IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 August 2022, accepted 6 September 2022, date of publication 8 September 2022, date of current version 16 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3205426

SURVEY

Security of Satellite-Terrestrial Communications: Challenges and Potential Solutions

IJAZ AHMAD[1], (Member, IEEE), JANI SUOMALAINEN[1], PAWANI PORAMBAGE[1,2], (Member, IEEE), ANDREI GURTOV[3], (Senior Member, IEEE), JYRKI HUUSKO[1], AND MARKO HÖYHTYÄ[1], (Senior Member, IEEE)

[1]VTT Technical Research Centre of Finland, 02044 Espoo, Finland
[2]Centre for Wireless Communications, University of Oulu, 90570 Oulu, Finland
[3]Department of Computer and Information Science, Linköping University, 58183 Linköping, Sweden

Corresponding author: Ijaz Ahmad (ijaz.ahmad@vtt.fi)

This work was supported in part by the CF_Space Project funded by VTT, in part by the AI-NET-ANTILLAS Project funded by Business Finland, and in part by 6G Genesis Flagship Project under Grant 318927. The work of Andrei Gurtov was supported by Automation Program II, Trafikverket and EU AiRMOUR Project under Agreement 101006601.

ABSTRACT The integration of satellite and terrestrial networks has become inevitable in the next generations of communications networks due to emerging needs of ubiquitous connectivity of remote locations. New and existing services and critical infrastructures in remote locations in sea, on land and in space will be seamlessly connected through a diverse set of terrestrial and non-terrestrial communication technologies. However, the integration of terrestrial and non-terrestrial systems will open up both systems to unique security challenges that can arise due to the migration of security challenges from one to another. Similarly, security challenges can also arise due to the incompatibility of distinct systems or incoherence of security policies. The resulting security implications, thus, can be highly consequential due to the criticality of the infrastructures such as space stations, autonomous ships, and airplanes, for instance. Therefore, in this article we study existing security challenges in satellite-terrestrial communication systems and discuss potential solutions for those challenges. Furthermore, we provide important research directions to encourage future research on existing security gaps.

INDEX TERMS Security, network security, satellite, satellite security, communications security, NTN security.

I. INTRODUCTION

Satellites have seen a great deal of innovation from many dimensions such as orbital locations, physical sizes, functional capabilities, and services. Moving from traditional Geostationary (GEO) satellites toward Low Earth Orbit (LEO) satellites brings considerable improvements, specifically in terms of higher throughput and lower latency and energy consumption [1]. Furthermore, comparatively less exposure to physical threats and natural disasters as well as cost-effective global coverage make satellites a favorable choice for remote connectivity. Therefore, the integration of satellites with terrestrial networks such as 5G have gained a lot of research momentum [2], [3].

Future communications networks will utilize satellites for enabling connectivity in areas and situations where terrestrial networks have difficulty in continuous connectivity. Such areas can be remote locations on ground, sea, and in space. The situations constitute many dimensions, including normal activities such as gathering of huge crowds and increased mobility of user equipment, and non-normal activities including human-caused accidents and natural disasters such as earthquakes, wildfires, etc. Due to higher coverage, satellite communications can be rapidly installed through enabling programmable run-time deployment capability in satellite communications. Therefore, the Third Generation Partnership Project (3GPP) has initiated standardization efforts to integrate Non-terrestrial Networks (NTN) to Terrestrial Networks (TN) such as 5G [4]. The term NTN includes satellites, High Altitude Platforms (HAPs), and Unmanned Aerial

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

Vehicles (UAVs). The focus in studies has been on the use of satellites and thus, we will also focus on satellite-terrestrial aspects in this paper.

3GPP pointed out three main areas where the integration of NTN with TN is important [4]. These are as follows:

- Improve the roll-out of 5G services in isolated and remote areas, on board aircrafts and vessels, and hlin sub-urban or rural areas to upgrade the performance of limited TNs in a cost-effective manner.
- Reinforce the reliability of 5G services by providing service continuity for Machine-to-Machine (M2M) and Internet of Things (IoT) devices or passengers in moving platforms such as ground-based vehicles, aircrafts, ships, and high-speed trains, etc.
- Increase the scalability of 5G through providing multicast and broadcast resources for data delivery toward the network edge or end-user device.

Satellite and 5G networks systems have experienced growth in adapting diverse technologies in each. For instance, satellites have begun to miniaturize in size and adopt the notion of programmability. 5G networks have also moved toward smaller cell sizes and adopted programmability from the core to Radio Access Networks (RANs). However, each of these attributes of satellites and 5G have their own security implications. For example, the small sizes of satellites make it challenging to deploy complex security techniques due to lack of resources on board. Similarly, programmability also opens doors for malicious applications. 5G also has similar challenges, with increased handover signaling potential creating bottlenecks and openness to malicious applications.

Along with their own challenges, integrating satellites with terrestrial communication systems can further increase the security challenges if proper attention is not paid to security weaknesses in each. The recent report of a cyber attack on the Viasat satellite (KA-SAT) network [5] in Ukraine reveals that security is already a major challenge in satellite communications. The cyber attack left modems inoperable in Ukraine and led to thousands of disruptions in organizations across Europe. The ground-based intrusion entered operator's management system by exploiting a misconfiguration and then instructed a large number of residential satellite modems to drop from the network. The incident reveals that the overall integrated system will have a higher degree of vulnerability and higher security threat landscape if technologies with security weaknesses and loopholes are integrated together. Therefore, in this article we study the potential security challenges in integrated TN-NTNs, and provide possible security solutions. We also highlight the existing research gaps that need immediate attention for further research.

This article is organized as follows: Section II discusses the background with a brief overview of the integration of satellite and terrestrial networks, and highlights the related work and contributions of this article. Section III reviews the existing security challenges from the perspectives of communications in satellite-to-satellite, satellite-to-ground stations, and satellite-to-User Equipment (UEs). Section IV discusses security solutions for the most prominent challenges from the same perspectives as in the prior section. Section V provides interesting future research directions, and the article is concluded in Section VI.

II. BACKGROUND

A. INTEGRATION OF SATELLITE AND TERRESTRIAL NETWORKS: A BRIEF OVERVIEW

Traditionally, satellite and terrestrial communication systems have been studied and developed along separate, parallel tracks. It is pretty obvious that satellite-terrestrial networks have multiple benefits over the conventional cellular networks. Among many such advantages like higher performance in time delay, increased mobility, and flexibility with more supporting technologies, we can see the most significant benefit as the elimination of geographical limitation to achieve the network integration and coverage globally. As a result satellite-terrestrial networks play an important role in the envisioned 6G era. Satellite connections are mostly used in places where terrestrial networks cannot provide connectivity, and the Digital Video Broadcasting standard for satellites (DVB-S2X) currently forms the basis for digital satellite transmissions across the globe [6]. Terrestrial networks can use DVB-based satellites, e.g., as backhaul connections but there is no tight integration between the separate networks.

3GPP has been developing the NTN standard to enable tighter integration between TN and NTN segments in order to improve availability of the 5G connections [7], [8]. The inclusion of satellites in 5G and 6G networks will increase ubiquity and global coverage, and support mobility for any platform regardless of location [3]. Satellites will also enable resilient connections in challenging communication scenarios such as emergency responses. There are two main ways for integration. First, in direct access mode the end user device is directly connected to the satellite similarly to the terrestrial base station. This enables accessing satellite services anywhere with the typical the mobile phone. Secondly, there is indirect access possibility where the end user terminal is connected to the terrestrial base station that is connected to the 5G core network via a satellite. This is also called backhauling.

Satellite-terrestrial communications represent a complex eco-system, as shown in Fig. 1. The whole eco-system is presented in three distinct types of satellites, such as GEO, Medium Earth Orbit (MEO) and LEO interconnected to each other and with terrestrial networks through ground stations or capable UEs. Considering HAPs as intermediaries, connected to satellites and terrestrial networks, eleven connectivity and communication points have been highlighted. There can surely be a higher number of connectivity options; however, in this article we focus on these as presented on the left side of Fig. 1. These connectivity models are described in Table 1.

Safety and security are essential parts to be taken care of in order to provide services to future generations. In 5G the integration of satellite and terrestrial components will still

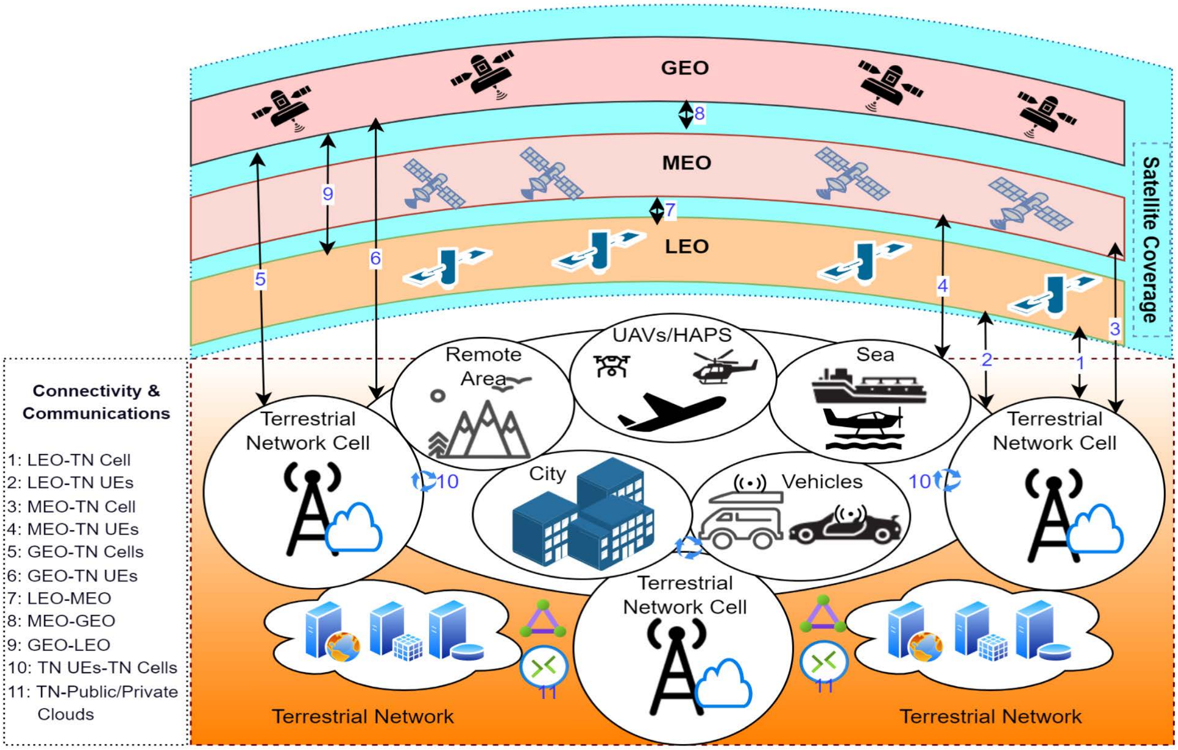


FIGURE 1. Generic architecture showing integrated terrestrial and non-terrestrial networks.

TABLE 1. Description of communication channels and links in the eco-system.

Communication Link	Description
1: LEO-TN Cell	Comm. links between LEO and base stations in TNs
2: LEO-TN UEs	Comm. linkss between LEO and UE in TNs.
3: MEO-TN Cell	Comm. links between MEO and base stations in TNs
4: MEO-TN UEs	Comm. links between MEO and UE in TNs
5: GEO-TN Cells	Comm. links between GEO and base stations in TNs
6: GEO-TN UEs	Comm. links between GEO and UE in TNs
7: LEO-MEO	Comm. links between LEO and MEO
8: MEO-GEO	Comm. links between MEO and GEO
9: GEO-LEO	Comm. links between GEO and LEO
10: TN UEs-TN BSs	Comm. links between UEs in TN and base stations in TNs
11: TN- Clouds	Comm. links between TNs and public/private clouds

be in the early phases, whereas in 6G the integration will be much higher. Figure 2 shows a functional diagram of the integrated network. It highlights central functional elements in 3GPP NTN. UE connects either through a satellite terminal or directly through the satellite or terrestrial network. Base stations, or gNBs, with rectangles of different colors in the figure, may locate either a) close to the user and use the satellite as a backhaul, b) in orbit, or c) behind the satellite access network and close to the core network and application services. Rounded green rectangles mark baseline security functions that are related to specific components or interfaces and that will be discussed more closely in the following sections.

B. RELATED WORK AND OUR CONTRIBUTIONS

A number of surveys have been published on the theme of satellite-terrestrial communications. Previous security-related surveys include work by Jiang *et al.* [9]. Their magazine article discusses several high-level challenges in space information networks, including security transmission control, secure key management, and secure routing. We extend the discussion with a more comprehensive listing of security challenges and a broader handling of potential research areas. The security of 5G and satellite converged communication networks was reviewed by Yan and Teng [10] who presented a security architecture, which emphasized four key protection technologies: identity authentication, lightweight communications security, availability enhancements, and fine-grained resource sharing and isolation. We present an alternative analysis with extended threat analysis, while also covering hierarchical multi-layered satellite infrastructure. Manulis *et al.* [11] surveyed security challenges in new space, i.e., in new and proposed private sector satellite constellations consisting of low-cost satellite equipment. They covered security from the perspective of ground, space, and user segments, as well as communications and regulation. While their focus was wide, it did not cover the 3GPP integration that is within our scope. Similarly, Guo *et al.* [12] presented a survey on security of space, air, ground, and sea integrated networks. The article elaborates the architecture and then delves into the characteristics. Security threats are discussed from the perspectives of physical threats, operational threats, network threats, and data threats. The attacks are categorized into jamming attacks, eavesdropping attacks, Denial of Service (DoS) attacks, and spoofing attacks. The countermeasures are discussed under

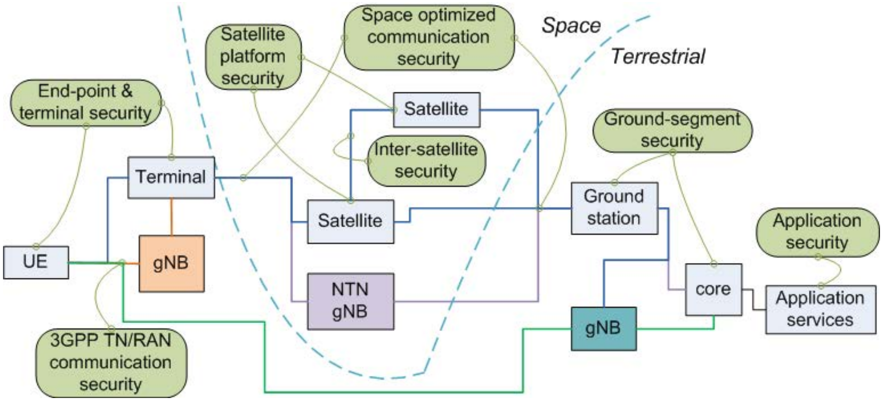


FIGURE 2. **Functional architecture for integrated network, which illustrates baseline security requirements (green rounded rectangles) and alternatives for base station (gNB) placement.**

anti-jamming attacks, secure routing, secure handover schemes, secure key management, and intrusion detection systems. While our survey overlaps partly with their article, we present an alternative communication domain-based categorization, apply alternative approach for solution analysis, and focus on 3GPP NTN.

Standardization efforts are essential to improve security of satellite-terrestrial communications. Standardization parties have specified baseline security requirements, architecture, and protocols both for mobile communication networks by 3GPP [13] and for space communications by Consultative Committee for Space Data Systems (CCSDS) [14], [15], [16]. However, it remains an open question as to what security solutions the forthcoming releases of integrated 3GPP NTN networks will adopt. We will contribute to these standardization and implementation efforts by surveying and analyzing security requirements and options for future NTN networks.

A generic satellite network survey by Kodheli *et al.* [1] addresses satellite communications in the new space era, consisting of satellite and terrestrial networks. Their focus is on architectures, use-cases, opportunities, and challenges in space-based communications, but they also discuss some security interests such as physical layer security. Similarly, Liu *et al.* [17] also discuss some security aspects in their generic survey on space-air-ground integrated networks. We provide more detailed treatment and categorization of challenges and solutions, and thus enable more detailed and comprehensive analysis of the security requirements.

5G use cases, technologies, and standardization activities are covered in [2] and [8]. Recently, the inclusion of large LEO constellations and visions toward three-dimensional 6G systems have been studied [3], [18], [19] and sustainability aspects of the satellite-terrestrial systems emphasized. A survey of non-terrestrial networks and its integration into future 6G networks with challenges and opportunities is presented in [20]. There are also other survey articles that discuss the satellite-terrestrial integrated networks on a general level, such as [12] and [21]. We acknowledge developments presented in these papers and provide a complementary security analysis. The main contributions of our article include:

- A study of the security landscape of the integrated satellite and terrestrial networks.
- An outline ofthe main security challenges in the integrated environment from three perspectives, i.e., i) satellite-to-satellite communications, ii) satellite-to-ground stations communications, and iii) satellite-to-ground UE communications.
- A discussion of the potential solutions for the identified security challenges.
- Bringing forth the existing research gaps in terms of remaining security challenges and interesting foresight on new technologies that can be very useful in providing efficient security.

In the following section, we begin the discussion with the most important security challenges.

III. SECURITY CHALLENGES

Future networks will be hybrid in nature, consisting of ground stations and users integrated with satellite components acting as relay nodes or even providing direct connectivity to users on the ground or HAPS, resulting in an integrated space-ground connected global environment [22]. The security challenges in the integrated environment are highly complicated due to the complex nature of independent technologies being combined. Furthermore, traditional security approaches do not suffice for the challenges arising due to the nature of satellite communications, such as higher latency and higher bit error rates. For example, the integration of Internet Protocol Security (IPsec) [23] has been as evaluated in [24] to have interoperability issues with Transmission Control Protocol (TCP). Moreover, the TCP performance degrades severely in satellite communications due to its congestion control algorithm, which is not suitable for such channel impairments. Therefore, security challenges can also arise due to issues other than direct cyber attacks.

The most suitable way to draw important conclusions is to first dive deep into the security challenges of each technology, and then shed light on possible solutions to those challenges. The security challenges and potential solutions for the important reference points, shown also in Fig. 1, can be categorized into:

- Satellite-to-Satellite Communications: Communications between all types of satellites, such as within GEO, MEO, and LEO, as well as inter-orbital communications such as between GEO and MEO, GEO and LEO, and MEO and LEO. Communication reference points: (7, 8, 9).
- Satellite-to-Ground Stations: Communications between satellites and ground stations such as base stations of cellular networks and other gateways that connect satellites to user-equipment. Communication reference points: (1, 3, 5).
- Satellite-to-Users: Communication between satellites and directly user devices on the ground, including urban and rural areas, as well as sea high-altitude platforms. Communication reference points: (2, 4, 6).

Each of these have different security implications, challenges and solutions. The communications, however, occur in a broadcast manner, which can cover a big geographic area on earth, and thus exposes communication secrecy if proper measures are not in place. Therefore, we must first properly identify the security challenges and then discuss the potential security solutions. Below, we discuss the security challenges in each of these.

A. SATELLITE-TO-SATELLITE COMMUNICATIONS

A survey of key security technologies of space information networks is presented in [25]. The article introduces different types of satellites such as GEO, MEO, and LEO, and then discusses a generic space information network architecture. The most important security requirements outlined in [25] are data confidentiality and integrity, key management, and authentication and access control. There are a number of security challenges in ensuring security of satellite-to-satellite communications. For example, satellites have limited resources in terms of storage, computation, and energy which are usually dedicated to specific functions such as monitoring and reporting various activities on earth. Therefore, security approaches that require greater resources, such as strong encryption techniques, are not applied. Moreover, satellite-to-satellite communications happen in a broadcast fashion that require strong encryption. Thus, confidentiality and integrity of communications can be compromised.

The difference in altitude and mobility among satellites in the three layers, i.e., GEO, MEO, and LEO, make some of the encryption techniques more challenging, mainly due to complexity in key distribution. First, asymmetric key cryptographic protocols require a universally trusted third party to issue, maintain, revoke, and manage certificates. However, due to the mobility of satellites, a lot of challenges exist in such systems, including higher latency and routing load in route discovery [26]. Performance Enhancing Proxies (PEPs) are introduced in satellite systems to overcome the limitations in the operating environment for TCP/IP. However, there are still challenges in the coordination of the TCP/IP security technique, IPsec, and PEP regarding extracting information from packet headers without compromising confidentiality of information and payload therein.

A survey of secure routing protocols for satellite networks is presented in [26]. The article elaborates security threats to satellite networks based on the routing process. Once a routing protocol is attacked and compromised, communication can be interrupted and disclosure can occur. Routing attacks can be generally be categorized into internal and external attacks. In an internal attack, satellite nodes can be captured and programmed, whereas, in an external attack the attacker does not have authorization to access the network. The attacks can target route discovery, data delivery, and route maintenance. The article [26] elaborates that routing attacks can cause unnecessary routing discovery requests, add invalid routes, increase packet loss, change network topology, and exhaust network resources, for instance.

B. SATELLITE-TO-GROUND STATIONS COMMUNICATIONS

Satellite-to-Ground stations communications, both in the downlink and uplink direction, will be the main part of the integrated system enabling satellite-terrestrial communications. The aim of NTN is to integrate these technologies into 5G to increase and boost connectivity. However, proper investigation from many aspects such as compatibility and security must be carried out. For instance, many of the technologies used in terrestrial networks, such as 5G, will have adverse effects due to higher latency and higher error rates [2]. Similarly, the security of 5G will have direct implications on the end-to-end security of integrated systems. Therefore, the security challenges in this context must be brought forth.

5G networks can be exposed to a number of security challenges due to the introduction of programmability and openness in the 5G infrastructures, as well as the integration of technologies such as IoT having their own security weaknesses exposing the network to even greater threat landscape [27]. For example, 5G uses the concepts of software-defined networking to enable programmability at run-time. These technologies, i.e., Software Defined Networking (SDN) and Network Function Virtualisation (NFV), are now proposed for satellite networks and have many benefits therein [28]. However, such programmable architectures can expose the network to an injection of malicious software, and provide privileges to applications that can bypass important security controls [29]. Similarly, the opennes in RAN components such as proposed by ORAN, leveraging on SDN and NFV to enable programmability, exposes RAN to the security threat that prevail in open source software, as discussed in [30]. Furthermore, satellites are also moving in the direction of programmability, i.e, leveraging software-defined payloads. Enabling satellites to be patched with software-defined payloads may open up further vulnerabilities due to immaturity of on-orbit reprogramming technologies. Since satellites and ground components are integrated products with hardware and software components from different manufacturers, such openness may also open the whole system up to security vulnerabilities. The main reason for such vulnerabilities stems from different and usually incongruent security practices and policies. Therefore, the satellite to ground communications segment of the whole system is highly complicated.

The ground stations mainly act as a gateway between satellites and users. Therefore, they also handle the compatibility issues before bridging the users to satellites. The ground stations, however, can be coupled with more computing and storage capabilities with the emergence of edge computing or multi-access edge computing. The same is not yet demonstrated for the onboard satellite gNBs. Therefore, efficient security techniques that require higher computing resources, for instance recent intrusion detection techniques and encryption schemes with larger key sizes, are still not viable for satellite gNBs due to limited onboard processing, storage, and energy resources. Therefore, there will be issues in both network layer (routing) security and link layer (interference) security, as discussed in [21].

There are also threats of direct security attacks such as jamming attacks, DoS attacks, spoofing attacks, etc. Jamming attacks introduce interference in communication channels to cause unavailability of communication channels between legitimate users [31]. In satellite-TNs, the challenge of jamming attacks is higher due to the higher coverage area of satellites and thus higher exposure to jamming attacks. Details about different types of jamming attacks and countermeasures are discussed in [31].

Furthermore, the non-compatibility of 5G security approaches must also be studied. There are amendments to existing wireless (5G) systems to make it interoperable with satellite systems, such as TCP PEP agents and extension [32]. However, as the TCP performance degrades [9], the necessary security techniques used therein also suffer. For example, satellite internet performance measurements are carried out in [33]. The authors reveal that using Virtual Private Networks (VPNs) and Transport Layer Security (TLS) further deteriorate the performance. Furthermore, TCP connections over VPN tunnels cannot benefit from PEPs.

Ground stations and connected systems are vulnerable to insider threats and intrusions from advanced adversaries who are able to circumvent the first lines of defences. Researchers have demonstrated attacks on maritime systems via SatCom vulnerabilities, allowing them to take control of vessels' steering, potentially causing collisions or running them aground [34]. The main weakness was the use of default or weak administrator passwords in the SatCom terminals. For example, Inmarsat and Cobham SatCom terminals can be found through a search on Shodan, a search engine for the Internet of Everything, and present an easy target for hackers. Satellite infrastructures are thus monitored to ensure that the security is functioning as expected. The Telemetry, Tracking and Control (TT&C) stations, controlled by the satellite operators, perform the control of satellites that include the monitoring of satellite subsystems, perform tests, and update configurations. The ground stations are controlled by the terrestrial network operators with traditional network control and monitoring systems.

Security monitoring should cover cyber attacks in the network and application layers, but also physical interference in the electromagnetic spectrum and kinetic threats from other space objects against onboard components. Cybersecurity-specific monitoring-related challenges include regulatory compliance issues, e.g., privacy or lawful-interception, as the satellite services are not bound to borders; scalability as the size of data from integrated infrastructure is large; as well as distributed global infrastructure, which may cause, e.g., delays to analysis and log timestamp synchronization issues. Central challenges for monitoring also include heterogeneous data sources and a lack of tools that can collect and analyze satellite-specific metrics. Satellite infrastructure consists of specialized devices producing log data in their own formats. Satellite systems differ considerably from terrestrial systems, e.g., considering delay and jitter. Thus, a monitoring system designed for known terrestrial patterns of normal or adversarial behaviors does not function well in the space domain.

C. SATELLITE-TO-USER EQUIPMENT COMMUNICATIONS

Satellite-to-user equipment security has many dimensions and dependability challenges. The user equipment can be very diverse and, therefore, have very diverse security requirements. For instance, HAPs, UAVs, and terminals in the sea will have different requirements than those of normal smartphones. Furthermore, there are many use cases for the integration of IoT to satellite networks, or using satellite links as backhaul to connect distant IoT devices to the mainstream network infrastructures such as 5G. Moreover, security challenges can arise from the physical attributes of user equipment such as low computing resources for cryptographic protocols. Similarly, security challenges can also arise from high mobility of user equipment.

Security challenges can arise due to frequent handovers between a highly mobile ground user and satellites [17]. For example, a hand-off scenario is discussed in [9] in which an airplane changes connection from an LEO to a GEO. The authors point out that the signaling messages carrying information about a previous point of attachment, an LEO in this case, can be eavesdropped, falsified, or fabricated. Furthermore, due to greater delays in vertical handovers between satellites in different layers, additional security approaches such as authentication and encryption make achieving higher security difficult and complicated, leaving room for security breaches. Another important challenge related to mobility of users connected to satellite networks is the authentication of the user, with acceptable delays, during roaming. It has been studied in [35] that most of the existing techniques do not suffice for satellite communications. The main reason for such challenges is higher latency and the exposed nature of the links. Usually satellite links are preferred for HAPs, which can operate anywhere and have quite high mobility.

However, mobility increases the need for secure authentication during handovers.

Air traffic communication systems make the most prominent use-case for satellite-to-UE communications. Wireless technologies in most of air traffic communication systems are insecure from a general perspective, as discussed in a study on security of next-generation air traffic communication networks [36]. The author outlines that since most of the technologies were developed without proper consideration to security, most of the aviation communication is insecure. The broadcast nature of communications makes it fairly easy to eavesdrop on communications. A variety of security attacks that can be used in aviation communication have been discussed in [36], ranging from jamming to message insertion and deletion, to mounting attacks on information and control systems. Researchers revealed that on-board Wi-Fi for passengers can enable access to airplane SatCom equipment on the same network [37]. It could provide SatCom access without any authentication, using the default password or weakness in the software. In some cases, SatCom terminals have even became a part of IoT botnet such as Gafgyt or Mirai. Security of the Controller-Pilot Data Link Communications (CPDLC) is investigated in [38] and [39]. The authors claim that most of the communication happens in plain text, leaving room for confidentiality and integrity threats, besides other security challenges in communication between pilots and Aviation Traffic Control (ATC) systems and persons. Interested readers are referred to [36] for detailed information on these topics.

The Internet Engineering Task Force (IETF) has recommended an authentication header protocol, Encapsulating Security Payload (ESP) [40] of IPsec, and Internet Key Exchange (IKE) [41] for secure message transmission. However, IKE relies on public key authentication or pre-shared keys, making it difficult to deploy IPsec due to higher latency and overhead costs. Furthermore, high bit error rate and long link delays make it difficult to deploy most encryption techniques. Moreover, the costs of encryption overheads lead to a trade-off between security and encryption costs, resulting in a security compromise [9]. Other than TCP, the Transport Layer Security and Secure Socket Layer (TLS/SSL) also have challenges arising due to server-client handshake and respective delays in keying mechanisms. The newest version TLS 1.3 [42] optimizes security handshake by reducing message exchange between client and server from four-way to two-way, and thus minimizes the session setup delay. Identity-based cryptography addresses also challenges related to high computational costs, which are problematic in satellite systems.

Another important challenge is related to key management, which has been on the forefront of communication security of satellite networks [9], [43]. All cryptography-based security technologies involve key management. Therefore, key management is important in every layer that requires encryption or security protocols. In satellite-to-user communications, key management becomes highly challenging due to the motion of satellites and extremely wide geographic area of coverage, making it highly complicated to build a powerful key management center.

IoT has made a huge leap in recent years where its integration to 5G has played the main role [44] and is researched for satellite connectivity [45]. However, major IoT devices studied recently [46] reveal that little attention has been paid to security except IIoT systems. Satellite connectivity enables the integration of vulnerable IoT devices dispersed over a highly distributed geographic area [47]. Such connectivity provides an opportunity for intruders to exploit the inherent weaknesses to mount Distributed Denial of Service (DDoS) attacks. Since most IoT devices have low computing and storage resources, deploying efficient security technologies is also difficult. Therefore, the integration of IoT into the satellite ecosystem poses a serious security challenge and must be further investigated in this regard.

Furthermore, critical infrastructures need satellite connectivity as the sole connectivity medium, such as autonomous and remote-controlled ships, specifically in far seas, as discussed in [48] and [49]. Cyber security risk assessment of modern ships is studied in [50], in which the authors provide several examples of security attacks such as compromising entire communication and Global Positioning System (GPS) systems.

In addition to the security challenges, privacy considerations with satellite-terrestrial networks are not widely discussed in the current state-of-the-art of 5G networking technologies. For instance, when base station traffic is offloaded with a proper integration of LEO and terrestrial networks, it can facilitate broadband transmission from satellites. Here it is important to maintain the confidentiality of that traffic for assuring the privacy of the users when the network traffic is offloaded to the terrestrial network. Furthermore, nowadays people are more concerned about their privacy more than ever. When there is a possibility that the collection and offload data may create privacy violations or privacy leakage, users can become the victims of malicious attacks. Once users are more concerned about such attacks, they may not continue to perform the sensing tasks that are engaged with crowd sensing activities.

Satellite-terrestrial crowd sensing is a relatively novel concept that allows real-time data aggregation to ensure worldwide user participation from all regions of the globe to cover a more sophisticated sensing task [51]. Although it covers a wide range of users, this may also endanger user privacy by revealing sensitive information related to the user locations. Since data is collected through the satellites, the precision is also in a higher range where the threat level may increase due to the rising cost of privacy leakage incidents.

To summarize, the security challenges in satellite-terrestrial communications are of a complex nature due to the nature of the eco-system. These challenges are also presented in a concise form in Table 2. The first column in Table 2 represents the types of security threats, such as DoS, routing, and hijacking attacks. The second column provides a brief description, mainly representing the achievable target. The communication links that can be compromised are presented next, with numbers 1-11 for brevity, which are described in Table 1. The communication links are also represented with these numbers in Figure 1. For example, satellite-to-satellite (Sat-Sat) links are represented with links numbered, 7, 8, and 9; satellite-to-Ground stations (Sat-Ground) links are represented with links numbered 1, 2, and 3; and satellite-to-UE (Sat-UE) links are represented with links numbered 2, 4, and 6. Links between terrestrial UEs and base stations are represented with link numbered 10, and links between terrestrial networks and clouds is represented with link numbered 11.

The main challenge wthathich needs immediate research attention is that traditional security approaches used in terrestrial networks are adopted, which do not suffice for satellite communications. However, most of the security challenges that exist in terrestrial networks, such as DoS and jamming attacks, also exist in satellite-based communications. Despite the similarity in challenges, similar solutions cannot be applied due to the latency and high mobility involved. Key management for cryptographic protocols is the most daunting task in this eco-system. Furthermore, the ground-based stations can be used as launchpads for security attacks against connected systems (5G base stations, gateways) and end-user devices (IoT). Conversely, due to the difficulty in applying latest security techniques (e.g., cryptographic protocols), security of the end-user devices is also at stake.

IV. POTENTIAL SECURITY SOLUTIONS

The security solutions for satellite communications are gradually increasing and gaining traction in terms of real-time deployment due constant news of exposures. The security solutions in this domain have also mostly followed the traditional approach of security incident-triggered solutions or patch-and-fix approach. In this section, we discuss the security solutions following the same approach of topics as the previous section.

A. SATELLITE-TO-SATELLITE COMMUNICATIONS

Satellite-to-satellite communications are comparatively secured due to their distant location and thus the complexity involved in mounting security attacks. For example, jamming attacks will require a jamming device producing higher interference in the same orbit and moving at the same speed. Similarly, DoS attacks are not simple and therefore there is a limited number of such attacks on satellite networks, mainly delimiting the non-state actors who do not have sophisticated devices to mount such attacks. Furthermore, the challenges that can be common in other communications, such as eavesdropping are also extremely difficult in satellite-to-satellite communications. In LEO satellites, simple solutions, such as using satellite diversity, can be helpful to mitigate the risks of jamming attacks, as discussed in [52].

The challenges of confidentiality and data integrity can be addressed through lightweight encryption technologies that do not complicate the process with the distribution of keys. To mitigate the challenges related to key distribution, a solution can be asymmetric keys and identity-based cryptography [53] that uses the user's identity as a public key. Such systems do not require public key certificates and, thus, simplify key management, and increase the overall performance [54]. Furthermore, Quantum Key Distribution (QKD) [55] has proved to be an efficient method for securely sharing keys. However, it has the challenges of fiber-attenuation and limits of longer distances [56], as discussed in earlier sections. Therefore, new techniques that use satellite relays to securely share keys over a long distance have been evaluated in several works, such as [57]. Moreover, physical layer techniques such as Direct Sequence Spread Spectrum [58] techniques can also improve security, as evaluated in [59] if the deployment of encryption technologies is not possible.

Edge computing for satellite networks to extend the capabilities (processing and storage) of satellite nodes has been proposed in [60]. Edge in the satellite can provide the necessary computing capability to perform and maintain some security procedures, such as encryption techniques. In particular, such enhancement will provide a remedy regarding the challenges associated with maintaining and managing keys required for cryptographic algorithms. Furthermore, local processing of information will also help to avoid error-prone and vulnerable long distance communication channels for processing of sensitive data. However, existing edge platforms and solutions are suited for ground stations. Very limited research is conducted on real-time evaluations of edge in satellite-to-satellite communications.

B. SATELLITE-TO-GROUND STATIONS COMMUNICATIONS

One of the most pertinent uses of satellite-to-ground stations is the use of satellite-based backhaul, which increases the use of this segment of the network. Therefore, its security is extremely important. Fortunately, the ground stations can be equipped with enough resources to perform security procedures, such as strong access control, authentication and authorization techniques. The security of the satellite-to-ground station communications can be broadly divided into i) security of the segment from ground-based attacks and vulnerabilities, and ii) improving the security of communication procedures and protocols used within the segment.

For securing satellite communications from the threats originating from ground segments, through connectivity with 5G, strong authentication and access control procedures must be in place. The vulnerabilities in 5G networks must be addressed before its integration into satellite networks. For example, solutions for the security challenges in SDN are discussed in [29], including access control, least privilege-based application access, and setting hierarchy of control platforms, etc., to mitigate the security vulnerabilities associated with SDNs. Similarly, for virtual networks and NFV, the security controls are discussed in [61]. There are many survey articles on the security of 5G, which discuss various security solutions to different challenges, from the physical to

TABLE 2. Different security attacks on various points of the eco-system from none ( ) to low (–), medium (+), and high (✓).

Security Threat	Description	Network/communication segments and links										
		Sat-Sat			Sat-Ground			Sat-UE			10	11
		7	8	9	1	3	5	2	4	6		
DoS attack	Network control/decision points and elements							✓	+	+	✓	✓
Routing attacks	Disrupt route discovery & maintenance, data delivery	✓	+	✓				+	+	+	-	
Hijacking attacks	Hijacking session or other resources							+	-	-	✓	-
Jamming attacks	Blocking legitimate access, mainly through interference	-	-	-	+	+	+	✓	✓	✓	✓	+
Signaling storms	Very frequent requests, e.g., for access, registration, etc.							✓	✓	✓	✓	✓
Resource theft	Spectrum, shared cloud resources							✓	✓	✓	✓	+
Configuration attacks	Attacks to access/change configurations, e.g., routing	✓		✓				✓	✓		-	
Eavesdropping attacks	Targeting communication channels	+	+	+	✓	✓	✓	✓	✓	✓	-	
Penetration attacks	Injecting software, code, misguiding information							✓	✓	✓		
Insider attacks	Untrustworthy employee, partner, or solution provider	-	-	-	✓	✓	✓	+	+	+	+	+
User identity theft	User information databases				-	-	-	✓	✓	✓	+	
TCP level attacks	Utilizing long delays, congestion window weaknesses	-	-	-	+	+	+	✓	✓	✓	-	-
Man-in-the-middle attack	Non-encrypted links and channels	+	+	+	✓	✓	✓	✓	✓	✓	-	
Scanning attacks	Open-air interfaces, lack of physical layer security				+	+	+	✓	✓	✓	-	
Security keys exposure	Un-encrypted channels	✓	✓	✓	-	-	-	✓	✓	✓	+	
Privacy challenges	Leak of personal or sensitive information				-	-	-	✓	✓	✓	✓	

the application layer [27], [62]. The main lesson is that strong security procedures and controls must be in place before the network is connected to satellite networks. Furthermore, the services and third party applications, which may require access to satellite networks, must also be given -the least privileges [63] when using satellite networks. For example, programmable function deployment for improving QoS must not be allowed and only specific authorized entities should be allowed to deploy programmable functions.

The security of the satellite segment can be based on the discussion in the previous sub-section, i.e., satellite-to-satellite communications. However, several additional procedures can be followed to secure the connectivity between the satellite and the ground station. For example, physical layer techniques such as beam-forming can be used to provide security against coordinated and uncoordinated eavesdropping, as evaluated in [64]. Furthermore, physical layer security has been adopted in different ways to provide security for satellite communications [65]. In addition, anti-jamming strategies, such as jamming signal filtering [66] and antenna array design [67], [68] for wireless networks discussed in [69] can be adopted for satellite communications, mainly to protect the ground stations or user terminals against jamming attacks.

To meet the challenges arising due to lack of resources in satellites, secure computation offloading, as proposed and evaluated in [70], presents an interesting solution. The authors demonstrate the use of reinforcement learning [71], [72] techniques to dynamically alter the computation offloading policies for different scenarios based on changing security threats. The main lesson is that the security techniques should be adopted according to the levels of threats. For example, techniques that require higher processing and more battery capacity should only be used when the threat mitigation requires it. Otherwise, lightweight security procedures should be used. Moreover, secure computation offloading should be used in cases of heavy computation. Blockchain-based techniques have also been evaluated [73] to improve security through distributed computing using ground-based cellular networks. Hence, blockchain technologies can also be used to further improve communication security between satellites and ground stations.

Processes and tools have been defined to collect and analyze indicators of potential security threats, and to mitigate these threats with appropriate actions. Cybersecurity Operations Centers (CSOC) [74] combine monitoring and decision-making technologies, human administrators, and processes to achieve an accurate cyber situational awareness and to actively respond to detected threats. CSOC functions identified essential for space domain include [75] proactive detection to identify threats, space threat intelligence, collaborative information sharing between organizations within space and terrestrial domains, forensic analysis, and training. The challenges for applying CSOC solutions in the space include lack of tools that are tailored and capable to analyze space and satellite specific protocols and equipment as well as attacks.

Ground stations connected to satellites but exposed to DoS attacks due to the nature of the network are studied in [76]. The authors propose a deep learning-based scheme, i.e., Long-Short Term Memory (LSTM) [77], to detect DoS attacks on the network control points in the ground segments. The results yield high accuracy in DoS attack detection. A spatial anti-jamming scheme for the internet of satellites based on the deep reinforcement learning and Stackelberg game is discussed in [78]. However, there are limitations when machine learning approaches are applied for security in satellite-ground stations. These include the higher costs associated with data acquisition from satellites, and data freshness due to higher delays. Higher altitudes and speed of satellites exacerbate such challenges.

C. SATELLITE-USER EQUIPMENT COMMUNICATIONS

The satellite to user equipment communication security is highly crucial, mainly due to the chances of most security threats and exposure of the communication links and user equipment, specifically IoT, to security attacks. The challenge of vulnerable IoT systems that are globally distributed and connected through satellite systems can be addressed through global solutions such as strengthening security standardization, and strict legislation on following the standards. Similarly, collaborative forensic knowledge and multi-jurisdictional cyber-security policies coupled with international (or multi-national) law enforcement collaboration efforts will be necessary [79].

Authentication security for roaming users has been proposed in [35], where a group signature technique has been used. The proposed mechanism, the Anonymous and Fast Roaming Authentication (AnFRA) protocol, provides sufficient anonymity to roaming users and avoids the real time involvement of a home network control center during the authentication process. Avoiding the home network control center in real-time helps minimize the utilization of satellite resources, which are usually very limited and dedicated for specific functions. Furthermore, the proposed technique supports user revocation, has fewer communication overheads, and provides sufficient privacy to users.

To cope with uncertainty, higher link latency and frequent failures, the authors in [43] propose and evaluate a group key management scheme, which uses a multi-decryption keys protocol, designed as a container, to involve shared decryption keys. The technique tolerates failure in keying or re-keying with lower costs and is suitable for higher delays. There are also other techniques such as hierarchical key management [22], and lightweight key agreement and authentication schemes [80], and the research is gaining further momentum. There has also been a great leap in using novel key distribution techniques such as quantum key distribution [81] for satellite to ground communications, as discussed in [82]. Double layer, i.e., MEO- and GEO-based quantum key distribution, has been proposed in [83] to overcome the limitations in each (MEO and GEO) and combine the strengths of both for efficient key distribution. The proposed technique takes benefit of the large coverage area of GEO satellites in situations where latency is not critical and takes benefit of MEO in latency critical-situations.

Solution to Aviation challenges: Potential solutions for securing CPDLC include Elliptic Curve Cryptography (ECC) [84], [85] to protect aircraft communications addressing and reporting systems. Similarly, the Host Identity Protocol (HIP) [86], [87] can improve the security of user-plane communications, helping improve confidentiality and integrity. Furthermore, Identity-Defined Networking (IDN) [88] provides interesting solutions for the entirety of air-traffic communication systems. Where encryption is challenging, for instance due to lack of resources such computing or key management systems, other techniques such as radio frequency fingerprinting should be used, as discussed in [89], to provide some level of defense against intrusion. Furthermore, hardware and software fingerprinting can further improve the security levels.

Physical layer security techniques that exploit the physical characteristics of communication signals have been emerging as promising solutions [17]. In the case of jamming attacks, the uncoordinated frequency hopping-based spread spectrum technique proposed in [90] provide an interesting opportunity to counter jamming attacks. The proposed technique enables two nodes to execute a protocol for key establishment in the presence of an active jammer, and thus securely transmits messages of varying lengths without relying on a shared secret key.

The use of TCP/IP in its original form for satellite communications does not seem suitable due to its apparent limitations in error and latency prone networks. However, various solutions have been proposed to integrate IPsec and PEPs to enable secure TCP/IP-based end-to-end satellite communications, as discussed in [24]. The authors enable cooperative procedure at the network level between IPsec and PEPs devices through premature acknowledgements with end users to avoid the slow start problem of the congestion control algorithm of the TCP/IP. Adaptive key distribution has been proposed [91] as a means of addressing re-keying failures, which are caused by bad signal conditions, e.g., due to bad weather. The timing and frequency of IPsec re-keying messages can be adjusted proactively based, e.g., on weather forecasts.

To ensure availability of capacity-limited satellite channels, it is essential that the network is able to control access over satellite resources as well as quality of service that is given for different users and applications. 3GPP has specified various mechanisms for ensuring quality as well as for controlling user priorities within network congestion situations. The 5G specifications introduced network slicing as a management concept to customize service levels for different types of users. In the context of integrated networks [92], [93], [94], network slicing provides a concept that can be used to control which users are given access to satellite-network specific resources, i.e., to slice networks to users with and without connectivity through space. Furthermore, network slicing can also be used to separate services of critical infrastructures, such as modern autonomous ships, from non-critical services in order to ensure security of critical infrastructures. However, network slicing requires effective authentication and authorization approaches. Moreover, further work is required for customization of security services and resources for integrated network slices. User data in the case of weak or lost links can also be secured using the latest developments in blockchain technologies. For example, authors in [95] evaluated that blockchain in a multi-hierarchy of satellite nodes can provide enough security to user data.

Privacy of user data also needs to be ensured, even if the end-user nodes lack resources for end-to-end security. In the current state-of-the-art satellite-terrestrial networks, privacy-related solutions are not widely discussed. Some works are proposed to address privacy issues that may arise with satellite-terrestrial crowdsensing. In [51], the authors introduce a satellite-terrestrial architecture with differential privacy for protecting user privacy in real-time data aggregation. The information related to user locations is quantified with differential privacy and the data aggregation is processed with satellite-terrestrial networks for data aggregation with

TABLE 3. Summary of security solutions for attacks on various points of the eco-system.

Security Threat	Solution Description	References
DoS attack	Deep learning, distribution and devolving control functions across the network	[76], [96]
Hijacking attacks	Resource control and security through control flow integrity verification and secure processing	[97], [98]
Jamming attacks	Energy harvesting, PLS, spectrum spreading and mobility, ML techniques	[99], [100], [101]
Signaling storms	Signal filtering, distributing control functions, decentralization, hierarchical authentication	[60], [66]
Resource theft	Efficient resource monitoring/auditing, slicing	[92], [94]
Configuration attacks	Least privilege-based access, strong AAA.	[63]
Eavesdropping attacks	PLS, beam-forming-based secrecy, e-to-end encryption	[64]
Penetration attacks	Service-based traffic isolation and zoning	[62], [102]
Insider attacks	End-point security for gateways and satellites; satellite-specific security monitoring and CSOCs	[75]
Identity blocking	Avoid multi-round authentication	[103]
TCP level attacks	Communication security through traffic anomaly detection techniques	[104]
Man-in-the-middle attack	Identity-based cryptography, QKD, and PLS techniques	[53], [55], [59]
Scanning attacks	PLS approaches	[65], [105]
Security keys exposure	Light-weight security protocols and encryption techniques, group key management	[27], [106], [107], [43]

auction-based incentive mechanisms. This is further used to process the communication between the buyers and sellers of data with preserved privacy. In [108], a blockchain-based distributed privacy preserving mechanism is proposed to handle incentives for the Internet-of-Vehicles (IoVs) in the satellite-terrestrial crowdsensing. The work in [109] proposes an efficient and secure handover authentication protocol for satellite-terrestrial network access which includes the satellite-UE communication. Their combined use of elliptic curve cryptographic primitives and blind factors will ensure the user traceability and anonymity in a privacy-preserved and trusted manner.

In summary, groundbreaking work is happening to secure satellite-based communications. Albeit all the efforts, there are several limitations. Except for a few use cases in the aviation and military industries, the approach of security-by-design has not been adopted. However, due to the increasing criticality of the ecosystem, novel security approaches have been investigated, with some devised and being deployed. Since most security challenges are traditional ones that exist in terrestrial networks, the solutions have also been borrowed from terrestrial networks or have been adapted to satellite networks. The solutions for challenges mentioned in Table 2 are also presented with a brief description and relevant references in Table 3. Since solutions still require more research, important research directions are discussed in Section V.

V. FUTURE RESEARCH DIRECTIONS

Interesting research activities are taking place in securing the satellite-terrestrial communications landscape. New technologies and technological concepts that are researched for wireless communications are also finding space and importance in satellite-terrestrial communications. For example, Artificial Intelligence (AI) and Machine Learning (ML) have gained a lot of research momentum in communications networks with its benefits from the physical to the application layer [110], and have recently gained attention in satellite communications [111]. Machine learning techniques can help satellite communications in many aspects, such as interference mitigation, optimization of radio resources, SatCom operations, management of large constellations, and enabling the co-existence of TN and NTNs. Dynamic spectrum management mechanisms can help the network to cope with jamming and enable interference-free coexistence, even in very dynamic environments [112]. However, AI and specifically ML have recently drawn research attention in terms of its security [113] and complexity in diverse systems and platforms [114]. Therefore, more research is needed in investigating the use of the concepts, tools, and technologies of machine learning in satellite-terrestrial communications.

Wireless networks are also benefiting from programmable network architectures and infrastructures. Hence, the concepts can also be put forward to the programmable control of space stations as well as their ground-based counterparts. However, programmability comes with its own costs of security and interoperability. Remote attestation could be one approach to verify the integrity of reprogrammed software-defined payloads. Attestation of IoT devices has been proposed through satellite networks [115] and recent standardization efforts for device attestation [116], [117] are also enabling attestation for resource-restricted devices, such as satellites. However, research on security of software-defined payloads, software-defined satellites, and software-defined security for such systems must be researched further to avoid costly mishaps and damages to extremely critical infrastructures.

Key distribution is an important research challenge in satellite and terrestrial networks. For example, asymmetric cryptography requires a universally trusted third party to issue certificates. The distribution of keys over large geographical areas creates distinct challenges. In the case of quantum key distribution, a signal transmitted over long distance (over 1000 km) optical fiber suffers high losses and depolarization, making it ineffective [118]. Satellite-based quantum key distribution, as discussed in [83], presents an interesting solution not only for satellite networks but also terrestrial networks. However, more research is needed in this direction since the current schemes have several limitations, such as the need for a comparatively higher number of optical links even in satellite communications.

Satellites contain more and more third-party software and hardware components. As computational capabilities of satellites have increased, open operating systems, particularly Linux [119], are being adopted. Further, Field Programmable

TABLE 4. Existing security challenges summarized according the ITU-T security dimensions.

Security Domain	Description	Network/communication segments and links										
		Sat-Sat			Sat-Ground			Sat-UE			10	11
		7	8	9	1	3	5	2	4	6		
Access control	Protects against unauthorized use of resources	L	L	L	M	M	M	H	H	L	M	L
Authentication	Confirms identities of communicating entities, ensures its validity.	L	L	L	M	M	M	H	H	H	L	L
Non-Repudiation	Provides means for associating actions with entities	L	L	L	M	M	M	H	H	H	M	L
Data Confidentiality	Protects data from unauthorized disclosures	M	L	M	M	M	M	H	H	H	M	L
Communication security	Ensures that information flows only between authorized end points	L	L	L	M	M	M	H	H	H	M	L
Data integrity	Ensures correctness of data, protects from unauthorized changes	L	L	L	M	M	M	H	H	H	M	L
Availability	Ensures authorized access to resources, information, and services	L	L	L	L	L	L	H	H	H	L	L
Privacy	Protects information to be derived from observations of comm. links	L	L	L	L	L	L	H	H	H	M	L

Numbers (1-11) represent communication links, described in Table 1, and Figure 1.

Gate Array (FPGA) approaches [120] make also hardware updatable in the orbit. Consequently, vulnerabilities originating from Linux, third-party components, or on orbit updates must be addressed. One challenge is that software updates to very critical satellite platforms take time as unverified software cannot be uploaded as they may make satellite completely unusable [121]. Consequently, adversaries are given additional time between the publication of security vulnerability and patching of it. The principle of least privilege [122] for third party applications, and role and attribute-based access control [123] must be researched for programmable satellites.

The existing security landscape pointing to security dimensions that require more research work is also presented in a visual form in Table 4. Security dimensions are represented according to the security recommendations provided by the International Telecommunication Union-Telecommunications (ITU-T) [124]. Notations such as H, M, and L are used to signify dimension where the existing security challenges are High (H), Medium (M), and Low (L), respectively, for different communication channels, links, or interfaces in the ecosystem. The main purpose is to attract more research to points where more security challenges still exist.

VI. CONCLUSION

The integration of satellite-based communications to terrestrial networks is constantly growing with new opportunities for both space-based systems, their terrestrial counterparts, and users. Critical infrastructures ranging from sea, air, and ground are benefiting from increased coverage offered by the converged communications infrastructures. However, the security concerns are also growing alongside increasing benefits. This article provides insights into the security concerns and possible mitigation techniques. The security challenges and solutions are broadly categorized into i) satellite-to-satellite communications, ii) satellite-to-ground station communications, and iii) satellite-to-UE communications to facilitate understanding of the complex security landscape. The main challenges pertaining to all types of communications that need further research are caused by the mobility of satellites that makes it difficult to deploy encryption technologies, higher latency due to comparatively higher distances, and lack of higher computing resources required by efficient and up-to-date security technologies. In 6G, satellite-based communications will be inevitable. Therefore, this article also provides interesting research directions to instigate further research in this direction.

REFERENCES

[1] O. Kodheli, "Satellite communications in the new space era: A survey and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 70–109, 4th Quart., 2021.

[2] A. Guidotti, A. Vanelli-Coralli, M. Conti, S. Andrenacci, S. Chatzinotas, N. Maturo, B. Evans, A. Awoseyila, A. Ugolini, T. Foggi, L. Gaudio, N. Alagha, and S. Cioni, "Architectures and key technical challenges for 5G systems incorporating satellites," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2624–2639, Mar. 2019.

[3] M. Höyhtyä, S. Boumard, A. Yastrebova, P. Järvensivu, M. Kiviranta, and A. Anttonen, "Sustainable satellite communications in the 6G era: A European view for multi-layer systems and space safety," 2022, *arXiv:2201.02408*.

[4] *Technical Specification Group Radio Access Network; Study on New Radio (NR) to Support Non-Terrestrial Networks (Release 15)*, Standard 3GPP TR 38.811, Tech. Rep., 2020.

[5] (2022). *Ka-Sat Network Cyber Attack Overview*. [Online]. Available: https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[6] P.-D. Arapoglou, A. Ginesi, S. Cioni, S. Erl, F. Clazzer, S. Andrenacci, and A. Vanelli-Coralli, "DVB-S2X-enabled precoding for high throughput satellite systems," *Int. J. Satell. Commun. Netw.*, vol. 34, no. 3, pp. 439–455, May 2016.

[7] *Technical Specification Group Services and System Aspects; Study on Architecture Aspects for Using Satellite Access in 5G (Release 17)*, Standard 3GPP TR 23.737, Tech. Rep., 2021.

[8] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE Access*, vol. 8, pp. 165178–165200, 2020.

[9] C. Jiang, X. Wang, J. Wang, H.-H. Chen, and Y. Ren, "Security in space information networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 82–88, Aug. 2015.

[10] X. Yan and H. Teng, "Study on security of 5G and satellite converged communication network," *ZTE Commun.*, vol. 19, no. 4, pp. 79–89, 2021.

[11] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space," *Int. J. Inf. Secur.*, vol. 20, no. 3, pp. 287–311, 2021.

[12] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 53–87, 1st Quart., 2022.

[13] *Security Architecture and Procedures for 5G System*, Standard 3GPP, TS 33.501. Release 15, 2018.

[14] I. A. Sanchez, G. Moury, and H. Weiss, "The CCSDS space data link security protocol," in *Proc. MILCOM Mil. Commun. Conf.*, Oct. 2010, pp. 219–224.

[15] *Security Architecture for Space Data Systems; Magenta Book*, document CCSDS 351.0-M-1, CCSDS, 2012.

[16] *Network Layer Security Adaptation Profile; Blue Book*, Standard CCSDS 356.0-B-1, CCSDS, 2016.

[17] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, 4th Quart., 2018.

[18] X. Lin, S. Cioni, G. Charbit, N. Chuberre, S. Hellsten, and J.-F. Boutillon, "On the path to 6G: Embracing the next wave of low Earth orbit satellite access," *IEEE Commun. Mag.*, vol. 59, no. 12, pp. 36–42, Dec. 2021.

[19] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[20] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities," *IEEE Netw.*, vol. 35, no. 2, pp. 244–251, Mar./Apr. 2021.

[21] S. Zhang, D. Zhu, and Y. Wang, "A survey on space-aerial-terrestrial integrated 5G networks," *Comput. Netw.*, vol. 174, Jun. 2020, Art. no. 107212. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128619314045

[22] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Commun.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.

[23] N. Doraswamy and D. Harkins, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[24] L. Djeddai and R. K. Liu, "IPSecOPEP: IPSec over PEPs architecture, for secure and optimized communications over satellite links," in *Proc. 7th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Aug. 2016, pp. 264–268.

[25] L. Jianwei, L. Weiran, W. Qianhong, L. Dawei, and C. Shigang, "Survey on key security technologies for space information networks," *J. Commun. Inf. Netw.*, vol. 1, no. 1, pp. 72–85, Jun. 2016.

[26] Y. Yan, G. Han, and H. Xu, "A survey on secure routing protocols for satellite network," *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, Art. no. 102415. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519302498

[27] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[28] L. Bertaux, S. Medjiah, P. Berthou, S. Abdellatif, A. Hakiri, P. Gelard, F. Planchou, and M. Bruyere, "Software defined networking and virtualization for broadband satellite networks," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 54–60, Mar. 2015.

[29] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, 4th Quart., 2015.

[30] (2022). *The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on all O-RAN Interfaces and Components*. [Online]. Available: https://www.o-ran.org/blog/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components

[31] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *Int. J. Prod. Econ.*, vol. 172, pp. 76–94, Feb. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S092552731500451X

[32] C. Caini, R. Firrincieli, and D. Lacamera, "PEPsal: A performance enhancing proxy designed for TCP satellite connections," in *Proc. IEEE 63rd Veh. Technol. Conf.*, May 2006, pp. 2607–2611.

[33] J. Deutschmann, K.-S. Hielscher, and R. German, "Satellite internet performance measurements," in *Proc. Int. Conf. Networked Syst. (NetSys)*, Mar. 2019, pp. 1–4.

[34] K. Eduard. (2018). *Hackers Can Hijack, Sink Ships: Researchers*. [Online]. Available: https://www.securityweek.com/hackers-can-hijack-sink-ships-researchers

[35] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li, and N. Yu, "AnFRA: Anonymous and fast roaming authentication for space information network," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 486–497, Jul. 2018.

[36] M. Strohmeier, "Security in next generation air traffic communication networks," Ph.D. dissertation, Dept. Comput. Sci., Univ. Oxford, Oxford, U.K.:, 2016.

[37] R. Santamarta, *Last Call for SATCOM Security*. Seattle, WA, USA: IOActive, 2018.

[38] S. Khan, J. Thorn, A. Wahlgren, and A. Gurtov, "Intrusion detection in automatic dependent surveillance-broadcast (ADS-B) with machine learning," in *Proc. IEEE/AIAA 40th Digit. Avionics Syst. Conf. (DASC)*, Oct. 2021, pp. 1–10.

[39] A. Gurtov, T. Polishchuk, and M. Wernberg, "Controller—Pilot data link communication security," *Sensors*, vol. 18, no. 5, p. 1636, May 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/5/1636

[40] S. Kent, "IP encapsulating security payload (ESP)," IETF, USA, Tech. Rep. 4303, 2005.

[41] C. Kaufman, *Internet Key Exchange (IKEv2) Protocol*, document RFC 4306, Tech. Rep., 2005.

[42] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, document RFC 8446, Tech. Rep., 2018.

[43] Z. Jian, S. Liyan, D. Kaiyu, and W. Yue, "Research on self-adaptive group key management in deep space networks," *Wireless Pers. Commun.*, vol. 114, no. 4, pp. 3435–3456, Oct. 2020.

[44] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[45] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, "A survey on technologies, standards and open challenges in satellite IoT," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1693–1720, 3rd Quart., 2021.

[46] G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, and G. Spezzano, "IoT platforms and security: An analysis of the leading industrial/commercial solutions," *Sensors*, vol. 22, no. 6, p. 2196, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/6/2196

[47] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[48] M. Höyhtyä and J. Martio, "Integrated satellite—Terrestrial connectivity for autonomous ships: Survey and future research directions," *Remote Sens.*, vol. 12, no. 15, p. 2507, 2020. [Online]. Available: https://www.mdpi.com/2072-4292/12/15/2507

[49] *Autonomous Shipping Initiative for European Waters*, Autoship, Salt Lake City, UT, USA, 2019.

[50] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Saf. Sci.*, vol. 131, Nov. 2020, Art. no. 104908. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753520303052

[51] B. Zhu, J. Li, Z. Liu, and Y. Liu, "A privacy-preserving incentive mechanism for data offloading in satellite-terrestrial crowdsensing," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–14, Dec. 2021.

[52] V. Weerackody, "Satellite diversity to mitigate jamming in LEO satellite mega-constellations," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[53] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. Austral. Unix Users Group Annu. Conf.*, 2004, pp. 95–102.

[54] F. Guo, Y. Mu, and Z. Chen, "Identity-based online/offline encryption," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Cham, Switzerland: Springer, 2008, pp. 247–261.

[55] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lükenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, p. 1301, Sep. 2009.

[56] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *NPJ Quantum Inf.*, vol. 3, no. 1, pp. 1–13, Dec. 2017.

[57] X. He, L. Li, D. Han, Y. Zhao, A. Nag, W. Wang, H. Wang, Y. Cao, and J. Zhang, "Routing and secret key assignment for secure multicast services in quantum satellite networks," *J. Opt. Commun. Netw.*, vol. 14, no. 4, pp. 190–203, 2022.

[58] C. Pöpper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 703–715, Jun. 2010.

[59] S. Spinsante, C. Warty, and E. Gambi, "DS-SS with de Bruijn sequences for secure inter satellite links," in *Proc. IEEE Aerosp. Conf.*, Mar. 2013, pp. 1–8.

[60] R. Xie, Q. Tang, Q. Wang, X. Liu, F. R. Yu, and T. Huang, "Satellite-terrestrial integrated edge computing networks: Architecture, challenges, and open issues," *IEEE Netw.*, vol. 34, no. 3, pp. 224–231, May 2020.

[61] I. Ahmad, J. Pinola, I. Harjula, J. Suomalainen, E. Harjula, J. Huusko, and T. Kumar, "An overview of the security landscape of virtual mobile networks," *IEEE Access*, vol. 9, pp. 169014–169030, 2021.

[62] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[63] J. Hertz, "Abusing privileged and unprivileged Linux containers," NCC Group, London, U.K., White Paper, 2016, vol. 48.

[64] Z. Lin, M. Lin, J.-B. Wang, Y. Huang, and W.-P. Zhu, "Robust secure beamforming for 5G cellular networks coexisting with satellite networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 932–945, Apr. 2018.

[65] M. Lin, Q. Huang, T. de Cola, J.-B. Wang, J. Wang, M. Guizani, and J.-Y. Wang, "Integrated 5G-satellite networks: A perspective on physical layer reliability and security," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 152–159, Dec. 2020.

[66] Y.-R. Chien, "Design of GPS anti-jamming systems using adaptive notch filters," *IEEE Syst. J.*, vol. 9, no. 2, pp. 451–460, Jun. 2015.

[67] Q. Li, W. Wang, D. Xu, and X. Wang, "A robust anti-jamming navigation receiver with antenna array and GPS/SINS," *IEEE Commun. Lett.*, vol. 18, no. 3, pp. 467–470, Mar. 2014.

[68] N. Rezazadeh and L. Shafai, ''A compact antenna for GPS anti-jamming in airborne applications,'' *IEEE Access*, vol. 7, pp. 154253–154259, 2019.

[69] H. Pirayesh and H. Zeng, ''Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,'' *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.

[70] S. Sthapit, S. Lakshminarayana, L. He, G. Epiphaniou, and C. Maple, ''Reinforcement learning for security-aware computation offloading in satellite networks,'' *IEEE Internet Things J.*, vol. 9, no. 14, pp. 12351–12363, Jul. 2022.

[71] M. A. Wiering and M. Van Otterlo, ''Reinforcement learning,'' *Adaptation, Learn., Optim.*, vol. 12, no. 3, p. 729, 2012.

[72] L. P. Kaelbling, M. L. Littman, and A. W. Moore, ''Reinforcement learning: A survey,'' *J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 237–285, Jan. 1996.

[73] C. Li, X. Sun, and Z. Zhang, ''Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology,'' *IEEE Access*, vol. 9, pp. 113558–113565, 2021.

[74] C. Zimmerman, *Cybersecurity Operations Center*. McLean, VA, USA: MITRE Corporation, 2014.

[75] S. Sanchez, R. Mazzolin, I. Kechaoglou, D. Wiemer, W. Mees, and J. Muylaert, '''Cybersecurity space operation center: Countering cyber threats in the space domain,'' in *Handbook of Space Security*. Cham, Switzerland: Springer, 2020, pp. 921–939.

[76] S. Khan, P. Kumar, A. Braeken, and A. Gurtov, ''Detection of evil flies: Securing air-ground aviation communication,'' in *Proc. 27th Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2021, pp. 852–854, doi: 10.1145/3447993.3482869.

[77] S. Hochreiter and J. Schmidhuber, ''Long short-term memory,'' *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.

[78] C. Han, L. Huo, X. Tong, H. Wang, and X. Liu, ''Spatial anti-jamming scheme for internet of satellites based on the deep reinforcement learning and Stackelberg game,'' *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5331–5342, May 2020.

[79] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, ''A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[80] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C.-M. Chen, ''A lightweight key agreement and authentication scheme for satellite-communication systems,'' *IEEE Access*, vol. 8, pp. 46278–46287, 2020.

[81] R. Renner, ''Security of quantum key distribution,'' *Int. J. Quantum Inf.* vol. 6, no. 1, pp. 1–127, Feb. 2008.

[82] S.-K. Liao, ''Satellite-to-ground quantum key distribution,'' *Nature*, vol. 549, pp. 43–47, Sep. 2017.

[83] D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, ''Quantum key distribution over double-layer quantum satellite networks,'' *IEEE Access*, vol. 8, pp. 16087–16098, 2020.

[84] K. Lauter, ''The advantages of elliptic curve cryptography for wireless security,'' *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 62–67, Feb. 2004.

[85] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Cham, Switzerland: Springer, 2006.

[86] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, *Host Identity Protocol*, document RFC 5201, Tech. Rep., Apr. 2008.

[87] A. Gurtov, *Host Identity Protocol (HIP): Towards Secure Mobile Internet*. Hoboken, NJ, USA: Wiley, 2008.

[88] A. Gurtov, T. Polishchuk, and M. Wernberg, ''Controller—Pilot data link communication security,'' *Sensors*, vol. 18, no. 5, p. 1636, May 2018.

[89] J. Hall, M. Barbeau, and E. Kranakis, ''Enhancing intrusion detection in wireless networks using radio frequency fingerprinting,'' *Commun., Internet, Inf. Technol.*, vol. 1, pp. 1–6, Nov. 2004.

[90] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, ''Jamming-resistant key establishment using uncoordinated frequency hopping,'' in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 64–78.

[91] J. Puttonen, ''Multicast security framework for multi-spot beam satellite network,'' in *Proc. 21st Ka Broadband Commun. Conf.*, 2015, pp. 1–8.

[92] C. Suzhi, W. Junyong, H. Hao, Z. Yi, Y. Shuling, Y. Lei, W. Shaojun, and G. Yongsheng, ''Space edge cloud enabling network slicing for 5G satellite network,'' in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 787–792.

[93] M. Höyhtyä, T. Ojanperä, J. Mäkelä, S. Ruponen, and P. Järvensivu, ''Integrated 5G satellite-terrestrial systems: Use cases for road safety and autonomous ships,'' in *Proc. 23rd Ka Broadband Commun. Conf.*, 2017, pp. 16–19.

[94] Y. Drif, E. Chaput, E. Lavinal, P. Berthou, B. T. Jou, O. Grémillet, and F. Arnal, ''An extensible network slicing framework for satellite integration into 5G,'' *Int. J. Satell. Commun. Netw.*, vol. 39, no. 4, pp. 339–357, Jul. 2021.

[95] S. Fu, B. Wu, S. Wu, and F. Fang, ''Multi-resources management in 6G-oriented terrestrial-satellite network,'' *China Commun.*, vol. 18, no. 9, pp. 24–36, Sep. 2021.

[96] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, ''DevoFlow: Scaling flow management for high-performance networks,'' in *Proc. ACM SIGCOMM Conf. SIGCOMM (SIGCOMM)*, 2011, pp. 254–265.

[97] S. Das, W. Zhang, and Y. Liu, ''A fine-grained control flow integrity approach against runtime memory attacks for embedded systems,'' *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 24, no. 11, pp. 3193–3207, Nov. 2016.

[98] S. Mao and T. Wolf, ''Hardware support for secure processing in embedded systems,'' *IEEE Trans. Comput.*, vol. 59, no. 6, pp. 847–854, Jun. 2010.

[99] G. Rezgui, E. V. Belmega, and A. Chorti, ''Mitigating jamming attacks using energy harvesting,'' *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 297–300, Feb. 2019.

[100] G. Han, L. Xiao, and H. V. Poor, ''Two-dimensional anti-jamming communication based on deep reinforcement learning,'' in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2017, pp. 2087–2091.

[101] V. François-Lavet, P. Henderson, R. Islam, M. G. Bellemare, and J. Pineau, ''An introduction to deep reinforcement learning,'' *Found. Trends Mach. Learn.*, vol. 11, nos. 3–4, pp. 219–354, Dec. 2018.

[102] S. Yi, Z. Qin, and Q. Li, ''Security and privacy issues of fog computing: A survey,'' in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2015, pp. 685–695.

[103] M. H. Ibrahim, S. Kumari, A. K. Das, and V. Odelu, ''Jamming resistant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks,'' *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5563–5580, Dec. 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1717

[104] G. Kaur, V. Saxena, and J. P. Gupta, ''Detection of TCP targeted high bandwidth attacks using self-similarity,'' *J. King Saud Univ. Comput. Inf. Sci.*, vol. 32, no. 1, pp. 35–49, Jan. 2020.

[105] B. Li, Z. Fei, C. Zhou, and Y. Zhang, ''Physical-layer security in space information networks: A survey,'' *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.

[106] B. J. Mohd and T. Hayajneh, ''Lightweight block ciphers for IoT: Energy optimization and survivability techniques,'' *IEEE Access*, vol. 6, pp. 35966–35978, 2018.

[107] K. Zhang, J. Long, X. Wang, H.-N. Dai, K. Liang, and M. Imran, ''Lightweight searchable encryption protocol for industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4248–4259, Jun. 2021.

[108] Z. Ma, Y. Wang, J. Li, and Y. Liu, ''A blockchain based privacy-preserving incentive mechanism for internet of vehicles in satellite-terrestrial crowdsensing,'' in *Proc. 7th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2021, pp. 2062–2067.

[109] Y. Liu, L. Ni, and M. Peng, ''A secure and efficient authentication protocol for satellite-terrestrial networks,'' *IEEE Internet Things J.*, early access, Feb. 18, 2022, doi: 10.1109/JIOT.2022.3152900.

[110] I. Ahmad, S. Shahabuddin, H. Malik, E. Harjula, T. Leppanen, L. Loven, A. Anttonen, A. H. Sodhro, M. M. Alam, M. Juntti, A. Yla-Jaaski, T. Sauter, A. Gurtov, M. Ylianttila, and J. Riekki, ''Machine learning meets communication networks: Current trends and future challenges,'' *IEEE Access*, vol. 8, pp. 223418–223460, 2020.

[111] F. Fourati and M.-S. Alouini, ''Artificial intelligence for satellite communication: A review,'' *Intell. Converged Netw.*, vol. 2, no. 3, pp. 213–243, Sep. 2021.

[112] M. Höyhtyä, M. Majanen, M. Hoppari, P. Järvensivu, H. Kokkinen, J. Ojaniemi, A. Reis-Kivinen, O. Pellay, D. Pham-Minh, and M. Guta, ''Licensed shared access field trial and a testbed for satellite-terrestrial communication including research directions for 5G and beyond,'' *Int. J. Satell. Commun. Netw.*, vol. 39, no. 4, pp. 455–472, Jul. 2021.

[113] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mammela, and I. Ahmad, ''Machine learning threatens 5G security,'' *IEEE Access*, vol. 8, pp. 190822–190842, 2020.

[114] I. Ahmad, S. Shahabuddin, T. Sauter, E. Harjula, T. Kumar, M. Meisel, M. Juntti, and M. Ylianttila, ''The challenges of artificial intelligence in wireless networks for the Internet of Things: Exploring opportunities for growth,'' *IEEE Ind. Electron. Mag.*, vol. 15, no. 1, pp. 16–29, Mar. 2021.

[115] Q. Wang, X. Chen, X. Jin, X. Li, D. Chen, and X. Qin, ''Enhancing trustworthiness of internet of vehicles in space–air–ground-integrated networks: Attestation approach,'' *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5992–6002, Apr. 2022.

[116] *Symmetric Identity Based Device Attestation*, Trusted Computing Group, Reference Version 1.0, Revision 0.95, Trusted Computing Group, Beaverton, OR, USA, Jan. 2020.

[117] S. Hristozov, J. Heyszl, S. Wagner, and G. Sigl, "Practical runtime attestation for tiny IoT devices," in *Proc. Workshop Decentralized IoT Secur. Standards*, 2018, pp. 1–6.

[118] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nature Photon.*, vol. 7, pp. 382–386, Mar. 2013.

[119] H. Leppinen, "Current use of Linux in spacecraft flight software," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 10, pp. 4–13, Oct. 2017.

[120] M. R. Maheshwarappa, M. D. J. Bowyer, and C. P. Bridges, "Improvements in CPU & FPGA performance for small satellite SDR applications," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 1, pp. 310–322, Feb. 2017.

[121] R. Merriam. (2016). *Software Update Destroys 286$ Million Japanese Satellite*. [Online]. Available: https://hackaday.com/2016/05/02/software-update-destroys-286-million-japanese-satellite/

[122] F. B. Schneider, "Least privilege and more [computer security]," *IEEE Security Privacy*, vol. 1, no. 5, pp. 55–59, Sep. 2003.

[123] I. Ahmad, S. Lembo, F. Rodriguez, S. Mehnert, and M. Vehkapera, "Security of micro MEC in 6G: A brief overview," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2022, pp. 332–337.

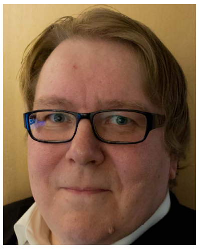
[124] *Security Architecture for Systems Providing End-to-End Communications*, document ITU-T, 2003.

IJAZ AHMAD (Member, IEEE) received the M.Sc. and Ph.D. degrees in wireless communications from the University of Oulu, Finland, in 2012 and 2018, respectively. He is currently a Senior Scientist at VTT Technical Research Centre of Finland. He is also an Adjunct Professor with the University of Oulu. He has visited several institutions as a Visiting Scientist, such as the Technical University of Vienna, Austria, in 2019, and Aalto University Finland, in 2018. He has more than 45 publications including journals, conference papers, book chapters, and patent application. He has published an edited book on the security of 5G, called *A comprehensive guide to 5G security* (Wiley Inc.). His research interests include cybersecurity, security of 5G/6G, and applications of machine learning in wireless networks. He was a recipient of several awards including the Nokia Foundation, Tauno Tönning and Jorma Ollila grant awards, and the VTT Research Excellence Award for 2020 and 2021. Furthermore, he has received two best paper awards at IEEE conferences.

JANI SUOMALAINEN received the M.Sc. (Tech.) degree from the Lappeenranta University of Technology, Finland, in 2001, and the D.Sc. (Tech.) degree from Aalto University, Finland, in 2022. Since 2000, he has been with VTT Technical Research Centre of Finland, Espoo, where he is currently a Senior Scientist. He is also specialized in cybersecurity. He has coauthored more than 40 scientific articles on network security. Recently, he has been involved in European and Finnish cooperation projects to develop, research, and trial secure next-generation technologies for mobile networks. His research interests include threat modeling, security architectures, as well as intelligent and active defenses for dynamic and heterogeneous network environments.

PAWANI PORAMBAGE (Member, IEEE) received the Ph.D. degree from the Faculty of Information Technology and Electrical Engineering (ITEE), University of Oulu, Finland. She was a Visiting Researcher at Nokia-Bell Laboratories, Finland; VUB; and the University of Zurich. She is currently a Senior Scientist at VTT Technical Research Centre of Finland. She is also an Adjunct Professor with the University of Oulu. She has over ten years of experience at the Centre for Wireless Communication, University of Oulu, Finland, in security and privacy in different networks, including wireless sensor networks, telecommunication networks, and the IoT. She is also involved in two EU projects, including INSPIRE-5Gplus and Hexa-X, and 6G Flagship supported by the Academy of Finland. She has coauthored more than 50 publications, including four book chapters. She is the Finnish National Coordinator for EU COST Action CA17124 and the Management Committee Member for IC1301 and CA16226.

ANDREI GURTOV (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from the University of Helsinki, Finland, in 2000 and 2004, respectively. He has supervised 15 Ph.D. theses. He was with the University of Oulu for three years and Aalto University for six years and visiting the International Computer Science Institute at Berkeley multiple times. He is currently a Professor of computer science with Linköping University, Sweden. He has coauthored over 200 publications, including four books, five IETF RFCs, six patents, over 60 journals, and 110 conference papers. His research interests include network protocols, security of vehicular, airborne, industrial systems, mobile, wireless and the IoT networks, and smart grids. He is an ACM Distinguished Scientist, an IEEE ComSoc Distinguished Lecturer, from 2016 to 2019, and the Chair of IEEE Sweden Section. He received best paper awards at IEEE CSCN'17 and IEEE Globecom'11. He was the Co-Adviser of the best Doctoral Thesis in CS, Finland, in 2017. He had served on numerous journal editorial boards and conference program committees, including IEEE Internet of Things Journal, *Sensors* (MDPI), IEEE ICNP, ACM MSWiM, and IFIP Networking.



JYRKI HUUSKO received the degree in theoretical physics with minor subjects in information technology and mathematics from the University of Oulu. He is currently working as a Research Team Leader with VTT Technical Research Centre of Finland. His current research interests include future autonomic networks and services, transport protocols and multimedia delivery optimization, cross-layer communication design in heterogeneous wireless and mobile networks, cross-layer communication aided network mobility, and multi-access.

MARKO HÖYHTYÄ (Senior Member, IEEE) received the D.Sc. (Tech.) degree in telecommunication engineering from the University of Oulu, where he holds an associate professor (docent) position. He was a Visiting Researcher with the Berkeley Wireless Research Center, CA, from 2007 to 2008, and a Visiting Research Fellow with the European Space Research and Technology Centre, The Netherlands, in 2019. Since 2005, he has been with VTT Technical Research Centre of Finland Ltd., in various positions as a researcher, a manager, and a team leader. He is currently working as a Research Professor, where he focusing on satellite communications and situational awareness technologies. He is also an Associate Professor with the National Defence University. His research interests include critical communications, autonomous systems, and resource management in terrestrial and satellite communication systems.