satellites in the same orbit and the two satellites in adjacent orbits [Internetworking]. In fact, ISL does not need to be restricted by

grid topology. It has become a new problem to design ISL configuration to maximize network bandwidth and minimize latency [Motif].

3.2. Open Access Environment

As transmission medium used by satellites, wireless microwave or laser channel, has inferior transmission quality comparing to wired channel. Moreover, the communication between satellites and GSs will be affected by weather, atmospheric conditions, signal attenuation. The transmission channel can be disturbed easily due to the open environment. In addition, the position description information, such as orbit of the satellite, is public. Therefore the motion can be accurately predicted through calculation [GPS-Precision]. This will increase the possibility of premeditated attack. Moreover, due to the global movement of the satellite, the majority of its cycle is in an uncontrolled environment, facing a large number of malicious hosts and users distributed all over the world.

3.3. Dynamic Networks

Due to the extremely fast speed of LEO satellites relative to the ground, it has short-lived coverage for terrestrial users (less than 3 minutes). What's more, under the minmax connection principle, a handover occurs in an average of about 40 seconds [In-Orbit-Computing]. The frequent handover between user terminals and LEO satellites will cause inevitable frequent updating of the IP address.

3.4. Limited Resources

Due to the limitation of rocket capacity, cost and manufacturing technology, satellite design will be subject to many restrictions. The processors on satellites also have worse performance than that of the terrestrial equipment. Up-to-date onboard processor have a CPU frequency ranging from 100MHz to 500MHz, much lower than commercial processors.

In particular, typical performance of spatial processor are as follows. The Cobham GR740 [GR740] is a 65 nm CPU with a 32-bit quad-core architecture that operates at 250 MHz with estimated power dissipation of under 1.5 W. The BAE Systems RAD5545 [RAD5545] is a 45 nm CPU with a 64-bit quad-core architecture that operates at 466 MHz with estimated power dissipation of under 20 W. The Boeing Maestro [Maestro] is a 90 nm CPU with a 64-bit 49-core architecture that operates at 350 MHz with estimated power dissipation of under 22.2 W. A space-grade 32 nm CPU HPSC [HPSC] with 64-bit dual quad-core architecture is considered that is currently being developed by Boeing, which is estimated to operate at 500 MHz with power dissipation of under 10 W.

3.5. Threat from Source Address Spoofing

The report [GLOBAL-DDoS] shows that attacks occur increasingly in satellite systems. In 2019, attacks on satellite systems increased 255 percent. Some hackers begun to attack the satellite constellations, rather than the previous ones on satellite monomers. DDoS attacks against satellite networks have feature of low-cost and low-detectability. And by congesting of the target link, or exploiting some vulnerable characteristics, the satellite networks are as vulnerable to DDoS attacks as terrestrial networks [ICARUS].

In the past, the attacks on satellite communication systems, such as eavesdropping, interference and frequency blocking mainly occur in the physical layer. The use of the ISL in ISTN increases the vulnerability of network layer and above. The attack object expands from satellite monomer to satellite network, and the attack method evolves from physical layer to higher layer.DDoS attack [DDoS-Attack] is one of the most common attack in network layer. Cisco predicts that the number of DDoS attacks will increase to 154 million worldwide in 2023 [Cisco-Report]. Through the query and test of DNS services in 62000 autonomous domains around the world, it is found that more than half of the networks are in danger of being DDoS attacked because they do not validate the source address of packets [Dns-Security].

Due to limited computing resource, lack of traceability, and exposure to the uncontrolled environment, source address spoofing attacks in ISTN are more severe than that in the terrestrial network.

3.6. Existing Solutions and Failure Analysis

Many measures have been actually deployed on the Internet to resist DDoS attacks, but they are difficult to adapt to the new features of mega-constellations and can not work as effectively as in terrestrial networks.

Professional firewall: identify and isolate the traffic according to some characteristics of the traffic to prevent malicious traffic from entering the network. Such firewalls are usually additional hardware, and their weight and volume greatly increase the cost of satellite launch. In addition, the energy consumption required for its high performance is also unbearable for satellites.

Scrubbing center: transfer the flow to the scrubbing center, filter and scrub it, and then return the normal flow to the original server. Traffic will occupy a lot of link bandwidth in the process of leading out and returning, increase the probability of congestion and occupy the traffic of normal users. In addition, due to the need to transfer to the scrubbing center, this operation will bring additional detour delay depending on the deployment location of the scrubbing center.

Equipment upgrade: upgrade the server, gateway and other equipment to improve the tolerance of large traffic. Once launched, the satellite will continue to move at a high speed in space, and it is difficult to upgrade its hardware in the future. Therefore, its bandwidth and processing speed, which are heavily dependent on the performance indicators of the hardware, can basically be considered as non scalable.

Source address validation: filter address spoofing packets and locate malicious users in the network through the traceability of source address [RFC5210][RFC7039][RFC7513][RFC8074]. In the terrestrial network, source address validation mechanisms such as SAVI have been deployed and proved effective to a certain extent. SAVI is an endogenous security mechanism at the protocol level and has little dependence on hardware. It is one of the most promising solutions to be transplanted to the ISTN scenario. However, due to the vulnerable characteristics of satellite constellations described in 3.2, 3.3 and 3.4, SAVI mechanism cannot be used directly in ISTN.

4. Problems of Source Address Spoofing in ISTN

4.1. Understand The Necessity of Onboard Source Address Validation

The most effective deployment scheme of SAVI is to deploy on the first hop switching device. In the traditional satellite communication system, the satellite adopts "bent-pipe-only" model, that is, satellites only relay terrestrial users' radio signals to the fixed ground stations without ISLs or routing. As ground station location is fixed, the storage location of anchor binding information is fixed accordingly. Therefore, the SAVI mechanism can take effect stably at a low cost in terrestrial networks.

ISTN is in a dilemma of vast global traffic and limited ground stations. If the "bent-pipe-only" model is adopted, all traffic on the network will converge to the thimbleful of ground stations. This will generate traffic convergence, resulting in bottlenecks and a sharp decline in network performance. That explains why ISLs are put on the Starlink agenda and routers are the most expected device in the network infrastructure. Further, in such a network structure, the source address validation mechanisms are naturally deployed on satellites.

The source address validation scenario for mega constellations is shown in Figure 1. It is divided into ground segment and satellite segment. The ground segment includes user terminal, authentication server and ground gateway, and is connected to the Internet through ground gateway. The space segment consists of satellites in the satellite Internet (support SAVI and ISL).

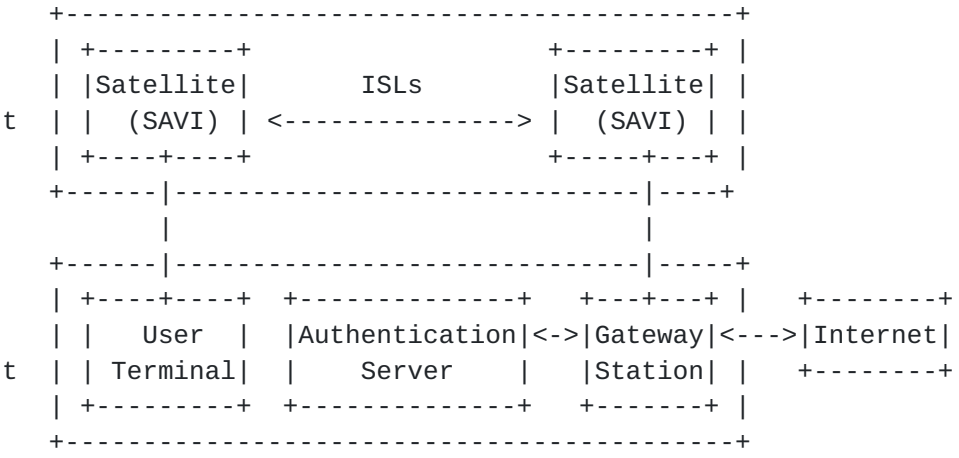

Figure 1: The source address validation scenario for ISTN.

However, in today's time-varying topology LEO satellite networks, SAVI mechanism faces the problem that the anchor binding information stored on the satellite is no longer stable. The router in satellites moves at a high speed, therefore the mobility mechanism in the terrestrial network is no longer effective. There are two possible terms of settlement as follows. Each has its respective unacceptable weaknesses.

4.2. Signaling Storm and Service Interruption

Reauthentication in ISTN contains the following steps according to its network composition:

1. Considering the resource limitation and information security of satellites, the authentication server (such as RADIUS Server) storing user identity information needs to be accessed after reaching the GS through the ISL,

2. The LEO satellite initially accessed by the user terminal acts as an authenticator to initiate an identity authentication request to the authentication server and assign an address to the user terminal,

3. As LEO satellites keep moving at a high-speed relative to ground, user terminals need to switch access to satellites every dozens of seconds,

4. After the handover, the user needs to find a new satellite as the access point and perform the reauthentication and rebinding process to access the network.

A. Signaling Storm

First, the user sends the authentication request to the NCC on the ground through the network for reauthentication process. This process requires multiple signaling interactions between the user and the access satellite, between the access satellite and the NCC. Secondly, the authenticated user executes the address configuration process to obtain the trusted address. In this process, multiple signaling interactions with specific servers or satellites will also occur according to the address configuration mechanism. From the perspective of the whole network, a large amount of users need to perform reauthentication at every moment, and each reauthentication contains a large amount of signaling. Therefore, as shown in Figure 2, if the number of users rises to 97000 under the scale of Starlink phase I, signaling storm occurs, which not only occupies the link bandwidth, but also generates the bottlenecks of NCC and cause bad deterioration of network performance.

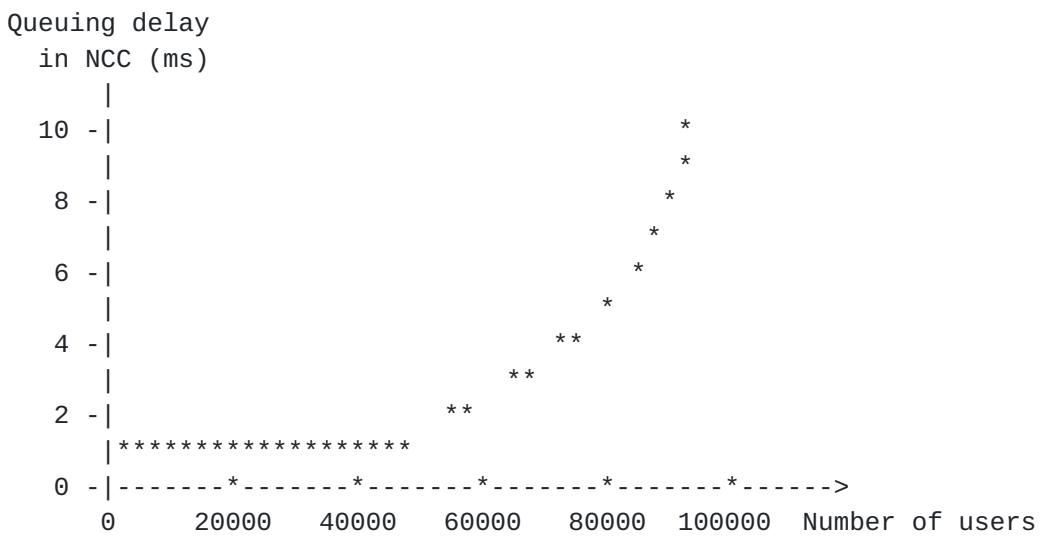

Figure 2: The bottlenecks of NCC.

B. Service Interruption

The legitimacy of user identity and the authenticity of address are the premise of realizing the function of upper layer protocol. During the period from the handover to the successful rebinding, the user cannot use the services at the network layer or above. This will cause interruption of the user's ongoing business. Users need to wait until the completion of the reauthentication process. This seriously affects user experience.

4.3. Delay Deterioration and Bandwidth Occupation

Tunnel forwarding in ISTN contains the following steps according to its network composition:

1. After disconnecting from the access satellite, the user forwards the data traffic to the satellite where the anchor binding information is located through the tunnel instead of reauthenticate or rebind,

2. After receiving the data packet, the satellite with anchor binding information unpacks it to obtain the user's original data packet, and then validates its source address.

A. Delay Deterioration

Since source address validation is required before the packet is forwarded, it needs to be forwarded to the satellite where the anchor binding information is located, and then routed after validation.

This causes traffic detour and additional delay. Moreover, due to the periodicity of satellite movement, after disconnecting from the user, the satellite will gradually move away from the user in half a cycle, and even on the other side of the earth in the worst case. It can be seen from Figure 3 and Figure 4 that the number of hops and time delay from the user are gradually increasing in the first half of the satellite cycle as the satellite brings the anchor binding information moves away.

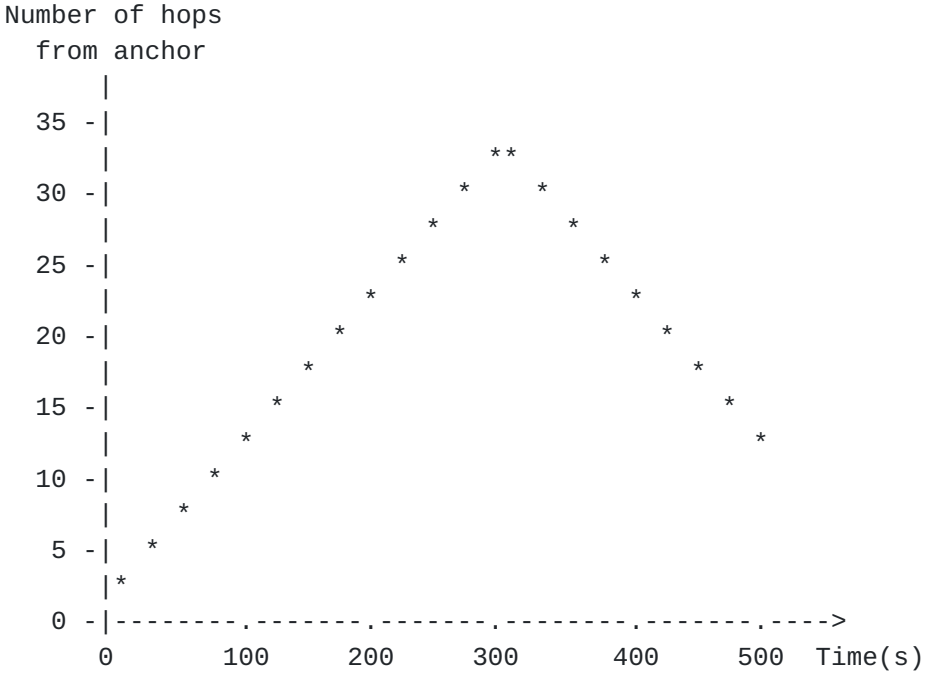

Figure 3: The number of hops from anchor to the user.

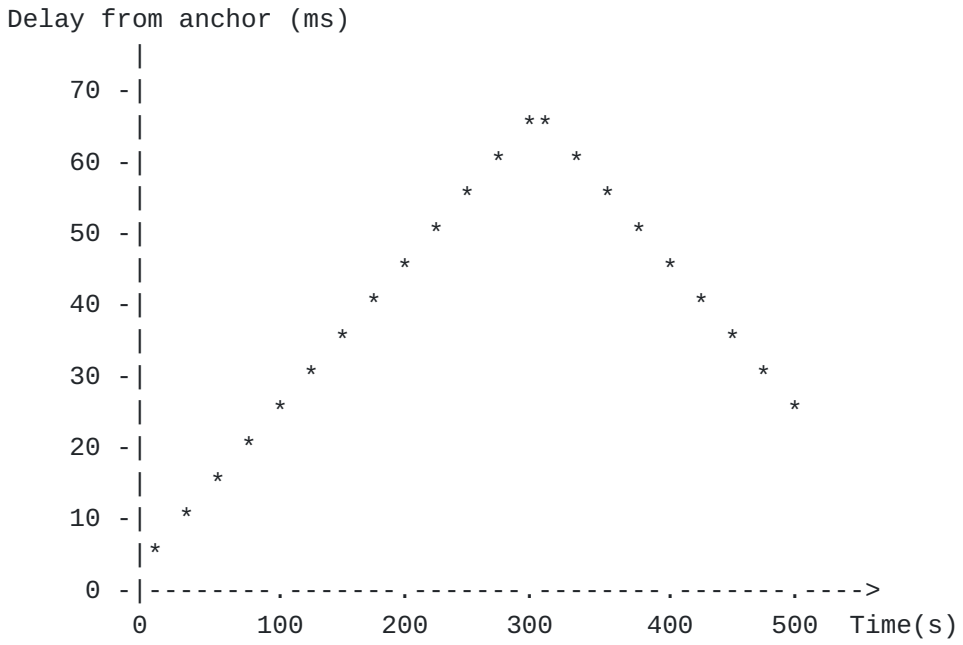

Figure 4: The delay from anchor to the user.

The introduction of such a large additional delay has completely suppressed the low delay advantage of mega constellations.

B. Capacity Deterioration

From the end-to-end perspective, the detour of data traffic causes delay. From the network perspective, the detour of data traffic causes additional ISLs to be used. Compared with the shortest path, tunnel forwarding needs to pass through more ISLs when delivering the same amount of end-to-end traffic, therefore occupying more bandwidth. The reduction of ISL bandwidth leads to the decline of the overall network capacity.

5. Requirements for Improvement on Source Address Validation for ISTN

In order to implement source address validation mechanism in ISTN, the following requirements for improvement should be made:

5.1. Scalability

A reasonable source address validation mechanism should be able to deploy as many satellites and user nodes as possible in ISTN. With the continuous development of constellation and user scale, the handover may occur more frequently, which increases the pressure on the processing capacity of the mechanism. The mechanism should ensure that the network performance indicators such as delay and

bandwidth do not deteriorate significantly, so as to support the long-term development of the network and users. A possible focus is that the signalling interaction process involved in source address validation should avoid bottleneck nodes caused by traffic aggregation in each link.

5.2. Lightweight

Due to on-board resources are very limited, source address validation mechanism should be lightweight. At present, more and more Internet services, such as Content Delivery Network (CDN) [CDN-ISTN], are expected to be extended to satellites. As a basic security support function, the source address validation mechanism should occupy less satellite resources and can be deployed under the limitation of existing satellite resources. Reduce the computing power and memory capacity required by the mechanism, so as to leave more available resources for upper layer services and applications..

5.3. Functional Integrity

The deployment of ISTN is a long-term work. A mega-constellation will require continuous launch and iterative version. A reasonable source address validation mechanism should be designed to ensure that its functional integrity is not limited by the current deployment completion of the constellation. The mechanism should include the processing of incremental deployment of newly launched and deployed satellites, such as database synchronization.

5.4. Transparency to Users

The handover of the physical layer will undoubtedly lead to the interruption of all upper layer services. The source address validation mechanism should be organically combined with the user re access related operations as much as possible to reduce additional operations, so as to ensure the transparency of the physical handover to the user. The goal is to make users unaware when handover at the bottom and running the source address validation mechanism. The delay sensitive Internet services at the top, such as video, conference and game services, can maintain continuity and the advantages of low delay and high bandwidth provided by ISTN.

5.5. Cost Stability

The operations involved in source address validation will inevitably bring a certain amount of cost. In order to limit the cost to a controllable range, it should be decoupled from the deployment location of the ground station and the real-time location of the initial access satellite. It has been proved in experiments that if the rebinding process after handover needs to visit the ground station or the initial satellite, it will introduce great volatility to the cost.

6. Acknowledgements

7. IANA Considerations

This memo includes no request to IANA.

8. References

8.1. Normative References

[RFC5210] Wu, J., Bi, J., Li, X., Ren, G., Xu, K., and M. Williams, "A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience", RFC 5210, DOI 10.17487/RFC5210, June 2008, <https://www.rfc-editor.org/info/rfc5210>.

[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

[CDN-ISTN] Yang, S., "A Synergic Architecture for Content Distribution in Integrated Satellite and Terrestrial Networks", 2020.

[Cisco-Report]
"Cisco Annual Internet Report (2018–2023) White Paper", 2018, <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspective s/annual-internet-report/white-paper-c11-741490.html>.

[DDoS-Attack]
Elion, J., "Distirbuted denial of sevrice attack and the zombie ant effect", 2000.

[Dns-Security]
Deccio, C., "Behind closed doors: A network tale of spoofing, intrusion, and false dns security", 2020.

[GLOBAL-DDoS]
"GLOBAL DDoS THREAT REPORT", 2019, <https://business.blogthinkbig.com%2Fwp-content%2Fuploads%2Fsites%2F2%2F2020%2F02%2FGTSA_Etisalat_DDoS_v2.pdf>.

[GPS-Precision]
Kelso, T., "Validation of SGP4 and IS-GPS-200D Against GPS Precision Ephemerides", 2007.

[GR740]
Hjorth, M., "GR740: Rad-Hard Quadcore LEON4FT System-on-Chip", 2017.

[Ground-Relays]
Handley, M., "Using ground relays for low-latency wide-area routing in megaconstellations", 2019.

[HPSC]
"High Performance Spaceflight Computing (HPSC) Processor Chiplet", 2017.

[ICARUS]
Giuliari, G., "ICARUS: Attacking low Earth orbit satellite networks", 2021.

[In-Orbit-Computing]
Bhattacherjee, D., "In-orbit Computing: An Outlandish thought Experiment?", 2020.

[Internetworking]
Wood, L., "Internetworking with satellite constellations", 2001.

[ITU-6G]
"ITU 6G vision", <https://www.itu.int/dms_pub/itu-s/opb/itujnl/S-ITUJNL-JFETF.V1I1-2020-P09-PDF-E.pdf>.

[Kuiper]
"Kuiper", <https://en.wikipedia.org/wiki/Kuiper_Systems>.

[LEO-MEO-GEO]
Vatalaro, F., "Analysis of LEO, MEO, and GEO Global Mobile Satellite Systems in the Presence of Interference and Fading", 1995.

[Low-Latency-in-Space]
Handley, M., "Delay is not an option: Low latency routing in space", 2018.

[Maestro] Suh, J., "Implementation of Kernels on the Maestro Processor", 2013.

[Motif] Bhattacherjee, D., "Network topology design at 27,000 km/hour", 2019.

[Networking-in-Heaven]
Klenze, T., "Networking in heaven as on earth", 2020.

[Nttdocomo-6G]
"NTTDPCOM 6G White Paper", <https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_20200124.pdf>.

[OneWeb] "OneWeb", <https://en.wikipedia.org/wiki/OneWeb>.

[RAD5545] Berger, R., "Quadcore Radiation-Hardened System-on-Chip Power Architecture Processor", 2015.

[Starlink] "Starlink", <https://en.wikipedia.org/wiki/Starlink>.

[STARLINK-ISL]
"Starlink Block v1.5", 2021, <https://space.skyrocket.de/doc_sdat/starlink-v1-5.htm>.

[Surrey-6G]
"Surrey 6G vision", <https://www.surrey.ac.uk/sites/default/files/2020-11/6g-wireless-a-new-strategic-vision-paper.pdf>.

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@mails.tsinghua.edu.cn

Qian Wu
Tsinghua University
Beijing 100084
China
Email: wuqian@cernet.edu.cn