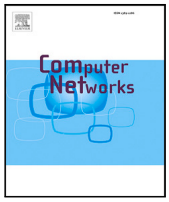
Satellite-based communications security

Computer Networks 216 (2022) 109246

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Survey paper

Satellite-based communications security: A survey of threats, solutions, and research challenges

Pietro Tedeschi [a,*], Savio Sciancalepore [b,*], Roberto Di Pietro [c]

[a] Technology Innovation Institute, Autonomous Robotics Research Center, Abu Dhabi, United Arab Emirates
[b] Eindhoven University of Technology, Eindhoven, Netherlands
[c] Division of Information and Computing Technology (ICT), College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU), Doha, Qatar

ARTICLE INFO

Keywords:
Satellites cybersecurity
Satellites jamming
GNSS spoofing
Cryptography for satellites
Quantum key distribution for satellites
3GPP
6G
Satellite-drones communications

ABSTRACT

Satellite-based Communication (SATCOM) systems are gaining renewed momentum in Industry and Academia, thanks to innovative services introduced by leading tech companies and the promising impact they can deliver towards the *global connectivity* objective tackled by early 6G initiatives. On the one hand, the emergence of new manufacturing processes and radio technologies promises to reduce service costs while guaranteeing outstanding communication latency, available bandwidth, flexibility, and coverage range. On the other hand, cybersecurity techniques and solutions applied in SATCOM links should be updated to reflect the substantial advancements in attacker capabilities characterizing the last two decades. However, business urgency and opportunities are leading operators towards challenging system trade-offs, resulting in an increased attack surface and a general relaxation of the available security services.

In this paper, we tackle the cited problems and present a comprehensive survey on the link-layer security threats, solutions, and challenges faced when deploying and operating SATCOM systems. Specifically, we classify the literature on security for SATCOM systems into two main branches, i.e., physical-layer security and cryptography schemes. Then, we further identify specific research domains for each of the identified branches, focusing on dedicated security issues, including, e.g., physical-layer confidentiality, anti-jamming schemes, anti-spoofing strategies, and quantum-based key distribution schemes. For each of the above domains, we highlight the most essential techniques, peculiarities, advantages, disadvantages, lessons learned, and future directions. Finally, we also identify emerging research topics whose additional investigation by Academia and Industry could further attract researchers and investors, ultimately unleashing the full potential behind ubiquitous satellite communications.

1. Introduction

SATCOMs play a vital role in the global telecommunication systems, having found applications in a plethora of domains throughout the last 50 years, including radio broadcasting, weather forecast, maritime communications, assisted navigation, and military operations, to name a few [1]. While the attention of Academia and Industry in the last years was mainly focused on ground communication systems, recent business initiatives launched by leading tech companies such as SpaceX, Facebook, and Amazon generated new renewed interest in satellite-based systems [2,3]. In particular, satellites are being deployed to provide services in a variety of new application domains, e.g., to reach remote locations providing unmatched connectivity (as per bandwidth and cost), or to support low-power constrained Internet of Things (IoT) devices [4]. As a result, recent commercial and standardization activities clearly indicate SATCOMs as one of the most important enabling technologies for supporting the development of the upcoming sixth-generation (6G) networks [5]. In addition, the business driving factors also seem to indicate a bright future for SATCOMs. Indeed, according to a dedicated research report by Market Research Future (MRFR), "Satellite Communication Market Information by Product, Technology, End-Use, and Region-Forecast till 2025", the SATCOM market is anticipated to reach USD 41,860 Million by 2025, sporting a 8.40% Compound Annual Growth Rate (CAGR).

Despite the promising applications and forecasting, the adoption of satellite links generally widens the threat surface of a system, introducing new vulnerabilities. Indeed, the ease to eavesdrop, tamper, disrupt, and reroute the satellite traffic provides the attacker with an extensive portfolio of opportunities to launch cyber-attacks at scale and affect the operations of such systems in different ways [6]. To complete the

* Corresponding authors.
E-mail addresses: pietro.tedeschi@tii.ae (P. Tedeschi), s.sciancalepore@tue.nl (S. Sciancalepore), rdipietro@hbku.edu.qa (R. Di Pietro).

https://doi.org/10.1016/j.comnet.2022.109246
Received 27 April 2022; Received in revised form 19 July 2022; Accepted 29 July 2022
Available online 3 August 2022

Table 1
Main addressed topics and differences between surveys touching SATCOM systems.

Ref.	Information-theoretic security	Anti-jamming	Anti-spoofing	Security research challenges	Machine learning	Cryptography
[8]	✗	✗	✗	✓	✗	✓
[9]	✗	✗	✗	✗	✓	✗
[10]	✓	✗	✗	✓	✗	✗
[11]	✗	✓	✓	✓	✗	✗
[12]	✗	✓	✓	✓	✗	✗
[13]	✗	✗	✗	✓	✓	✗
[14]	✗	✗	✓	✓	✗	✓
[15]	✗	✗	✓	✗	✗	✓
[16]	✗	✗	✓	✓	✗	✓
[17]	✗	✗	✗	✗	✗	✗
[18]	✓	✗	✓	✓	✗	✓
[19]	✓	✗	✗	✓	✗	✗
This survey	✓	✓	✓	✓	✓	✓

scenario, there is also the fact that the military satellite backbone is subject to the same (if not bigger) issues [7].

The severity of the cited threats could be even higher when considering that most of the current satellite systems either do not integrate security at all or run outdated security techniques, unable to face the complex attacks launched today [8]. As a result, security solutions for SATCOM should be revisited and coupled with the unique features of satellite-based systems.

Several contributions in the last decade already investigated security issues in the context of SATCOM (refer to Table 1 for an overview). Looking at the main contributions on SATCOM security, valuable insights are provided by, e.g. [11,12,14,15,18], and [16]. However, they only preliminarily identified the GNSS spoofing and GNSS jamming attacks and presented the adopted solutions and mitigation techniques available from the literature. Moreover, the study by the authors in [10] only summarize the schemes targeting data secrecy at the physical layer, with a focus on information-theoretic schemes only. Other surveys, such as the one in [19], focused specifically on some research areas, such as quantum computing, missing the contextualization of such areas to other research in the SATCOM domain. It is also worth mentioning the recent contribution by [20], highlighting the threats affecting specific application areas where SATCOM links play a role. However, such a survey focuses on the review of the literature, rather than on the identification of the research areas where such contributions are provided. Moreover, although many contributions are available on secure routing, e.g. [21,22], the focus of our investigation is link-layer security in satellite communications, and secure routing is therefore out of scope. As a result, we notice that the current literature is still missing a comprehensive survey, presenting and exploring all the facets of the threat surface to be considered when deploying SATCOM systems at the link-layer, as well as related countermeasures.

Contribution. In this paper, we fill the afore-described gaps by providing a comprehensive survey on security threats, solutions, mitigation strategies, and research challenges faced when designing and deploying secure SATCOM systems. In detail, we classify the security solutions related to the link-layer of SATCOM systems available in the literature into two main research domains, i.e., physical-layer approaches and cryptography techniques. Next, we delve into each area, looking at the offered security services and how such schemes guarantee the desired security objectives. For each area, as a novel contribution, we describe the threat models, assumptions, system requirements, and operational strategy, and we cross-compare the most important proposals along their characterizing features (see Fig. 1 for a graphical overview). Finally, within each research domain, we also identify novel future research directions and additional research challenges.

Roadmap. The rest of this paper is organized as follows. Section 2 introduces the basics of SATCOMs; Section 3 introduces information-theoretic security strategies and solutions to enhance data secrecy; Section 4 analyzes the applications of cryptography schemes in SATCOMs; Section 5 outlines emerging research domains; and, finally, in Section 6 we tighten some conclusions. Refer to Table 2 for the acronyms list.

2. Background

This section introduces the main notions related to SATCOM systems used within our manuscript, including the satellites constellations, architectures, and the involved protocols. Overall, this section aims to provide the reader with the needed background on SATCOM technologies and their main features, that will be used in the sequel of the paper.

2.1. Satellite constellations

The main features that distinguish satellites orbits are the shape (circular or elliptical), the altitude (Low-Earth, Medium-Earth, or Geostationary), the travel direction (clockwise or counterclockwise), and the inclination to the plane of the Earth's equator [23]. The most popular of the previously cited features is the altitude: we distinguish Low Earth Orbit (LEO), Medium Earth Orbit (MEO) and Geostationary Equatorial Orbit (GEO). The respective altitude ranges from the Earth surface are 500 to 900 km for LEO, 5000 to 25,000 km for MEO, and 36,000 km for GEO [24]. The altitude is directly related to the services offered to the end users. Without loss of generality, the farther is the satellite from the Earth surface, the greater is the Earth coverage area. Indeed, the Earth Coverage for LEO satellites is quite small, for MEO is larger and for GEO is sizeable. For instance, according to the authors in [25], a LEO satellite located 550 km over the Earth surface, having an elevation of 40 degrees, can cover an area of approx. 1.05 million km squared, with an approximate radius of 580 km. At the same time, according to the authors in [26], a GEO satellite can cover 40 degrees of latitude, i.e., approximately one-third of the Earth surface. Given that the coverage range is directly related to the number of satellites to be operated, such a number decreases when the distance from the Earth increases.

SATCOM uplink and downlink channels adopt different frequencies to mitigate the interference on the ground and at the satellite. The band, frequency regulations, and recommendations are authorized by Federal Communications Commission (FCC) and International Telecommunications Union (ITU). For instance, according to the European Space Agency (ESA) [27], SATCOMs frequency bands are standardized in the range of $1 \sim 40$ GHz, as reported in Table 3.

For instance, Inmarsat [28] is a provider of SATCOM services that adopt GEO satellites to provide telephone and data services to users worldwide. Companies like SpaceX [29] and Iridium [30,31] are planning to launch in orbit thousands of LEO satellites to provide low latency, broadband internet systems, voice, and data services anywhere on Earth.

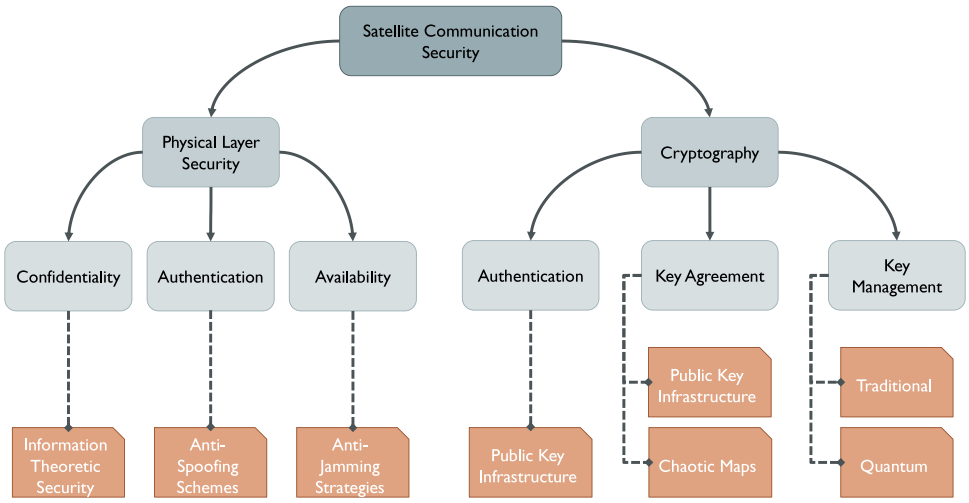


Fig. 1. Taxonomy and classification of the major scientific contributions dealing with security in SATCOM. We identified two major research streams, i.e., physical-layer security and cryptography solutions. Within each stream, we extract specific research domains, where several different solutions are available.

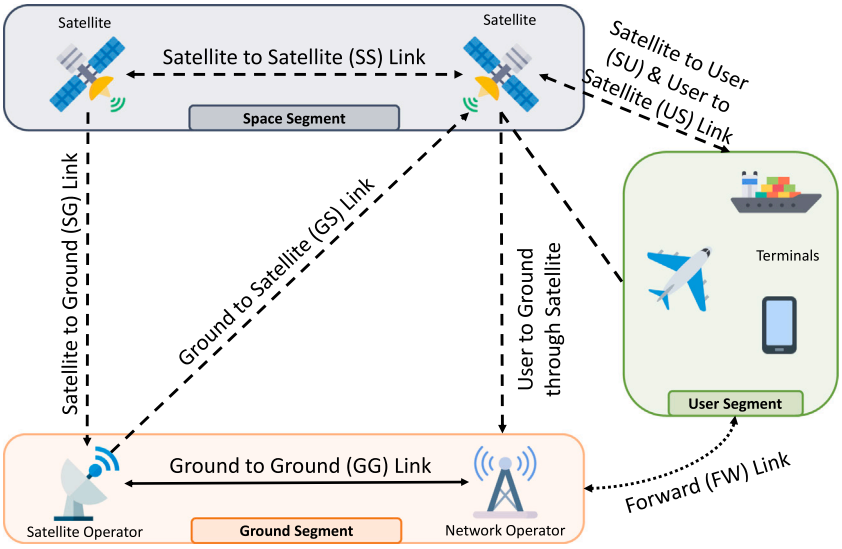


Fig. 2. SATCOM architecture.

2.2. Communication architecture

The reference communication architecture of a SATCOM system, as depicted in Fig. 2, is generally characterized by: (i) a space segment including the *Satellite to Satellite* (SS) and the *Satellite to Ground* (SG) links; (ii) a ground segment, defined by the satellite operators (or gateways) and network operators, enabling the *Ground to Satellite* (GS), *Ground to Ground* (GG), *Satellite to Ground* (SG), forwarding, and the *Satellite to User* (SU) links; and finally, (iii) a user segment, which includes the terminals, e.g., ships, airplanes, and satellite smartphones, enabling the additional *User to Ground* (UG) and the *User to Satellite* (US) links.

The space segment of a SATCOM architecture is one of the three main components of a SATCOM system. This segment comprises GEO satellites to support business in navigation, data, mobile television, and radio broadcasting systems. At the same time, MEO satellites are deployed to deliver low-latency and high-bandwidth data connectivity to service providers, agencies and industries, and to support the network connectivity in the avionic/maritime domain. LEO satellite constellations are also adopted for several applications such as imaging, and low-bandwidth telecommunications and broadband internet. Each of these satellites is placed in orbit by a launch vehicle. The space segment also includes military and defense communication systems, as well as commercial SATCOM transponders and payloads. Note that the afore-mentioned communication links involving satellites all use frequencies in the L-band, in the range [1 – –2] GHz.

The ground segment can help to establish the communication between the satellites and all the terminals defined in the user segment. It comprises dedicated Gateway stations, namely Satellite Operator, infrastructures for control, Network Operator such as the Network Control Centre (NCC) and the Network Management Centre (NMC) supporting the satellite access requests from users.

The user segment includes the user terminals, such as satellite mobile phones, ships, and airplane, to name a few. These devices can communicate with satellites by leveraging the link between the ground segment and the user segment, such as the forward link [32], while their communication with the gateways can take place over any communication technology. The forward link consists of both an uplink (base station to satellite) and a downlink (satellite to mobile user). Conversely, constellations like Iridium, Globalstar, Thuraya and Inmarsat allow a direct connection of the user handsets to the satellites, using the *User to Satellite* (US) link that typically uses frequencies in the L-band.

Table 2
Acronym list.

Abbreviation	Definition
AES	Advanced Encryption Standard
AF	Amplify and Forward
AGC	Automatic Gain Control
AI	Artificial Intelligence
AWGN	Additive White Gaussian Noise
CNR	Carrier-to-Noise Ratio
CPS	Cyber–Physical Systems
CRN	Cognitive Radio Network
CSI	Channel State Information
D2D	Device-to-Device Communications
DF	Decode and Forward
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ESA	European Space Agency
ESR	Ergodic Secrecy Rate
FDMA	Frequency Division Multiple Access
GG	Ground-to-Ground
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IoST	Internet of Space Things
IoT	Internet of Things
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MITM	Man-In-The-Middle
mMIMO	Massive MIMO
NFC	Near Field Communication
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NOMA	Non-Orthogonal Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiplexing Access
OTP	One-Time-Pad
PDR	Packet Delivery Ratio
PS	Power Splitting
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency IDentification
RSMA	Rate-Splitting Multiple Access
SATCOM	Satellite-based Communication
SDN	Software Defined Networking
SDR	Software Defined Radio
SEE	Secrecy Energy Efficiency
SG	Satellite-to-Ground
SIMO	Single-Input Multiple-Output
SINR	Signal to Noise plus Interference Ratio
SISO	Single-Input Single-Output
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SRM	Secrecy Rate Maximization
SS	Satellite-to-Satellite
TDMA	Time Division Multiple Access
TS	Time Splitting
UAV	Unmanned Aerial Vehicles
VLC	Visible Light Communications
VSAT	Very Small Aperture Terminal

While the above discussion covers the traditional SATCOM architecture, many variations can be found. In this context, it is worth noting that the 3GPP issued several standards over the last few years, with the objective to define the general architecture of non-terrestrial satellite networks in the context of 5G networks. Such standards are meant for several types of non-terrestrial communications, including GNSS, High-Altitude Platform Systems (HAPS), and air-to-ground communications—illustrating use-cases, scenarios, channels to be used, and modulation formats, to name a few [33].

Finally, from the security perspective, note that attacks can be launched in any of the identified segments. Thus, the ground segment should be appropriately secured, as well as any communication originating from the satellite should be protected, independently from its target destination (ground or space). More details on the specific threats will be provided in the following sections.

3. Physical layer security schemes for SATCOM

In this section, we introduce, review, and classify approaches investigating security issues of SATCOM technologies at the physical layer. Specifically, Section 3.1 introduces information-theoretic security approaches for physical layer confidentiality of communications, Section 3.2 focuses on GNSS anti-spoofing techniques, while Section 3.3 includes considerations on anti-jamming solutions of SATCOM. To conclude our critical discussion, Section 3.4 summarizes the main lessons learned while Section 3.5 highlights future research directions in the area of physical-layer security.

3.1. Information theoretic security

SATCOMs are particularly prone to eavesdropping due to the broadcast nature of the wireless medium and the very large coverage area. Usually, the confidentiality of SATCOM communications is provided via traditional cryptographic protocols such as Advanced Encryption Standard (AES), working at the MAC-layer or above. However, legacy satellites deployments often use old and proprietary customized versions of AES, frequently found later to be insecure. As a result, motivated adversaries featuring powerful capabilities and tools can easily collect a consistent amount of encrypted data and possibly compromising communications confidentiality. Moreover, many satellites deployments were set up several years ago, when wireless security was not conceived as a requirement. Indeed, attacks on SATCOM channels was conceived by the operators as hard to achieve, and overall, security was thought as a slow-down factor rather than an enabler. Thus, many satellites do not implement any security protection, and updating them today would require high costs [34].

Taking into account the above exposed issues, in the last years many contributions proposed to provide confidentiality to SATCOM scenarios by applying information-theoretic security schemes. The rationale supporting such schemes is the following: information-theoretic security approaches leverage the inherent randomness and noise of SATCOM communication channels to minimize the amount of information that can be extracted at the PHY layer by an unauthorized receiver [35]. This is typically achieved by guaranteeing that the quality of the channel, expressed in terms of Signal-to-Noise Ratio (SNR), exceeds a given bound only at the authorized receiver's location while remaining below the set threshold in other locations, so that an eavesdropper cannot decode the received message. Moreover, such schemes typically do not assume any constraints for the eavesdropper in terms of processing capabilities or network parameter knowledge, and the resulting security features can be quantified analytically via dedicated channel-level metrics. The afore-mentioned security features are achieved without resorting to cryptography materials (e.g. shared key, certificates) or crypto related computations, hence resulting in a very efficient solution (from the computational, storage, and bandwidth point of view).

We present a comprehensive classification of the scientific contributions that achieve confidentiality via information-theoretic schemes in SATCOM scenarios in Table 4. In the following, we summarize the most important features identified throughout our analysis.

Performance Metrics. Many performance metrics can be used to evaluate the effectiveness of a scheme proposed to ensure confidentiality at the PHY-layer via information-theoretic schemes, including, e.g., the secrecy capacity/secrecy rate, average secrecy rate, and secrecy outage probability, to name a few. We hereby present the definition of the most important ones, leading to the definition of all the others.

We assume that a malicious user E is interested in eavesdropping the traffic exchanged between two legitimate network entities and correctly decoding the information. The *Secrecy Rate* of the communication

Table 3
Satellites frequency bands and applications.

Satellite frequency [GHz]	Band name	Applications
1–2	L	Positioning Systems, Mobile phones, Sea/Land/Air Communications, Radio
2–4	S	NASA communications with Space Shuttle and International Space Station
4–8	C	Satellite TV/feed
8–12	X	Military, radar (continuous-wave, pulsed, single-polarization, dual-polarization, synthetic aperture radar, phased arrays), weather monitoring, air traffic control, maritime vessel traffic control, defence tracking, vehicle speed detection
12–18	Ku	Broadcast satellites
26–40	Ka	Close-range targeting radars on military aircraft

Table 4
Comparison of scientific contributions adopting information-theoretic approaches for SATCOM confidentiality.

Ref.	Link	CSI	Adversary	Adversary antennas	Adversary antenna type	Performance metrics
[36]	SG	Imperfect, Statistical	External	Single	Omni-Directional	SOP, SR
[37]	SG	✓	Internal, External	Single	Omni-Directional	SR
[38]	SG	✓	Internal	Multiple	Omni-Directional	SR
[39]	SG, GS	✓, Imperfect	External	Single	Omni-Directional	Secrecy Capacity (SC)
[40]	SG	✗	External	Dual Polarized Antenna	Omni-Directional	Polarization Filtering
[41]	SG	Imperfect	Internal	Single	Omni-Directional	Sum SR
[42]	SG, GS	✓, Statistical	Internal	Single	Omni-Directional	SC
[43]	SG	✓	External	Single	Omni-Directional	SR
[44]	SG	✓	External	Unipolar Parabolic Antennas	Omni-Directional	SR, SC
[45]	SG	✓, Imperfect	External	Single	Omni-Directional	SR
[46]	SG, GS	✓	External	Single	Omni-Directional	Sum SR
[47]	SG	✓	External	Single	Omni-Directional	SR
[48]	SG	✓	External	Single	Omni-Directional	SR
[49]	SG	✗	External	Single	Omni-Directional	SC, SNR, BER
[50]	SG	✓	External	Single	Omni-Directional	SC, SOP
[51]	SG	Imperfect	External	Multiple	Omni-Directional	SR
[52]	SG	Imperfect	External	Single	Omni-Directional	SR
[53]	SG	✓	External	Single	Omni-Directional	SOP, SC
[54]	SG, GS	✓, Imperfect	External	Single	Omni-Directional	SC, SOP
[55]	SG	✓	External	Single	Omni-Directional	SC

link is defined as the difference between the capacity of the eavesdropper E and the capacity of the legitimate user [56], where the *capacity* is the maximum transmission rate at which an eavesdropper is unable to decode any information. The *secrecy rate* of the legitimate source-to-destination communication link at the physical layer is defined as in the following Eq. (1):

$$S = C_L - C_E, \tag{1}$$

where C_L is the capacity of the legitimate channel and C_E is the capacity of the channel source-eavesdropper.

Another important metric is the *Secrecy Outage Probability (SOP)*, defined as the probability that the instantaneous secrecy capacity drops below a specific threshold value, representing a target secrecy rate [57]. The other metrics listed in Table 4 can be derived from the ones previously introduced. Additional details can be found in surveys dedicated to the topic, such as [35].

Link. The largest part of the analyzed works considered the Satellite-to-Ground (SG) link, applying information-theoretic approaches to secure the communications from the satellite to the ground receivers. To the best of our knowledge, only four works considered the Ground-to-Satellite link, i.e., [39,42,46], and [54], while other links are never considered.

CSI Availability. One of the prominent features allowing to compare the contributions on physical-layer security is the amount of information known to the network about the attacker. Looking at the adversary model, the most restrictive assumption is the complete unavailability of information about the channel experienced by the eavesdropper (in technical terms, this is the Channel State Information (CSI)). The vast majority of the works assume the perfect knowledge of the channel quality at the eavesdropper side. This is the most secure approach to analyze the problem from an information-theoretic perspective, as it allows to maximize in analytical terms the difference between the legitimate channel and the (potentially) eavesdropped one, i.e. the secrecy rate. In practice, the cited objective is guaranteed by either reducing the probability of correct signal decoding by the adversary, or maximizing the secrecy rate of the main communication links. Few other approaches, instead, assume to know either partially (Imperfect) or completely the channel experienced by potential eavesdroppers. Such adversary model is often referred to as an *active eavesdropper*, as it is a legitimate network node, interacting with the network at times (so, its CSI parameter is known), but also equipped with eavesdropping capabilities on other communications. A few contributions, such as [36,39,41,45,51,52,54] evaluated the impact of the aforementioned assumption on the related security metrics.

Adversary. In line with related work, we consider two types of adversaries: the internal and the external one. In particular, we define an *internal* adversary as an attacker playing the role of a legitimate network entity, actively participating in the network activities by transmitting and receiving information, such as an *active eavesdropper* [58]. We define an *external* adversary as an attacker who is not part of a legitimate SATCOM, also striving to remain not detected–*hidden*. This latter category also comprises the *external eavesdropper*, needing a simple receiving antenna tuned on the same frequency of the legitimate communication channel to receive packets successfully.

Adversarial Receiving Antennas. The simplest adversary model, considered by most of the analyzed contributions, is a single eavesdropper, not sharing any information with other receivers [36,37,39,41–43,45–50,52–54]. We remark that this is the easiest to analyze from the security perspective, as the previously-mentioned performance metrics only have to consider a single adversary. Just a few works, i.e., [44,51], considered multiple antennas, even if no collusion between them is considered, thus reducing the adversary model to the same of multi single-antenna adversaries.

Adversarial Antenna Type. All the analyzed contributions consider adversaries equipped with omnidirectional antennas, i.e., antennas capturing the information independently from the source location and

Table 5
Comparison of GPS/GNSS Spoofing Detection Methods and related system requirements.

Ref.	GNSS Spoofing Detection Means	No need of multiple antennas	No PHY-layer information required	No need of ad-hoc network infrastructure	No need of dedicated hardware
[63]	Statistics Approach	✓	✓	✓	✓
[64]	HF Antenna Motion & Carrier-Phase	✓	✗	✓	✗
[65]	Phase-Only Analysis of Variance	✗	✗	✓	✗
[66]	Symmetric Difference Autocorrelation Distortion Monitor and a Total in-band Power Monitor	✓	✗	✓	✗
[59]	Meteor Burst Communications	✗	✗	✗	✓
[62]	Cellular Network	✓	✓	✓	✓
[67]	Cross-Check Receivers	✗	✗	✗	✗
[68]	Multilateration Phasor Measurement Units in Smart Grids	✗	✓	✗	✗
[69]	Cross-Correlation and Cooperative Authentication	✓	✓	✗	✓
[70,71]	Carrier-Phase Measurements	✗	✗	✓	✗
[72]	Code Signals Correlation	✓	✓	✓	✗
[73]	Total Signals Energy Measurement	✓	✗	✓	✗
[74]	Time Authentication	✓	✗	✗	✗
[75]	Multi-Receiver Hybrid Communication Network for Power Grid Timing Verification	✓	✗	✗	✗
[76]	Fraction Parts of Double-difference Carrier Phases	✗	✗	✓	✗
[77,78]	Channel Gain/Estimation Noise	✓	✓	✓	✓
[79]	Least Absolute Shrinkage and Selection Operator	✓	✗	✓	✓
[80]	Chips-Message Robust Authentication	✓	✗	✓	✗
[81]	Neural Network	✓	✓	✓	✓
[82–84]	Maximum-Likelihood	✓	✗	✓	✗
[85]	K-mean clustering	✓	✗	✓	✓
[86]	Control Theory (IMU sensor) in UAVs	✓	✓	✓	✓
[87]	Cooperative Receivers Positions	✓	✓	✗	✓
[88]	Semi-Codeless Receiver	✓	✗	✓	✗
[89]	Genetic Algorithm, Shortest Path and Pattern Matching	✓	✓	✓	✓
[90]	Supervised Machine Learning	✓	✗	✓	✓
[31]	IRIDIUM Ring Alert	✓	✓	✓	✓

(partially) radio environment. While such a model could appear the strongest, it does not consider a realistic SATCOM scenario, where obstacles at the ground could alter the profile of the received signal, as well as the previously-mentioned performance metrics.

3.2. Anti-spoofing schemes

Without loss of generality, *spoofing* refers to disguising a communication from an unknown source as being from a known, trusted source [18].

Like any other wireless communication technology, SATCOMs are in principle vulnerable to spoofing attacks. The issue is even more cogent because of the presence of legacy deployments, as previously described in Section 3.1. Today, several satellite systems transmit either unauthenticated messages, or authenticated at the application layer, via either symmetric key (implicit authentication) or public key solutions. A few examples include GNSS technologies such as GPS, Beidou, Glonass, and Galileo, and weather satellites such as National Oceanic and Atmospheric Administration (NOAA) and Meteor [59].

Given the considerable threat surface, the design of anti-spoofing techniques for SATCOM scenarios has been largely focused on GNSS technologies due to their widespread use and increasing importance in the modern connected society [60]. Today, thanks to the sensitive advances in the design of Software Defined Radios (SDRs), performing GNSS spoofing attacks is surprisingly easy. An attacker needs an SDR and an omnidirectional transmitting antenna; by downloading freely-available tools such as `gps-sdr-sim` [61], the attacker just needs to run a script to emulate a complete satellite constellation and move the target wherever in the world, also for a significant period of time [62]. Considering that GNSS satellites are also used for time synchronization in several IoT deployments, detecting spoofing attacks with lightweight and effective techniques is of paramount importance.

Table 5 summarizes the most important contributions in the topic of GNSS anti-spoofing and cross-compares them across reference system features.

GNSS Spoofing Detection Means. A large variety of means have been used to detect GNSS spoofing attacks. Approaches use either PHY-layer information [59,64–67,70,71,73–76,79,80,82–85,88,90], or additional communication technologies [31,62,63,68,69,72], or techniques based on Machine Learning (ML) over heterogeneous data [81–85,89,90]. All these techniques share the basic consideration that the bitstrings in GNSS signals cannot be modified to be more secure before being transmitted. Indeed, such modifications would require temporarily stopping the operation of the GNSS satellite, causing significant and unmanageable costs and effort.

Usage of Multiple Receiving Antennas. Simplest GNSS spoofing attacks assume that the adversary transmits a fake GNSS signal using only a single antenna. Signal cross-correlation detection methods identify such attacks by discriminating the injected signal from the expected one, as it is transmitted using different devices than the ones the target satellite is equipped with. Comparing the correlation of the received signals using more than one antenna at the receiver side will result in a significant difference in signal characteristics, such as the carrier phase and amplitude. This is just an example of a technique employing multiple receiving antennas to detect GNSS spoofing, and other examples include the contributions by the authors in [59,65,67,68,70,71,76]. Although being relatively cheap to deploy, such solutions usually require the deployment of multiple antennas and their connection to a single system, i.e., the hardware modification of the receiving device. Often, such operations might be too expensive or impractical to be applied due to application-specific limitations.

Usage of PHY-layer information. GNSS messages transmitted by satellites go through different phases of signal processing before being converted into a digital form at the receiver side. The anomalies in the characteristics of signals during any of these processing phases could be used to detect counterfeit GNSS signals [91]. Anomalies can be found in signals features such as received power, Carrier-to-Noise Ratio (CNR), quality, correlation, Automatic Gain Control (AGC), clock bias, and angle of arrival, to name a few. Such features are used in many approaches, e.g., [64–66,74], to detect GNSS spoofing attacks. On the one hand, such techniques could be compelling and reliable. On the other hand, they require the receiving devices to access such information, which is not always possible. Indeed, many modern chipsets do not provide PHY-layer information to the devices they are connected to or integrated into, preventing the application of such approaches.

Usage of Ad-Hoc Network Infrastructures. Other contributions leverage additional network infrastructures, set up ad-hoc for GNSS spoofing detection. This is the case of approaches using dedicated sensors deployments [59,67–69,74,75,87]. Other approaches, such as [31,62], use opportunistic signals gathered by other communication infrastructures, such as the cellular network and the IRIDIUM constellation. While the first set of approaches require a dedicated setup, that is not always possible, the security of the second class of approaches mostly depends on the adversary model and on its capability to spoof also the additional wireless signals.

Usage of Dedicated Hardware. Many solutions have been proposed in the last years, recurring to dedicated hardware to detect GNSS spoofing attacks. Such approaches leverage either specific information available from the radio channel [64–67,70,71,73–76,80,82–84,88], or specific type of arrays of antennas, or the use of dedicated sensors providing inertial measurements [86]. Similarly to previous approaches using multiple antennas, such techniques might be very efficient. However, they require the adoption of compatible hardware, which sometimes does not represent a viable solution.

3.3. Anti-jamming strategies

In this section, we discuss the most important contributions dealing with *anti-jamming* methods in SATCOM scenarios. Without loss of generality, *jamming* is defined as the injection of intentional interference into the wireless channel in a way to disrupt the operations of a legitimate communication channel [92]. Several classes of jammers have been proposed in the scientific literature throughout the last years [93]. With reference to the portion of time where they are active, jammers can be constant, alternate, proactive (if they choose a channel in advance, and jam it) [94], or reactive (if they jam a specific channel only when RF activity is detected on that channel). Considering the number of frequencies jammed at the same time, jammers can be spot (a single jammed frequency) [95], sweep (multiple frequencies, at different times) [96], or barrage (multiple frequencies at the same time) [97]. Finally, based on the type of signal injected to cause interference, we can have noise-jammers (if noise of a different type, e.g., Additive White Gaussian Noise (AWGN) is injected on the channel), or deceptive-jammers (if they inject a signal similar to the legitimate ones). The effectiveness of a jammer strictly depends on the communication parameters [98] set by both the transmitter and the receiver [99]. Overall, to maximize the performance of the jammer, the adversary should carefully analyze the radio link and then design and deploy the appropriate type of jammer.

Jamming is particularly relevant in the context of SATCOM links, and several contributions highlight the inefficacy of currently-deployed communication schemes, e.g., Code Division Multiple Access (CDMA), when powerful jammers target the communication links [100]. Table 6 reviews the most important contributions providing anti-jamming techniques in the SATCOM context and cross-compares them across reference features.

In the following, we summarize the most important considerations emerging from our analysis.

Link. Similarly to previous physical-layer solutions, also anti-jamming strategies mostly considered the Satellite-to-Ground communication link, focusing on increasing the availability of satellite services on the ground. A few works, such as [107,111], and [119], considered also the Ground-to-Satellite link, while only one work, i.e, [119], discussed anti-jamming solutions for the Ground-to-Ground link. The Satellite-to-Satellite link is never considered because of the actual hardness of the jamming at high distances, though further studies on this segment would be valuable. **Technology.** While some works focused on a generic SATCOM technology, most were more specific, and analyzed the jamming issue in GNSS [104,106,108,110,116,117,121] and Military SATCOM constellations. Others were even more focused, proposing anti-jamming schemes tailored to the specific GNSS technology, such as the Chinese Beidou [115], the Russian Glonass [105], and the US GPS [101–103,112,120].

Number of Jammers. Most of the analyzed works considered single jamming devices that are usually easier to detect and isolate from a SATCOM link due to its vast coverage range. Other recent contributions, such [107,109,111,113,114,119] introduced particular techniques to defend the commercial and civilian SATCOMs when one or more jammers are deployed in the scenario, thus being more effective in real deployments. Indeed, the deployment of multiple jammers is an essential problem in tactical and military scenarios, where the adversary is so powerful to make the adoption of the current solutions challenging or impractical.

Type of Jammer. Characterizing and profiling the type of jamming affecting the communication link is the first step towards the deployment of an effective anti-jamming solution. Based on such considerations, the authors in [109,112,116,117,119,121] proposed anti-jamming algorithms able to characterize the jamming signals emitted from multiple jammers and still guarantee the communication quality. In this context, it is worth mentioning the work by the authors in [118], mitigating jamming in SATCOM by proposing a cost-effective solution able to thwart jamming through an efficient jamming-dependent adaptive frequency hopping pattern.

Anti-Jamming Technique. Many scientific contributions used physical layer parameters to estimate and guarantee the availability of downlink and uplink SATCOMs under jamming. For instance, to face malicious jamming attacks, the contributions in [101–103,105,112,120] recommended the use of well-known techniques such as fast orthogonal search, signals cross-correlation, turbo codes, and distance theoretical models for the GPS signals. Alternatively, the authors in [105] demonstrate that the single-frequency multi-constellation receivers offer better jamming resilience than multi-frequency (L1 + L2) GPS receivers and that the GLONASS constellation demonstrated a better resilience than GPS. Indeed, they propose a multi-constellation solution that adopts GPS and GLONASS receivers for maritime applications.

No need of Dedicated Hardware. It is worth noticing that contributions such as [103,104,111,113,118–120] do not require any dedicated hardware to deploy the provided solution in a real environment. Such solutions can be implemented via simple software updates—a cheap and convenient feature. Conversely, the remaining solutions require to intervene on the hardware, and their deployment depends on the opportunity, cost, and convenience of such a modification.

Assessment Methodology. Finally, we notice that most of the analyzed approaches were evaluated using simulations. Although simulations provide useful details into the performance of the disclosed approaches, they often miss some elements of the actual deployment, hard to be modeled and controlled into a computer-based environment. Taking into account such considerations, approaches such as [102,105,108,110,120,121] worked on real deployments, showing the effectiveness of their solutions through via practical experiments or real-world data.

3.4. Lessons learned

In the following, we summarize the main lessons learned from the investigation and cross-comparison of the approaches working on improving the security of SATCOM deployments via physical-layer solutions.

No Satellites Hardware Update. All the analyzed approaches do not propose the modification of the transmitted signals or the transmitting chain. Indeed, modifying a satellite is assumed to be too expensive to be performed, both from the financial and the operational perspective. Thus, assuming that the authenticity/availability received signal cannot be fully guaranteed, the studied proposals come up with solutions able to minimize the impact of different security attacks.

Table 6
Comparison of anti-jamming techniques and related system requirements.

Ref.	Link	Technology	Jammers	Jammer type	Technique	No dedicated hardware	Assessment
[101]	SG	GPS	Single	Sweep, Spot	Fast Orthogonal Search	✗	Simulations
[102]	SG	GPS	Single	AWGN, Spot	Signals Cross Correlation	✗	Experimental
[103]	SG	GPS	Single	Constant, Spot, Barrage	Turbo Codes	✓	Simulations
[104]	SG	GNSS	Single	Deceptive, AWGN	ML Classification	✓	Simulations
[105]	SG	GLONASS, GPS	Single	Sweep, Spot	Dual Frequencies Correlation	✓	Experimental
[106]	SG	GNSS	Single	Generic	Various Filtering	✗	Analysis
[107]	GS, SG	40 GHz UL, 20 GHz DL	Single	Reactive	Geometric Jamming Constraints	✗	Simulations
[108]	SG	GNSS	Single	Sweep	Sum-of-Squares, Correlation	✗	Experimental
[109]	SG	SATCOM	Multiple	Reactive	Dynamic Spectrum Access	✗	Simulations
[110]	SG	GNSS	Single	Constant	Pulse Blanking	✗	Experimental
[111]	GS	SATCOM	Single	Constant, AWGN	Game Theory	✓	Simulations
[112]	SG	GPS	Multiple	Constant, Barrage	Multi-objective optimization	✗	Experiments
[113]	SG	SATCOM	Single	Constant, AWGN	Convolutional Neural Network	✓	Simulations
[114]	SG	SATCOM	Single	Generic	Polarization Diversity	✗	Simulations
[115]	SG	Beidou	Single	Generic	Spatial-Time Polarization	✗	Simulations
[116]	SG	GNSS	Multiple	Constant, AWGN	Cross Spectral Self-Coherence Restoral algorithm	✗	Simulations
[117]	SG	GNSS	Multiple	Sweep	Adaptive-Partitioned Subspace Projection	✗	Simulations
[118]	SG	SATCOM	Single	Constant, Barrage	Frequency Hopping	✓	Simulations
[119]	GS, GG	SATCOM	Multiple	Constant	Maximum Ratio Combining	✓	Simulations
[120]	SG	GPS	Single	Constant, Barrage	Distance Theoretical Model	✓	Experimental
[121]	SG	GNSS	Multiple	Continuous Wave	Wavelet Transform	✗	Simulations, Experiments

Significant Receivers Updates. Consequently to the previous point, the proposed security techniques have a large impact on the receivers, requiring either hardware or software modification that impacts their operations. When uninterrupted operations should be guaranteed, deploying a new solution for either confidentiality, anti-spoofing, or anti-jamming working at the PHY-layer might find challenges, even if potentially guaranteeing high efficiency at low energy and processing costs.

Channel State Information (CSI) Availability. Looking at information-theoretic schemes for SATCOM confidentiality, being aware of the CSI experienced by the passive eavesdropper(s) is critical when calibrating the effectiveness of a security solution. Indeed, if the CSI experienced by the eavesdropper when communicating with the network is available to the transmitter: (i) the secrecy capacity can be maximized; and, (ii) the SNR of the adversary is minimized. Data secrecy and secrecy capacity are handled as constraints of the overall optimization problem, where the overall aim is to ensure that the secrecy rate of the main communication link does not degrade below a minimum threshold or, equivalently, the secrecy outage probability does not exceed a specified upper bound.

Detection vs. Prevention. Approaches working on anti-jamming and anti-spoofing mainly focus on detecting the attack once it has been launched. This is a crucial difference from approaches providing confidentiality using information-theoretic schemes that prevent the attacker from gaining information. Such difference is due to the different adversarial models (active in the first two mentioned cases, passive in the second one), that lead to different countermeasures. Combining approaches for multiple security objectives, e.g., anti-jamming and confidentiality, might require new feasibility studies and solutions.

3.5. Future directions

We can identify a few promising future research directions in the area of physical layer security for SATCOM as a result of the investigation carried out in this section.

Directional Adversarial Antenna. Almost all the contributions in the three analyzed sub-areas assumed adversaries equipped with omnidirectional antennas. Omnidirectional antennas radiate equal radio power in all directions; thus, they can often be assumed as the worst-case for the integrity of the satellite communications. However, there are specific situations where an adversary equipped with directional antennas can be more disruptive, e.g., in cases where the location of the target communication link is well-known. Directional and semi-directional antennas focus the radiated power in narrow beams, particularly in one direction only [122]. From the security perspective, this is an additional powerful feature for an adversary, as it can help to reduce the interference caused by other radio activities, improving the adversary's expected performance. This is an interesting scenario to be investigated for satellite links' security, which has still not been fully explored by Industry and Academia.

Security of the Satellite to Satellite Communication Links. Despite being effective, none of the above-described security solutions provided a security evaluation of the satellite to satellite communication links. This is because of the hardness of both obtaining information about the communication protocols used by such links (often protected by intellectual property rights) and by the nature of such links, envisioned as a kind of core network, far from users' services. However, due to the wireless nature of such communications, attacks on these links are both possible and potentially dreadful, as they can disrupt the availability of a SATCOM by just affecting the operation of a single link. For instance, Viasat affirms that because LEO satellites are not in constant communication with the ground, a satellite to satellite link can ease the data-sharing mechanism between adjacent satellites [123]. A malicious user could interrupt these types of communications by just jamming such a link. Also, it is unclear if and how physical-layer security techniques can be applied effectively for these links. Thus, investigating the security of Satellite-to-Satellite links is an appealing future research direction.

Intelligent Reflecting Surfaces (IRS). Intelligent Reflecting Surfaces are one of the most attracting topic in the physical-layer security research community, and they are gaining momentum [124]. Thanks to the deployment of a massive number of antenna elements on the satellites, it is possible, in principle, to assist the non-terrestrial network communications by focusing the electromagnetic energy in the intended direction, with consequent benefits in terms of security—receivers out of the intended direction are implicitly excluded from receiving signals [125]. A few recent works investigated the theoretical performance of secure communications associated with intelligent reflecting surfaces and the deployment of intelligent reflecting surfaces on UAVs and satellites, e.g., [126–128], just to name a few. Therefore, in line with the current trend, we expect a surge of scientific contributions in the upcoming period focusing on the application of IRS for SATCOM scenarios. On the one hand, such works will explore the validity of

previous results on PHY-layer security for terrestrial links when deployed to satellite links. On the other hand, when IRSs are deployed, new security threats might arise, specific to the new technology. Just to provide an example in this direction, an adversary could use a drone flying at significant altitude to boost its SNR when receiving a signal from an IRS deployed on a satellite, or to move within an area with a better coverage without being noticed by terrestrial receivers.

GNSS Spoofing Detection via Artificial Intelligence. In line with a worldwide scientific trend, many recent proposals applied Artificial Intelligence (AI) algorithms to solving GNSS issues, including the detection of spoofing attacks [129]. Specifically, AI-based solutions can be used to detect anomalies in the received signals, so as to identify the presence of the attacker. For instance, the recent proposal by the authors in [130] use cross-correlation of the received signals to detect anomalous messages, indicating the presence of an attacker. Still, there are several challenges that are to be solved, including the discrimination of legitimate and malicious interference, mobility of the attacker, and use of publicly-available data of satellites (e.g., ephemeris) to imitate satellites movement. In this context, we also notice that several real-world dataset are available and released as open-source, such as [131,132]. Thus, we the are seems ripe to experience a renewed interest, likely ignited by researchers and industry with expertise in the application of AI algorithms to different domains.

Friendly Jamming. Friendly jamming techniques disrupt all the communications in a given area by allowing, at the same time, legitimate parties to communicate [58]. Friendly jamming can be achieved in several different ways, e.g., through pre-shared knowledge of jamming time and frequency patterns, or via specific positioning of the legitimate communicating devices, in a way that the SNR exceeds the minimum required values only in specific locations, where the legitimate receiving nodes are deployed.

Overall, deploying friendly jamming in SATCOM scenarios may be relevant and useful, e.g., to minimize eavesdropping capabilities of the adversary in military scenarios, while still allowing legitimate devices to communicate in a cheap way. We notice that none of the security techniques discussed in the previous subsections investigated the feasibility of friendly jamming in the context of SATCOM. Note that achieving friendly jamming is not as easy as jamming a communication link. Indeed, friendly jamming requires controlling with extreme precision the timing, the frequency, and the context to be jammed, in a way to know precisely when and how to transmit. In this context, analytical and experimental results about the feasibility and the degrees of freedom of friendly jamming in SATCOM are still needed.

Spoofing of non-GNSS constellations, e.g., NOAA. At the time of this writing, the majority of contributions dealing with spoofing and anti-spoofing techniques in the SATCOM context focused on GNSS constellations, due to their higher impact and involvement in everyday life. However, non-GNSS constellations such as NOAA and Very Small Aperture Terminal (VSAT) are also widely used, e.g., by ships or other devices in remote locations. At the same time, their (low) security is comparable to the one offered by GNSS satellites. Solutions to detect and overcome spoofing of the signals emitted by such satellites are still to be investigated and might represent an appealing research opportunity.

Powerful Inter-Communications Adversaries. Most of the approaches using signals from additional communication infrastructures to detect and overcome GNSS spoofing and jamming assumed that the adversary only focused on a single communication link. However, a powerful adversary able to inject noise or spoofing signal of SATCOM and non-SATCOM technologies, eventually using a high powerful antenna, could be disruptive and nullify the effectiveness of such countermeasures. For instance, the adversary could fine-tune its attack strategy, so as to deteriorate the performance of such detection strategies. Such powerful adversaries are not too unrealistic to be thought, and thus, are worth investigating.

4. Cryptography techniques for SATCOM

Many contributions have proposed to apply cryptography techniques to secure SATCOM links. Such works mainly focus on the authenticity and confidentiality of SS and SG communications, and adapt security primitives originated from other domains to work efficiently with SATCOM systems. We can notice that part of the scientific contributions in this area adapt the implementation and network architecture of well-known cryptographic solutions to the SATCOM scenario, while the other part study the effectiveness and consequences of the introduction of novel paradigms, such as quantum computing, with an eye on the requirements of SS and SG communication links. In this section, we review and classify contributions dealing with the application of cryptography schemes in SATCOM, classifying them based on the provided security service. Section 4.1 focuses on techniques for peer authentication, Section 4.2 discusses key agreement schemes, while Section 4.3 introduces approaches for key distribution based on quantum channels. The main lessons learnt from our study are reported in Section 4.4, while Section 4.5 outlines promising research directions in this domain.

4.1. Authentication

SATCOM systems involving users, mobile devices, and ground stations (or network control centers) require establishing trust among the cited entities. However, due to the presence of the wireless medium, SATCOMs are more prone to impersonation attacks. To mitigate this problem, various authentication protocols have been proposed in the literature. Table 7 provides a comprehensive classification of the most important scientific contributions in the field, cross-comparing them across the selected communication architecture, the proposed cryptographic technique, the security properties, the security analysis, and the assessment methodology.

Link. Most of the analyzed works considered the User to Ground Station/Network Control Center through Satellite link depicted in Fig. 2, applying standard cryptography techniques to secure the channel. Many schemes, i.e., [141–144,147,148], considered the protection of the GPS/GNSS communication link, while other links are rarely taken into account.

Key Sharing Technique. Many different key sharing techniques are used for equipping the entities with the crypto material necessary to run authentication protocols. The authors in [133,136,149] proposed a public key cryptographic scheme based on Elliptic Curve Cryptography (ECC) to provide peer entity authentication. Conversely, other proposals assume a pre-shared key, statically known by one or more users. Some other approaches, i.e., [141–144,147,147,148], adopt the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol conceived by Perrig et al. in [150] to provide delayed source authentication for broadcast communications in very resource-limited environments, by leveraging only symmetric cryptographic primitives and hash chains. Focusing on schemes adopting asymmetric cryptography solutions, the adoption of ECC rather than the traditional RSA provides benefits in terms of smaller public and private keys for the same security level, faster key generation and signature operations, as well as low overhead on CPU and memory usage. Rivest–Shamir–Adleman (RSA) schemes are usually very simple to implement, widely deployed in the industry, and specific public key operations such as the signature verification are usually faster than the ones on ECC, considering the same size of the elements. However, the setup of a public-key infrastructure to manage, distribute, and revoke public key certificates is costly and time-consuming. Thus, when a public key infrastructure is not desirable or affordable, and the efficiency of the crypto operations is at premium, symmetric cryptography solutions for digests generation are adopted, such as the TESLA protocol [150]. Symmetric solutions allow to execute very fast encryption and decryption operations, as well as to generate authentication digests that can be produced and verified

Table 7
Comparison of Different Authentication Methods for SATCOM links.

Ref.	Link	Key sharing technique	Security properties	Security analysis	Assessment
[133]	User to Network Control Center through Satellite	ECC	Mutual Authentication, User Anonymity, Unlinkability, Non-Repudiation	Formal	Simulations
[134]	User to Network Control Center through Satellite	Pre-Shared Key	Mutual Authentication, User Privacy, Minimum Trust	Informal	✗
[135]	User to Network Control Center through Satellite	Pre-Shared Key	Mutual Authentication, User Privacy, Minimum Trust	Formal	Simulations
[136]	User to Network Control Center through Satellite	ECC	Mutual Authentication, User Anonymity, Untraceability	Informal	Informal
[137]	User to Network Control Center through Satellite	Pre-Shared Key	Mutual Authentication, User Privacy, Minimum Trust	Informal	✗
[138]	Satellite to Network Control Center	Pre-Shared Key	Mutual Authentication	Informal	✗
[139]	User to Network Control Center through Satellite	Pre-Shared Key	Mutual Authentication	Formal	✗
[140]	User to Network Control Center through Satellite	Pre-Shared Key	Mutual Authentication, User Privacy, Minimum Trust	Discussion, Formal	✗
[141, 142]	GPS/GNSS Satellites	TESLA	Message Authentication	Informal	Simulations
[143]	Galielo/GNSS Satellites	TESLA	Message Authentication	Informal	Simulations
[144]	GPS/GNSS Satellites	PKC and TESLA	Message Authentication	Informal	Simulations
[145]	SS, SG Control Center	Symmetric Encryption	Mutual Authentication, Message Authentication	Informal	Experiments
[146]	User to Network Control Center through Satellite	Pre-Shared Key	Mutual Authentication, User Privacy	Informal	✗
[147]	GPS/GNSS Satellites	TESLA	Message Authentication	Informal	Simulations
[148]	Galielo/GNSS Satellites	TESLA	Message Authentication	Informal	Experiments
[149]	User to Ground Station through Satellite	ECC	Unforgeability, Mutual Authentication, Conditional Anonymity	Formal	Experiments

very quickly. However, differently from public-key solutions, solutions based on symmetric cryptography requires the communicating parties to share a secret, to be kept private at least for a given amount of time (e.g., in case of TESLA). If a shared key is compromised, it should be discarded and replaced. However, replacing and updating a key can be a time-consuming activity, especially in a context where the communicating entities are orbiting several kilometers above the Earth surface.

Security Properties. The main security property provided by the proposed schemes is mutual authentication, i.e., entities authenticate each other before establishing mutual communication. Equal importance is given to message authentication, which ensures that the message was actually sent by the entity that claimed to have done so. Contributions such as [133–137,140,146,149] guarantee additional properties, such as anonymity and user privacy, adopting techniques that hide the user identity during a communication.

Security Analysis. The schemes proposed by the authors in [133, 139,143,149] are formally proved as secure with reference to certain formal specifications or properties. Some tools that help to prove these properties are ProVerif [151], CryptoVerif [152], AVISPA [153], and Tamarin [154], to name a few. Note that only the security of the cryptographic scheme can be verified through this mechanism, while its integration in the reference system architecture could widen the threat surface.

Assessment Methodology. Similarly to the works dealing with physical-layer security, most of the analyzed schemes use simulation-based evaluation. Only few of them, i.e., [145,147–149], used real data and deployed proof-of-concept.

4.2. Key agreement

Key agreement protocols (a.k.a. key establishment protocols) are used to allow two (or possibly more) entities that could not have anything in common to agree on a shared key to be used to secure further mutual communications [155]. Nowadays, key agreement protocols via public key cryptography or pre-shared keys are used in a range of different security protocols. Although several works proposed lightweight key establishment solutions integrating well-known cryptographic approaches in a variety of application domains, key establishment mechanisms in SATCOM have received only reduced attention. Table 8 provides a comprehensive classification of the scientific contributions dealing with key agreement in SATCOM scenarios, considering reference system requirements and features.

Link. Most of the presented approaches focus on the key establishment in SG and SS links. It is also worth noting that most of the solutions require a software update that can be done via radio link or, in particular situations, by intervening offline on the satellite.

Cryptography Technique. Many different techniques are used to allow the entities to derive a shared secret. Overall, the same considerations introduced for the key sharing techniques in Section 4.1 are still valid for key agreement protocols adopted in SATCOM links. For completeness, we introduce the pro and cons also for the Identity Based Cryptography and the Chaotic Maps. In Identity Based Encryption (IBE) schemes, each communicating entity owns a unique identifier, adopted to compute the correspondent public key. With such an approach, no certificates are needed and no pre-enrollment is required. However, the architecture requires a key generation center, which might be vulnerable to key-escrow attacks, and therefore, exposed to a risk of information disclosure [164]. Unlike public-key cryptography systems, chaotic maps do not require modular arithmetic, being therefore very fast for both encryption and digital signature. Moreover, algorithms based on chaotic maps might not require that large private keys, being computationally efficient. On the downside of such a technique, chaotic maps can produce ciphertext that are bigger than the plain-text [165].

Target Security Service. Most of the presented schemes focus on the balanced protection of the Confidentiality, Integrity, and Availability of data (CIA) by providing, at the same time, identity verification.

Table 8
Comparison of Different Key Agreement Methods for SATCOM links.

Ref.	Link	Cryptography technique	Target security service	Adversary model	Assessment
[156]	SG	ECC	Authentication, Confidentiality, Integrity	Canetti–Krawczyk	Simulations and experiments on smartphone
[157]	General purpose, SG, SS	ECC, RSA	Authentication, Integrity	Active	Formal analysis
[158]	SG (GNSS)	ECC, RSA	Authentication, Integrity	Active	Simulations
[159]	SG (Beidou)	RSA	Authentication, Integrity	✗	Experimental (Ground part)
[160]	SG, SS	Pre-shared key	Authentication, Confidentiality, Integrity, Anonymity	Active/Passive	Formal analysis, Simulations
[161]	SG, SS	Identity based cryptography	Authentication, Confidentiality, Integrity	Extended Canetti–Krawczyk	Formal analysis
[162]	SG (VSAT)	Chaotic Maps	Authentication, Confidentiality, Integrity, Availability	Active	Complexity analysis
[163]	SG	Pre-shared key, ECC, RSA	Authentication, Confidentiality, Integrity, Availability	Active	Formal and complexity analysis

Adversary Model. The Canetti–Krawczyk (CK) and the extended Canetti–Krawczyk (eCK) security models [166], are widely used to verify and provide the aforementioned security properties for key agreement protocols. These models have been developed to build secure protocols that guarantee peer entity authentication and message authenticity during the key exchange procedure. Indeed, the main aim of these models is to provide a method so that the security protocols proposed in the literature can have a match between the implementation and the adoption in a real environment by taking into consideration also possible attacks of an active adversary [167].

Assessment Methodology. In order to evaluate the performance of a key agreement protocol, authors can evaluate the offered security properties by using the formal analysis or discuss the solution. Further, they can estimate the efficiency via simulation tools, like [156,158, 160], or by performing a complexity analysis such as [162,163]. The only contributions providing performance on a real system, i.e., [156, 159], worked on the ground link due to the viability of the approach and its reduced costs.

4.3. Quantum key distribution

Although the soundness of the adopted encryption techniques typically relies on traditional mathematics proofs, quantum architectures are coming out of laboratories to be used in many contexts, based on different assumptions. Overall, Quantum key distribution (QKD) allows two remote parties to securely negotiate a cryptographic key even in the presence of an eavesdropper. However, compared to traditional key distribution schemes, the security of such distribution mechanisms does not rely on cryptographic assumptions (i.e., difficulty of solving specific mathematical problems), but on the unique quantum mechanics properties of the adopted communication strategy at the physical-layer. Thus, even assuming a powerful adversary with unlimited computational capabilities and able to break cryptography assumptions, the robustness of the protocols still holds—basically, QKD protocols allow detecting the presence of an eavesdropper on the communication link [168].

Currently, several QKD solutions have been proposed in the literature, even if there is still a gap between the information theory and practical implementations. As depicted in Fig. 3, QKD systems work by using photons, i.e., particles which transmit light to transfer data [169]. Quantum technology allows two distant entities to agree on a common symmetric key even if they do not share any previous knowledge. The key is adopted with the respective encryption algorithm to transmit and receive encrypted messages over a standard communication channel, even if the One-Time-Pad (OTP) encryption scheme is the most used one. The benefit of this "unbreakable" encryption is that the data is carried via photons, which cannot be copied or eavesdropped without leaving evidence of such an attempt. Indeed, an adversary measuring the state of a photon would disturb the channel, hence compromising the key agreement procedure and providing a kind of tamper-detection evidence. In terms of security, quantum computing could make the current state of the art on security obsolete, jeopardizing the protection of data and communications. This aspect is leading to an acceleration of the adoption of countermeasures (e.g. post-quantum encryption algorithms), especially to protect data and critical infrastructures such as SATCOMs [170,171]. Table 9 provides an overview of the most important QKD techniques proposed in the context of SATCOM, and cross-compares them across reference system features and requirements.

Link. Most of the analyzed contributions propose approaches leveraging a quantum technology for SG and SS communication links. Note that such communication links might be challenging to manage when considering interference, natural phenomena such as sunlight, and the long distances among the entities.

Quantum Protocols. QKD protocols are today already adopted to protect communications through optical communication channels. QKD systems are already operational in different contexts, also allowing long-distance connections in Point to Point (P2P) communications. Several works in the literature such as [172,173,175,183] adopt the well known BB84 quantum key distribution scheme, developed by Charles Bennett and Gilles Brassard in 1984. BB84 was originally described using photon polarization states where no quantum entanglement was required. Conversely, the authors in [174], and [184] propose schemes based on quantum entanglement, i.e., a particular phenomenon where particles remain intimately connected, even if separated by long distances [188]. When it comes to QKD, while the high-level protocols are well understood and are taught in university courses, and commercial products are available on the market [189], the underlying phenomena that make them possible are rooted on the evolving frontiers of physics [190]. As such, a detailed discussion of the cited protocols is beyond the scope set for this survey. However, interested readers can resort to recent authoritative surveys on QKD available in the literature, such as [191–193], to cite a few.

Main Contribution. A large variety of contributions used to distribute the cryptographic key via QKD. Approaches use either free space QKD [172,180], or perform feasibility and efficiency analysis with reference to some specific schemes [174,175,177,179,183,186]. All these techniques share the basic consideration that the quantum technology cannot be compromised due its intrinsic properties.

Assessment Methodology. Differently from approaches based on classical cryptography, most of the contributions focusing on QKD carry out also an experimental assessment, allowing the authors to demonstrate the feasibility of satellite-based quantum communications by experimentally analyzing their efficiency, error tolerance, and security properties.

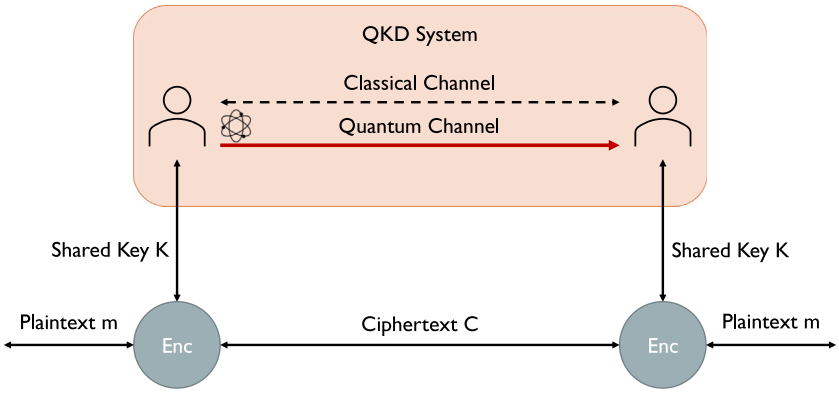


Fig. 3. Generalization of the QKD system architecture.

Table 9
Comparison of different QKD methods proposed for SATCOM applications.

Ref.	Link	Protocol	Main contribution	Assessment
[172]	SG, SS	BB84	Free space QKD	Experiments
[173]	SG (GEO, LEO), SS	BB84/BB84 + Decoy/B92	Estimate Link Attenuation and SNR	Simulation
[174]	Generic	Entanglement-based	Efficiency and Security Analysis	Experiments
[175]	SG (LEO)	BB84	Feasibility of QKD	Experiments
[176]	SG (LEO)	Generic QKD	Radiation Tolerance estimation of single photon detector	Simulation
[177]	SG (LEO)	BB84 + Decoy	Efficiency of QKD in high-loss regime scenarios	Experiments
[178]	SG (LEO)	BB84 + Decoy	QKD with Quantum Repeaters	Experiments
[179]	SG	B92	Communication Feasibility of QKD	Experiments
[180]	GS	B92	Prototype of free-space QKD	Experiments
[181]	SG	Custom QKD	Long Distance QKD	Experiments
[182]	SG (LEO)	Generic QKD	Quantum Error Correction Technique	Simulation
[183]	SG (LEO)	BB84 ± Decoy/Ekert91	Efficiency & Performance Analysis	Simulation
[184]	SG	Entanglement-based QKD	Miniaturized entangled photon sources	Experiential
[185]	SG (LEO)	Decoy-State QKD	Performances Analysis on High-loss	Experiments
[186]	SG (LEO), SS (LEO)	Custom QKD	Feasibility of satellite-based quantum communication in daylight	Experiments
[187]	GS (LEO)	BB84	Securing Key Exchange Sat to Ground	Experiments

4.4. Lessons learned

In the following, we summarize the most important lessons learned from the analysis of cryptography approaches for SATCOM reported in the previous subsections.

Software Modifications. Differently from approaches based on PHY-layer security, cryptography solutions always require the modification of the software running on the receivers and on the satellites. Some approaches actually provided the required modifications, while others assume that the advantages of such modifications overcome the cost and effort required to install them.

Impact of Software Updates in SATCOM. Cryptography-based solutions always require a dedicated software update on the satellite, and this could also affect the operational status of the SATCOM communication link. Thus, the cost of their integration should be carefully taken into account, and they should be applied only when other solutions (e.g., PLS-based ones) do not guarantee sufficient security.

Quantum Key Agreement for SATCOM. Due to its promising level of security, quantum computing strategies show appealing advantages for SATCOM links, and researchers have already started to evaluate its feasibility due to the large involved distances [188]. We expect to see many contributions to come on this topic in the following years.

4.5. Future directions

Analysis of Security Requirements. Most of the works considered in the first two subsections of this section only apply well-known cryptography schemes in SATCOM, plugging them in without a strong motivation or a detailed description of the underlying security requirements. Due to the significant impact that cryptography has on the operation and performance of SATCOM deployments, researchers and industry should come up with a dedicated security analysis of SATCOM links, explaining precisely what the threats are and why cryptography solutions are advantageous compared to Physical-layer ones in solving such issues. To the best of our knowledge, such a study is still not available in the literature.

Communication Channel Availability. In the presence of an eavesdropper, a quantum-based communication channel is disrupted, and the parties cannot continue to communicate. In principle, this capability could help to detect Man-In-The-Middle (MITM) attacks and identify potential eavesdroppers quickly. However, it also paves the way for easy Denial of Service (DoS) attacks, even harder to detect in the context of SATCOM due to the large reception range and coverage area of the communication. In this context, backup solutions for guaranteeing the availability of the service are needed, as well as tools to discriminate if the channel if compromised because of an eavesdropper, or because of the channel noise.

Quantum Channel Security Assessment Tools. At the time of this writing, no works are available that evaluate the physical-layer security of QKD signal generation tools. In principle, passive side-channel attacks can be conducted to extract meaningful information from a QKD channel, without affecting and compromising the robustness provided by QKD strategies. It is essential to explore this research area to provide methods and tools to mitigate this open issue [194].

5. Emerging research challenges

The previous sections delved into the most active research branches related to the SATCOM domain and provided some appealing future research directions in those specific contexts. However, in addition to the identified research areas, our investigation highlighted further security-related SATCOM-based application domains that are receiving

increasing attention from the scientific and business community. In the following, we discuss some of them, showing their key challenges and potential to attract additional interest in the years to come.

Cognitive Satellite Terrestrial Networks. Cognitive radio in the context of wireless communication systems is a research area that attracted lots of interest in the few last years. In a nutshell, cognitive radio systems allow the coexistence of primary users (using devices that own the license to use a specific frequency band) and secondary users (allowed to share resources with the primary network, but not in possession of the license) on the same network and spectrum, sharing the same radio resources. A few works applied the concept of cognitive radio networks in the context of SATCOM. For instance, the authors in [36,43,51,52] propose to secure the communication in cognitive satellite–terrestrial networks. They assume a scenario where the primary network is constituted by GEO, MEO, or LEO satellites, sending confidential messages to the fixed-satellite operator in the presence of eavesdroppers (secondary users) attempting to capture the satellite information signal. In their own (secondary) network, the network operator communicates with the user terminals. Still, doubts are there on the actual applicability of cognitive radio techniques in the context of satellite–terrestrial networks. This is mainly because of the extremely wide coverage of satellites, where the CR techniques might not work well. In line with a large amount of work done in the context of cognitive radio for terrestrial networks [195], we expect increased interest in this domain in the next years.

Drone-To-Satellite. Unmanned Aerial Vehicles (UAV), a.k.a. drones, have gained increased momentum in the last years, in both academia and Industry [196]. In the context of SATCOM, one of the most critical challenges consists of allowing secure communication between small/commercial UAVs and satellites. For instance, the authors in [197] proposed a physical layer security framework in space–air–ground (SAGIN) downlink multi-beam satellite-enabled vehicle communications, where the UAV is adopted as cooperative node, interacting with the legitimate user and acting as a source of artificial noise to mitigate eavesdropping. In the same network setup, the authors in [198] investigated the IoT computing offloading problem by proposing a reinforcement learning approach to allocate the resources of the UAV edge server efficiently. In the same domain, the authors in [199] proposed a software defined architecture supporting different vehicles in an efficient manner. In line with existing works such as [200], we forecast numerous appealing applications involving drones and satellites. Using satellites links, users can: (i) drive drones remotely; (ii) stream video from the drone's camera; (iii) use the drone to collect information from remote satellites; and, (iv) use the drone for optical remote sensing applications. Due to the well-known security, safety, and privacy issues posed by drones usage, and due to the central role of drones in the development of the upcoming 6G communication systems [201], we expect significant research activity in this domain in the years to come.

AI in SATCOM. The usage of AI-based techniques is gaining increasing importance in almost any application domain, cybersecurity included. In the context of SATCOM, AI techniques could be used for many purposes, e.g., to identify physical-layer characteristics of the signals emitted by the satellites, to discriminate between authentic and injected signals, and for intrusion detection, to name a few . In this context, the authors in [202] experimentally show that using a dedicated Convolutional Neural Network (CNN) it is possible to fingerprint the raw IQ samples received from LEO Satellites (Iridium) and authenticate the emitting transceiver on board of the satellite, despite the large distances. We expect increasing attention towards this research domain, targeting additional satellites constellations (GNSS ones included) or other applications of AI.

Software-defined satellites. The integration of Software Defined Networking (SDN) into SATCOM could improve the connectivity coverage and performance for using broadband communications by allowing the operators to reconfigure the satellites as needed [203–205]. However, SDN also come with their security issues, that are further specialized in SATCOM use-cases [206]. Additional research is needed in this context.

Network Slicing for the Internet of Space Things. The continuous development of nano-satellites is accelerating the deployment of low-cost satellite networks [207]. Emerging paradigms, such as the Internet of Space Things (IoST), require a network slicing framework to provide the support for the plethora of space-application scenarios. A network slice is a part of the network that is independent and logically separated from the rest. A specific slice has specific security policies, used to protect the slice while meeting specific system requirements. However, there are neither common strategies nor protocols suitable to design a network slice in the context of SATCOM. Despite initial studies in this context are available [208,209], major work is still to be done, and we expect increasing attention towards this topic.

Green Satellites. The design of environmentally-friendly satellites can help to reduce the environmental impact of a satellite, its production cost, and maintenance compared to traditional ones. However, reducing the cost and the impact of the satellite inevitably could affect the provided security services. This emerging research area, also suggested from the ESA [210], leads to a potential redesign of the existing procedures and technologies, also including the security domain. Definitively, a novel and interesting research topic.

Satellites Signals for Opportunistic Navigation. Specific satellites signals can be used to pinpoint a specific location on Earth, similar to the GPS. A group of researchers developed a working solution based on the cited logic, leveraging signals broadcasted by Starlink internet service satellites [211]. The usage of additional satellite constellations could provide reliability and spoofing detection mechanisms for devices on Earth, and more research into the robustness of such solutions is needed.

Cybersecurity for Commercial Satellite Operations. The National Institute of Standards and Technology (NIST) is seeking comments on the draft specification NISTIR 8270, which describes the security procedures and the concepts for commercial space operations. The draft considers the management aspects, risk management operations, and defines the requirements that "might coexist within space vehicle systems". The NIST is requiring feedback on the overall approach, the example use case, and the identified controls for the proposed use case [212]. We expect that several research contributions could come out due to the study and application of this (yet to come) recommendation to real use-cases.

Standardization of Security for Non-Terrestrial Networks. In the standardization community, and in particular, within the Third Generation Partnership Project (3GPP) committee, satellite communications are specifically considered in the design of the Non-Terrestrial Networks (NTNs), anticipating the upcoming tight integration between terrestrial, aerial and satellite networks [213]. Specifically, the standardization of Non-Terrestrial Networks (NTNs) has been launched by 3GPP in the 3GPP Release 16 [214]. At the same time, new security aspects have been recently defined by the 3GPP in the Release 17 [215], and new amendments are planned in the upcoming Release 18 [216].

In this context, none specifications edited by the 3GPP specifically took into account network security issues for NTNs. As a result, the current approach recommended by the 3GPP consists of a straightforward integration of the 5G security architecture and protocols into NTNs. Such an integration, however, comes with several challenges, in terms of communication overhead, software updates, and unreliability of the wireless links. Specifically, security issues in the operation of NTNs have been investigated by the Working Group on Satellite 5G, established within the IEEE Future Networks Initiative [217]. In one of the latest deliverables of the WG, i.e., [218], they drew a roadmap of the priorities to be addressed in this regard, highlighting that new security mechanisms might be needed for specific deployments, and that the emphasis should be put on the isolation of the end-users from the

shared NTN network. The WG realized several security-related activities, i.e.,: (i) analyzed the state of the art about security for NTNs; (ii) provided a threat analysis for the NTN scenario; (iii) identified specific complications derived from using of 5G security solutions on 5G-NTN networks, by experimentally verifying them on prototyping platforms; and, finally, (iv) identified additional security concerns, mainly related to the integration of emerging technologies such as network slicing, edge computing, and multicasting over satellite networks (see Section 2.6.2 of [217]. The temporary recommendation proposed by the WP was to adopt the IPSec protocol suite to secure the communication link, but they also recommended further study into the issues at the 3GPP standardization level. However, the 3GPP refused to investigate further into the issue, at the time of this writing, still recommending a straightforward integration of 5G security into the NTN domain [218].

Nonetheless, due to the forecasted performance issues arising from such the integration of 5G-security into NTNs, we expect significant contributions by the research community in the years to come, potentially triggering dedicated and ad-hoc initiatives by the 3GPP.

Security and Privacy for 6G. 6G networks will accommodate satellites, UAVs, and undersea communications [219]. It is crucial that any security proposal framed in this context protect the communications while guaranteeing reliability, low latency, and secure and efficient transmission services. Physical-layer security is the first candidate defense for these new emerging technologies, but emerging cryptography-based solutions could also play a role if their integration is carefully systematized and orchestrated with the existing services. In the context of 6G initiatives, the 3GPP claimed that for the next few years (2030s) additional research is needed into this application area. Adapting and integrating the security services on satellites with mobile terrestrial/sea systems while meeting the requirements of 6G communication services will indeed represent a complex and difficult challenge [220]. For the cited scenario, we expect the adoption of real-time security communication protocols and emerging architectural solutions, such as Zero Trust [221].

6. Conclusion

In this contribution, we have provided a survey of the most significant link-layer security issues, threats, and mitigation techniques adopted in the context of Satellite-based Communications systems. First, we presented general background on the SATCOM architecture, the most important constellations, and network parameters. Then, we divided the relevant literature on the topic into two major research areas, i.e., physical-layer security and cryptography, and we further identified dedicated topics in each macro-area, focusing on specific threats. For the physical-layer area, we discussed and cross-compared solutions based on the usage of information-theoretic security schemes, anti-jamming strategies, and anti-spoofing schemes. For the cryptography area, we specifically discussed approaches for authentication, key agreement, and key distribution based on the emerging quantum computing paradigm. We also identified lessons learned and specific future directions for each of the cited threats and research areas. Finally, we presented a few appealing emerging challenges in the SATCOM security domain, pointing out the main research challenges to be solved and the areas where new contributions from the scientific community might have major impact.

Overall, we believe that the exposed research challenges highlight that the design and testing of cybersecurity strategies for SATCOMs is still an active research domain. In particular, our contribution calls for collaboration between Industry and Academia to unlock new business opportunities and services, while enjoying the needed level of security for communications, applications, and infrastructures.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

The authors would like to thank the anonymous reviewers, that helped improving the quality of the paper.

This publication was partially supported by the Technology Innovation Institute, Abu Dhabi - UAE, and awards NPRP-S-11-0109-180242 from the QNRF-Qatar National Research Fund, a member of The Qatar Foundation, and NATO Science for Peace and Security Programme - MYP G5828 project "SeaSec: DronNets for Maritime Border and Port Security". This work has been partially supported also by the INTERSECT project, Grant No. NWA.1162.18.301, funded by Netherlands Organisation for Scientific Research (NWO). The findings reported herein are solely responsibility of the authors.

References

[1] G. Maral, M. Bousquet, Z. Sun, Satellite Communications Systems: Systems, Techniques and Technology, John Wiley & Sons, 2020.
[2] Space.com, Starlink: SpaceX's satellite internet project, 2021, (Accessed: 2022-Jul-10). URLStarlink: SpaceX's satellite internet project.
[3] J. Porter, Facebook's satellite internet team joins Amazon, 2021, (Accessed: 2022-Jul-10). URL https://www.theverge.com/2021/7/14/22576788/amazon-acquires-facebook-satellite-team-project-kuiper.
[4] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, C.-X. Wang, 5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks, IEEE Internet Things J. 8 (18) (2021) 14399–14417.
[5] T.S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, G.C. Trichopoulos, Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond, IEEE Access 7 (2019) 78729–78757.
[6] R. Santamarta, SATCOM terminals: Hacking by air, sea, and land, Blackhat USA (2014).
[7] J. Trevithick, U.S. satellites are being attacked every day according to space force general, 2021, (Accessed: 2022-Jul-10). URL https://www.thedrive.com/the-war-zone/43328/u-s-satellites-are-being-attacked-everyday-according-to-space-force-general.
[8] M. Manulis, C. Bridges, R. Harrison, V. Sekar, A. Davis, Cyber security in new space: Analysis of threats, key enabling technologies and challenges, Int. J. Inf. Secur. (2020) 1–25.
[9] O. Kodheli, E. Lagunas, N. Maturo, S.K. Sharma, B. Shankar, J.F.M. Montoya, J.C.M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T.X. Vu, G. Goussetis, Satellite communications in the new space era: A survey and future challenges, IEEE Commun. Surv. Tutor. 23 (1) (2021) 70–109.
[10] B. Li, Z. Fei, C. Zhou, Y. Zhang, Physical-layer security in space information networks: A survey, IEEE Internet Things J. 7 (1) (2020) 33–52.
[11] J. Zidan, E. Adegoke, E. Kampert, S.A. Birrell, C.R. Ford, M.D. Higgins, GNSS vulnerabilities and existing solutions: A review of the literature, IEEE Access (2020).
[12] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente, E.S. Lohan, A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft, IEEE Commun. Surv. Tutor. 22 (1) (2019) 249–291.
[13] M. Rath, S. Mishra, Security approaches in machine learning for satellite communication, in: Machine Learning and Data Mining in Aerospace Technology, Springer, 2020, pp. 189–204.
[14] L. Junzhi, L. Wanqing, F. Qixiang, L. Beidian, Research progress of GNSS spoofing and spoofing detection technology, in: 2019 IEEE 19th International Conference on Communication Technology (ICCT), IEEE, 2019, pp. 1360–1369.
[15] D. Margaria, B. Motella, M. Anghileri, J. Floch, I. Fernandez-Hernandez, M. Paonni, Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives, IEEE Signal Process. Mag. 34 (5) (2017) 27–37.
[16] T. Saroj, G.S. Gaba, S.K. Arora, A survey on authentication schemes for satellite communications, Int. J. Control Theory Appl. (2016).
[17] R. Radhakrishnan, W.W. Edmonson, F. Afghah, R.M. Rodriguez-Osorio, F. Pinto, S.C. Burleigh, Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view, IEEE Commun. Surv. Tutor. 18 (4) (2016) 2442–2473.
[18] D. Schmidt, K. Radke, S. Camtepe, E. Foo, M. Ren, A survey and analysis of the GNSS spoofing threat and countermeasures, ACM Comput. Surv. 48 (4) (2016) 1–31.
[19] N. Hosseinidehaj, Z. Babar, R. Malaney, S.X. Ng, L. Hanzo, Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook, IEEE Commun. Surv. Tutor. 21 (1) (2018) 881–919.

[20] H. Guo, J. Li, J. Liu, N. Tian, N. Kato, A survey on space-air-ground-sea integrated network security in 6G, IEEE Commun. Surv. Tutor. 24 (1) (2022) 53–87.

[21] Y. Xu, J. Liu, Y. Shen, X. Jiang, Y. Ji, N. Shiratori, QoS-aware secure routing design for wireless networks with selfish jammers, IEEE Trans. Wireless Commun. 20 (8) (2021) 4902–4916.

[22] Y. Xu, J. Liu, Y. Shen, J. Liu, X. Jiang, T. Taleb, Incentive jamming-based secure routing in decentralized internet of things, IEEE Internet Things J. 8 (4) (2021) 3000–3013.

[23] A.K. Maini, V. Agrawal, Satellite orbits and trajectories, in: Satellite Technology: Principles and Applications, John Wiley & Sons, 2014, pp. 37–78.

[24] B.R. Elbert, The Satellite Communication Applications Handbook (Artech House Space Applications Series), Artech House, Inc., USA, 2003.

[25] S. Cakaj, The parameters comparison of the" starlink" LEO satellites constellation for different orbital shells, Front. Commun. Netw. 2 (2021) 7.

[26] K.M. Peterson, Satellite communications, in: R.A. Meyers (Ed.), Encyclopedia of Physical Science and Technology (Third Edition), third ed., Academic Press, New York, 2003, pp. 413–438.

[27] ESA, Satellite frequency bands, 2021, (Accessed: 2022-Jul-10). URL https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellite_frequency_bands.

[28] S.D. Ilčev, Inmarsat GEO GMSC system, in: Global Mobile Satellite Communications Applications: For Maritime, Land and Aeronautical Applications Volume 2, Springer International Publishing, Cham, 2018, pp. 1–100.

[29] J. Foust, SpaceX's space-internet woes: Despite technical glitches, the company plans to launch the first of nearly 12,000 satellites in 2019, IEEE Spectr. 56 (1) (2019) 50–51.

[30] M. Caprolu, R.D. Pietro, S. Raponi, S. Sciancalepore, P. Tedeschi, Vessels cybersecurity: Issues, challenges, and the road ahead, IEEE Commun. Mag. 58 (6) (2020) 90–96.

[31] G. Oligeri, S. Sciancalepore, R. Di Pietro, GNSS spoofing detection via opportunistic IRIDIUM signals, in: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, in: WiSec '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 42–52.

[32] Y. Abe, H. Tsuji, A. Miura, S. Adachi, Frequency resource management based on model predictive control for satellite communications system, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E101.A (12) (2018) 2434–2445.

[33] X. Lin, S. Rommer, S. Euler, E.A. Yavuz, R.S. Karlsson, 5G from space: An overview of 3GPP non-terrestrial networks, IEEE Commun. Stand. Mag. 5 (4) (2021) 147–153.

[34] S. Tanase, Satellite turla: APT command and control in the sky, 2015, (Accessed: 2022-Jul-10). URL https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

[35] A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1550–1573.

[36] K. An, M. Lin, J. Ouyang, W. Zhu, Secure transmission in cognitive satellite terrestrial networks, IEEE J. Sel. Areas Commun. 34 (11) (2016) 3025–3037.

[37] J. Lei, Z. Han, M.A. Vazquez-Castro, A. Hjorungnes, Secure satellite communication systems design with individual secrecy rate constraints, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 661–671.

[38] G. Zheng, P. Arapoglou, B. Ottersten, Physical layer security in multibeam satellite systems, IEEE Trans. Wireless Commun. 11 (2) (2012) 852–863.

[39] R. Xu, X. Da, H. Hu, L. Ni, Y. Pan, Self-interference cancellation scheme for secure AF satellite communication based on FH-MWFRFT, IEEE Commun. Lett. 23 (11) (2019) 2050–2053.

[40] Z. Luo, H. Wang, K. Zhou, Polarization filtering based physical-layer secure transmission scheme for dual-polarized satellite communication, IEEE Access 5 (2017) 24706–24715.

[41] W. Lu, K. An, T. Liang, Robust beamforming design for sum secrecy rate maximization in multibeam satellite systems, IEEE Trans. Aerosp. Electron. Syst. 55 (3) (2019) 1568–1572.

[42] R. Xu, X. Da, Y. Liang, L. Ni, H. Hu, Secure transmission in AF satellite system based on FH-MWFRFT and null space beamforming, IET Commun. 13 (10) (2019) 1506–1513.

[43] M. Lin, Z. Lin, W. Zhu, J. Wang, Joint beamforming for secure communication in cognitive satellite terrestrial networks, IEEE J. Sel. Areas Commun. 36 (5) (2018) 1017–1029.

[44] X. Zhang, B. Zhang, D. Guo, Physical layer secure transmission based on fast dual polarization hopping in fixed satellite communication, IEEE Access 5 (2017) 11782–11790.

[45] Z. Lin, M. Lin, J. Wang, Y. Huang, W. Zhu, Robust secure beamforming for 5G cellular networks coexisting with satellite networks, IEEE J. Sel. Areas Commun. 36 (4) (2018) 932–945.

[46] A. Kalantari, G. Zheng, Z. Gao, Z. Han, B. Ottersten, Secrecy analysis on network coding in bidirectional multibeam satellite communications, IEEE Trans. Inf. Forensics Secur. 10 (9) (2015) 1862–1874.

[47] Q. Huang, M. Lin, K. An, J. Ouyang, W. Zhu, Secrecy performance of hybrid satellite-terrestrial relay networks in the presence of multiple eavesdroppers, IET Commun. 12 (1) (2017) 26–34.

[48] Y. Yan, B. Zhang, D. Guo, S. Li, H. Niu, X. Wang, Joint beamforming and jamming design for secure cooperative hybrid satellite-terrestrial relay network, in: 2016 25th Wireless and Optical Communication Conference (WOCC), 2016, pp. 1–5.

[49] J. Liu, J. Wang, W. Liu, Q. Wang, M. Wang, A novel cooperative physical layer security scheme for satellite downlinks, Chin. J. Electron. 27 (4) (2018) 860–865.

[50] K. An, M. Lin, T. Liang, J. Ouyang, C. Yuan, W. Lu, Secrecy performance analysis of land mobile satellite communication systems over Shadowed-Rician fading channels, in: 2016 25th Wireless and Optical Communication Conference (WOCC), 2016, pp. 1–4.

[51] B. Li, Z. Fei, X. Xu, Z. Chu, Resource allocations for secure cognitive satellite-terrestrial networks, IEEE Wirel. Commun. Lett. 7 (1) (2018) 78–81.

[52] B. Li, Z. Fei, Z. Chu, F. Zhou, K. Wong, P. Xiao, Robust chance-constrained secure transmission for cognitive satellite–terrestrial networks, IEEE Trans. Veh. Technol. 67 (5) (2018) 4208–4219.

[53] K. Guo, K. An, Y. Huang, B. Zhang, Physical layer security of multiuser satellite communication systems with channel estimation error and multiple eavesdroppers, IEEE Access 7 (2019) 96253–96262.

[54] R. Xu, X. Da, H. Hu, L. Ni, Y. Pan, A secure hybrid satellite-terrestrial communication network with AF/DF and relay selection, IEEE Access 7 (2019) 171980–171994.

[55] M.G. Schraml, R.T. Schwarz, A. Knopp, Multiuser MIMO concept for physical layer security in multibeam satellite systems, IEEE Trans. Inf. Forensics Secur. 16 (2021) 1670–1680.

[56] G. Aliberti, R.D. Pietro, S. Guarino, Reliable and perfectly secret communication over the generalized Ozarow-Wyner's wire-tap channel, Comput. Netw. 109 (2016) 21–30, Special issue on Recent Advances in Physical-Layer Security.

[57] J. Barros, M.R. Rodrigues, Secrecy capacity of wireless channels, in: 2006 IEEE International Symposium on Information Theory, IEEE, 2006, pp. 356–360.

[58] P. Tedeschi, S. Sciancalepore, R. Di Pietro, Security in energy harvesting networks: A survey of current solutions and research challenges, IEEE Commun. Surv. Tutor. 22 (4) (2020) 2658–2693.

[59] S. Sciancalepore, G. Oligeri, R.D. Pietro, Shooting to the stars: Secure location verification via meteor burst communications, in: 2018 IEEE Conference on Communications and Network Security (CNS), 2018, pp. 1–9.

[60] Z. Wu, Y. Zhang, Y. Yang, C. Liang, R. Liu, Spoofing and anti-spoofing technologies of global navigation satellite system: A survey, IEEE Access 8 (2020) 165444–165496.

[61] Osqzss, GPS-SDR-SIM, 2021, (Accessed: 2022-Jul-10). URL https://github.com/osqzss/gps-sdr-sim.

[62] G. Oligeri, S. Sciancalepore, O. Ibrahim, et al., Drive me not: GPS spoofing detection via cellular network: (Architectures, models, and experiments), in: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, in: WiSec '19, 2019, pp. 12–22.

[63] T.E. Humphreys, Detection strategy for cryptographic GNSS anti-spoofing, IEEE Trans. Aerosp. Electron. Syst. 49 (2) (2013) 1073–1090.

[64] M. Psiaki, S. Powell, B. O'hanlon, GNSS spoofing detection using high-frequency antenna motion and carrier-phase data, in: Proceedings of the ION GNSS+ Meeting, 2013, pp. 2949–2991.

[65] D. Borio, PANOVA tests and their application to GNSS spoofing detection, IEEE Trans. Aerosp. Electron. Syst. 49 (1) (2013) 381–394.

[66] K.D. Wesson, B.L. Evans, T.E. Humphreys, A combined symmetric difference and power monitoring GNSS anti-spoofing technique, in: 2013 IEEE Global Conference on Signal and Information Processing, 2013, pp. 217–220.

[67] L. Heng, D.B. Work, G.X. Gao, GPS signal authentication from cooperative peers, IEEE Trans. Intell. Transp. Syst. 16 (4) (2014) 1794–1805.

[68] D.-Y. Yu, A. Ranganathan, T. Locher, S. Capkun, D. Basin, Short paper: Detection of GPS spoofing attacks in power grids, in: Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks, 2014, pp. 99–104.

[69] L. Heng, D.B. Work, G. Gao, Cooperative GNSS authentication, in: Reliability from Unreliable Peers. Inside GNSS, Vol. 8, 2013, pp. 70–75.

[70] M.L. Psiaki, B.W. O'hanlon, S.P. Powell, J.A. Bhatti, K.D. Wesson, T.E. Humphreys, GNSS spoofing detection using two-antenna differential carrier phase, in: Radionavigation Laboratory Conference Proceedings, 2014.

[71] N. Stenberg, E. Axell, J. Rantakokko, G. Hendeby, GNSS spoofing mitigation using multiple receivers, in: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), IEEE, 2020, pp. 555–565.

[72] B.W. O'Hanlon, M.L. Psiaki, J.A. Bhatti, D.P. Shepard, T.E. Humphreys, Real-time GPS spoofing detection via correlation of encrypted signals, Navigation 60 (4) (2013) 267–278.

[73] Y. Hu, S. Bian, K. Cao, B. Ji, GNSS spoofing detection based on new signal quality assessment model, GPS Solut. 22 (1) (2018) 1–13.

[74] S. Bhamidipati, T.Y. Mina, G.X. Gao, GPS time authentication against spoofing via a network of receivers for power systems, in: 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), IEEE, 2018, pp. 1485–1491.

[75] T.Y. Mina, S. Bhamidipati, G.X. Gao, Detecting GPS spoofing via a multi-receiver hybrid communication network for power grid timing verification, in: Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Hyatt Regency Miami, FL, USA, 2018, pp. 24–28.
[76] Y. Hu, S. Bian, B. Ji, J. Li, GNSS spoofing detection technique using fraction parts of double-difference carrier phases, J. Navig. 71 (5) (2018) 1111–1129.
[77] F. Formaggio, S. Tomasin, G. Caparra, S. Ceccato, N. Laurenti, Authentication of galileo GNSS signal by superimposed signature with artificial noise, in: 2018 26th European Signal Processing Conference (EUSIPCO), IEEE, 2018, pp. 2573–2577.
[78] F. Formaggio, S. Tomasin, Authentication of satellite navigation signals by wiretap coding and artificial noise, EURASIP J. Wireless Commun. Networking 2019 (1) (2019) 1–17.
[79] E. Schmidt, N. Gatsis, D. Akopian, A GPS spoofing detection and classification correlator-based technique using the LASSO, IEEE Trans. Aerosp. Electron. Syst. (2020).
[80] J.M. Anderson, K.L. Carroll, N.P. DeVilbiss, J.T. Gillis, J.C. Hinks, B.W. O'Hanlon, J.J. Rushanan, L. Scott, R.A. Yazdi, Chips-message robust authentication (Chimera) for GPS civilian signals, in: Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2017), 2017, pp. 2388–2416.
[81] S. Tohidi, M.R. Mosavi, Effective detection of GNSS spoofing attack using a multi-layer perceptron neural network classifier trained by PSO, in: 2020 25th International Computer Conference, Computer Society of Iran (CSICC), IEEE, 2020, pp. 1–5.
[82] J.N. Gross, C. Kilic, T.E. Humphreys, Maximum-likelihood power-distortion monitoring for GNSS-signal authentication, IEEE Trans. Aerosp. Electron. Syst. 55 (1) (2018) 469–475.
[83] F. Wang, H. Li, M. Lu, GNSS spoofing detection and mitigation based on maximum likelihood estimation, Sensors 17 (7) (2017) 1532.
[84] K.D. Wesson, J.N. Gross, T.E. Humphreys, B.L. Evans, GNSS signal authentication via power and distortion monitoring, IEEE Trans. Aerosp. Electron. Syst. 54 (2) (2017) 739–754.
[85] Y. Jiang, Y. Xing, Satellite spoofing identification method based on radio frequency feature extraction, JPhCS 1069 (1) (2018) 012079.
[86] Q. Zou, S. Huang, F. Lin, M. Cong, Detection of GPS spoofing based on UAV model estimation, in: IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2016, pp. 6097–6102.
[87] E. Axell, E.G. Larsson, D. Persson, GNSS spoofing detection using multiple mobile COTS receivers, in: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2015, pp. 3192–3196.
[88] G. Caparra, C. Wullems, R.T. Ioannides, An autonomous GNSS anti-spoofing technique, in: 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), IEEE, 2016, pp. 1–8.
[89] S. Singh, J. Singh, S. Singh, Mitigating spoofed GNSS trajectories through nature inspired algorithm, GeoInformatica (2020) 1–20.
[90] S. Semanjski, I. Semanjski, W. De Wilde, S. Gautama, GNSS spoofing detection by supervised machine learning with validation on real-world meaconing and spoofing data—Part II, Sensors 20 (7) (2020) 1806.
[91] G. Falco, M. Nicola, E. Falletti, M. Pini, An algorithm for finding the direction of arrival of counterfeit GNSS signals on a civil aircraft, in: Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2019), 2019, pp. 3185–3196.
[92] S. Vadlamani, B. Eksioglu, H. Medal, A. Nandi, Jamming attacks on wireless networks: A taxonomic survey, Int. J. Prod. Econ. 172 (2016) 76–94.
[93] L. Zhang, J. Ren, T. Li, Time-varying jamming modeling and classification, IEEE Trans. Signal Process. 60 (7) (2012) 3902–3907.
[94] T. Wang, X. Wei, J. Fan, T. Liang, Adaptive jammer localization in wireless networks, Comput. Netw. 141 (2018) 17–30.
[95] T. Morehouse, C. Montes, M. Bisbano, J.F. Lin, M. Shao, R. Zhou, Incremental learning-based jammer classification, in: Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III, Vol. 11746, International Society for Optics and Photonics, 2021, p. 117462E.
[96] D. Borio, Swept GNSS jamming mitigation through pulse blanking, in: 2016 European Navigation Conference (ENC), 2016, pp. 1–8.
[97] O.A. Topal, S. Gecgel, E.M. Eksioglu, G. Karabulut Kurt, Identification of smart jammers: Learning-based approaches using wavelet preprocessing, Phys. Commun. 39 (2020) 101029.
[98] A.G. Dempster, E. Cetin, Interference localization for satellite navigation systems, Proc. IEEE 104 (6) (2016) 1318–1326.
[99] D. Borio, F. Dovis, H. Kuusniemi, L. Lo Presti, Impact and detection of GNSS jammers on consumer grade satellite navigation receivers, Proc. IEEE 104 (6) (2016) 1233–1245.
[100] H. Jung, K. Kim, J. Kang, T.S. Lee, S. Kim, An iALM-ICA-based antijamming DS-CDMA receiver for LMS systems, IEEE Trans. Aerosp. Electron. Syst. 54 (5) (2018) 2318–2328, http://dx.doi.org/10.1109/TAES.2018.2814319.
[101] M. Tamazin, A. Noureldin, Robust GPS anti-jamming technique based on fast orthogonal search, in: Recent Advances in Engineering Mathematics and Physics, Springer, 2020, pp. 233–244.
[102] M. Bažec, B. Luin, F. Dimc, GPS jamming detection with SDR, in: Proc. of the 24th International Symposium on Electronics in Transport (ISEP 2016), ITS for Efficient Energy Use, Electrotechnical Association of Slovenia, Ljubljana, Slovenia, Mar, 2016, pp. 1–4.
[103] A. Purwar, D. Joshi, V.K. Chaubey, GPS signal jamming and anti-jamming strategy—A theoretical analysis, in: 2016 IEEE Annual India Conference (INDICON), IEEE, 2016, pp. 1–6.
[104] P. Gao, S. Sun, Z. Zeng, C. Wang, GNSS spoofing jamming recognition based on machine learning, in: International Conference on Signal and Information Processing, Networking and Computers, Springer, 2017, pp. 221–228.
[105] O. Glomsvoll, L.K. Bonenberg, GNSS jamming resilience for close to shore navigation in the Northern Sea, J. Navig. 70 (1) (2017) 33–48.
[106] G.X. Gao, M. Sgammini, M. Lu, N. Kubo, Protecting GNSS receivers from jamming and interference, Proc. IEEE 104 (6) (2016) 1327–1338.
[107] M. Lichtman, J. Reed, Analysis of reactive jamming against satellite communications, Int. J. Satell. Commun. Netw. 34 (2) (2016) 195–210.
[108] D. Borio, C. Gioia, Real-time jamming detection using the sum-of-squares paradigm, in: 2015 International Conference on Localization and GNSS (ICL-GNSS), 2015, pp. 1–6.
[109] Y. Shi, Y.E. Sagduyu, Spectrum learning and access for cognitive satellite communications under jamming, in: 2016 IEEE Conference on Communications and Network Security (CNS), 2016, pp. 472–479.
[110] D. Borio, Swept GNSS jamming mitigation through pulse blanking, in: 2016 European Navigation Conference (ENC), 2016, pp. 1–8.
[111] Q. Wang, T. Nguyen, K. Pham, H. Kwon, Satellite jamming: A game theoretic analysis, in: MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), 2017, pp. 141–146.
[112] R. Lang, H. Xiao, Z. Li, L. Yu, A anti-jamming method for satellite navigation system based on multi-objective optimization technique, PLoS One 12 (7) (2017).
[113] Z. Wu, Y. Zhao, Z. Yin, H. Luo, Jamming signals classification using convolutional neural network, in: 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2017, pp. 62–67.
[114] L. Sun, B. Jing, Y. Cheng, L. Yuan, Jamming monitoring and anti-jamming by polarization diversity reception in the satellite navigation system, in: 2015 8th International Congress on Image and Signal Processing (CISP), 2015, pp. 1303–1307.
[115] H. Wang, L. Yang, Y. Yang, H. Zhang, Anti-jamming of beidou navigation based on polarization sensitive array, in: 2017 International Applied Computational Electromagnetics Society Symposium (ACES), 2017, pp. 1–2.
[116] K. Dong, Z. Zhang, X. Xu, A hybrid interference suppression scheme for global navigation satellite systems, in: 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), 2017, pp. 1–7.
[117] P. Wang, Y. Wang, E. Cetin, A.G. Dempster, S. Wu, GNSS jamming mitigation using adaptive-partitioned subspace projection technique, IEEE Trans. Aerosp. Electron. Syst. 55 (1) (2019) 343–355.
[118] M. Hannon, S. Feng, H. Kwon, K. Pham, Jamming statistics-dependent frequency hopping, in: MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 138–143.
[119] S.P. Winter, C.A. Hofmann, A. Knopp, Antenna diversity techniques for enhanced jamming resistance in multi-beam satellites, in: MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 618–623.
[120] B. Lubbers, S. Mildner, P. Oonincx, A. Scheele, A study on the accuracy of GPS positioning during jamming, in: 2015 International Association of Institutes of Navigation World Congress (IAIN), 2015, pp. 1–6.
[121] Y. Chien, P. Chen, S. Fang, Novel anti-jamming algorithm for GNSS receivers using wavelet-packet-transform-based adaptive predictors, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 100 (2) (2017) 602–610.
[122] C. Hurley, R. Rogers, F. Thornton, D. Connelly, B. Baker, Chapter 2 - Understanding antennas and antenna theory, in: C. Hurley, R. Rogers, F. Thornton, D. Connelly, B. Baker (Eds.), WarDriving and Wireless Penetration Testing, Syngress, Rockland, 2007, pp. 31–61.
[123] ESA, ViaSat - Intersatellite communications, 2021, (Accessed: 2022-Jul-10). URL https://www.viasat.com/space-innovation/space-systems/intersatellite-communications/.
[124] S. Gong, X. Lu, D.T. Hoang, D. Niyato, L. Shu, D.I. Kim, Y.-C. Liang, Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey, IEEE Commun. Surv. Tutor. 22 (4) (2020) 2283–2314.
[125] A. Almohamad, A.M. Tahir, A. Al-Kababji, H.M. Furqan, T. Khattab, M.O. Hasna, H. Arslan, Smart and secure wireless communications via reflecting intelligent surfaces: A short survey, IEEE Open J. Commun. Soc. 1 (2020) 1442–1456.
[126] H. Dong, C. Hua, L. Liu, W. Xu, Towards integrated terrestrial-satellite network via intelligent reflecting surface, in: ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1–6, http://dx.doi.org/10.1109/ICC42927.2021.9500640.
[127] S. Xu, J. Liu, Y. Cao, J. Li, Y. Zhang, Intelligent reflecting surface enabled secure cooperative transmission for satellite-terrestrial integrated networks, IEEE Trans. Veh. Technol. 70 (2) (2021) 2007–2011.

[128] K. Tekbıyık, G.K. Kurt, A.R. Ekti, A. Görçin, H. Yanikomeroglu, Reconfigurable intelligent surfaces empowered THz communication in LEO satellite networks, 2020, arXiv preprint arXiv:2007.04281.
[129] A. Siemuri, H. Kuusniemi, M.S. Elmusrati, P. Välisuo, A. Shamsuzzoha, Machine learning utilization in GNSS—Use cases, challenges and future applications, in: 2021 International Conference on Localization and GNSS (ICL-GNSS), 2021, pp. 1–6, http://dx.doi.org/10.1109/ICL-GNSS51451.2021.9452295.
[130] R. Calvo-Palomino, A. Bhattacharya, G. Bovet, D. Giustiniano, Short: LSTM-based GNSS spoofing detection using low-cost spectrum sensors, in: 2020 IEEE 21st International Symposium on "a World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2020, pp. 273–276, http://dx.doi.org/10.1109/WoWMoM49955.2020.00055.
[131] S. Semanjski, A. Muls, I. Semanjski, W. De Wilde, Use and validation of supervised machine learning approach for detection of GNSS signal spoofing, in: 2019 International Conference on Localization and GNSS (ICL-GNSS), 2019, pp. 1–6, http://dx.doi.org/10.1109/ICL-GNSS.2019.8752775.
[132] S. Semanjski, I. Semanjski, W. De Wilde, A. Muls, Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part I, Sensors 20 (4) (2020) 1171.
[133] M.H. Ibrahim, S. Kumari, A.K. Das, V. Odelu, Jamming resistant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks, Secur. Commun. Netw. 9 (18) (2016) 5563–5580.
[134] C.L. Chen, K.W. Cheng, Y.L. Chen, C. Chang, C.C. Lee, An improvement on the self-verification authentication mechanism for a mobile satellite communication system, Appl. Math. Inf. Sci. 8 (1L) (2014) 97–106.
[135] W. Xinghua, Z. Aixin, L. Jianhua, Z. Weiwei, L. Yuchen, A lightweight authentication and key agreement scheme for mobile satellite communication systems, in: Information Security and Cryptology, Springer International Publishing, Cham, 2017, pp. 187–204.
[136] S. Xu, X. Liu, M. Ma, J. Chen, An improved mutual authentication protocol based on perfect forward secrecy for satellite communications, Int. J. Satell. Commun. Netw. 38 (1) (2020) 62–73.
[137] Y. Zhang, J. Chen, B. Huang, An improved authentication scheme for mobile satellite communication systems, Int. J. Satell. Commun. Netw. 33 (2) (2015) 135–146.
[138] H. Lin, Efficient dynamic authentication for mobile satellite communication systems without verification table, Int. J. Satell. Commun. Netw. 34 (1) (2016) 3–10.
[139] W. Zhao, A. Zhang, J. Li, X. Wu, Y. Liu, Analysis and design of an authentication protocol for space information network, in: MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 43–48.
[140] Y. Liu, A. Zhang, S. Li, J. Tang, J. Li, A lightweight authentication scheme based on self-updating strategy for space information network, Int. J. Satell. Commun. Netw. 35 (3) (2017) 231–248.
[141] G. Caparra, S. Sturaro, N. Laurenti, C. Wullems, Evaluating the security of one-way key chains in TESLA-based GNSS navigation message authentication schemes, in: 2016 International Conference on Localization and GNSS (ICL-GNSS), 2016, pp. 1–6.
[142] G. Caparra, S. Sturaro, N. Laurenti, C. Wullems, R.T. Ioannides, A novel navigation message authentication scheme for GNSS open service, in: ION GNSS, Vol. 2016, 2016.
[143] I.F. Hernández, V. Rijmen, G.S. Granados, J. Simón, I. Rodríguez, J.D. Calle, Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service, in: Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2014), 2014, pp. 2810–2827.
[144] A.J. Kerns, K.D. Wesson, T.E. Humphreys, A blueprint for civil GPS navigation message authentication, in: 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014, IEEE, 2014, pp. 262–269.
[145] C. Huang, Z. Zhang, M. Li, L. Zhu, Z. Zhu, X. Yang, A mutual authentication and key update protocol in satellite communication network, Automatika 61 (3) (2020) 334–344.
[146] A.D. Jurcut, J. Chen, A. Kalla, M. Liyanage, J. Murphy, A novel authentication mechanism for mobile satellite communication systems, in: 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW), IEEE, 2019, pp. 1–7.
[147] K. Ghorbani, N. Orouji, M. Mosavi, Navigation message authentication based on one-way hash chain to mitigate spoofing attacks for GPS L1, Wirel. Pers. Commun. 113 (4) (2020) 1743–1754.
[148] J.T. Curran, M. Paonni, J. Bishop, Securing the open-service: A candidate navigation message authentication scheme for galileo E1 OS, in: European Navigation Conference,(ENC-GNSS), 2014.
[149] W. Meng, K. Xue, J. Xu, J. Hong, N. Yu, Low-latency authentication against satellite compromising for space information network, in: 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2018, pp. 237–244.
[150] A. Perrig, R. Canetti, J.D. Tygar, D. Song, The TESLA broadcast authentication protocol, Rsa Cryptobytes 5 (2) (2002) 2–13.
[151] B. Blanchet, Automatic verification of correspondences for security protocols, J. Comput. Secur. 17 (4) (2009) 363–434.
[152] B. Blanchet, CryptoVerif: A Computationally-Sound Security Protocol Verifier, Tech. Rep., 2017.
[153] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P.H. Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron, The AVISPA tool for the automated validation of internet security protocols and applications, in: K. Etessami, S.K. Rajamani (Eds.), Computer Aided Verification, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 281–285.
[154] S. Meier, B. Schmidt, C. Cremers, D. Basin, The TAMARIN prover for the symbolic analysis of security protocols, in: N. Sharygina, H. Veith (Eds.), Computer Aided Verification, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 696–701.
[155] W. Stallings, L. Brown, M.D. Bauer, A.K. Bhattacharjee, Computer Security: Principles and Practice, Pearson Education, Upper Saddle River, NJ, USA, 2012.
[156] A. Ostad-Sharif, D. Abbasinezhad-Mood, M. Nikooghadam, Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications, Comput. Commun. 147 (2019) 85–97.
[157] A. Murtaza, T. Xu, S. Jahanzeb, H. Pirzada, L. Jianwei, A lightweight authentication and key sharing protocol for satellite communication, Int. J. Comput. Commun. Control (2019) (in press).
[158] G. Caparra, S. Ceccato, S. Sturaro, N. Laurenti, A key management architecture for GNSS open service navigation message authentication, in: 2017 European Navigation Conference (ENC), IEEE, 2017, pp. 287–297.
[159] L. Deng, S. Ye, H. Qiu, Transmission security platform for transportation information based on BeiDou navigation satellite system, in: 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2018, pp. 2110–2113.
[160] I. Altaf, M.A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, C.-M. Chen, A lightweight key agreement and authentication scheme for satellite-communication systems, IEEE Access 8 (2020) 46278–46287.
[161] Z. Yantao, M. Jianfeng, A highly secure identity-based authenticated key-exchange protocol for satellite communication, J. Commun. Netw. 12 (6) (2010) 592–599.
[162] C.-C. Lee, A simple key agreement scheme based on chaotic maps for VSAT satellite communications, Int. J. Satell. Commun. Netw. 31 (4) (2013) 177–186.
[163] M. Qi, J. Chen, Y. Chen, A secure authentication with key agreement scheme using ECC for satellite communication systems, Int. J. Satell. Commun. Netw. 37 (3) (2019) 234–244.
[164] M. Joye, G. Neven, Identity-Based Cryptography, Vol. 2, IOS Press, 2009.
[165] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits Syst. Mag. 1 (3) (2001) 6–21.
[166] A.P. Sarr, P. Elbaz-Vincent, J.-C. Bajard, A new security model for authenticated key agreement, in: J.A. Garay, R. De Prisco (Eds.), Security and Cryptography for Networks, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 219–234.
[167] M. Bellare, R. Canetti, H. Krawczyk, A modular approach to the design and analysis of authentication and key exchange protocols, in: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, 1998, pp. 419–428.
[168] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution, Npj Quantum Inf. 2 (1) (2016) 1–12.
[169] L. Gyongyosi, S. Imre, A survey on quantum computing technology, Comput. Sci. Rev. 31 (2019) 51–71.
[170] I. Khan, B. Heim, A. Neuzner, C. Marquardt, Satellite-based QKD, Opt. Photonics News 29 (2) (2018) 26–33.
[171] R. Bedington, J.M. Arrazola, A. Ling, Progress in satellite quantum key distribution, Npj Quantum Inf. 3 (1) (2017) 1–13.
[172] D.M. Benton, P.M. Gorman, P.R. Tapster, D.M. Taylor, A compact free space quantum key distribution system capable of daylight operation, Opt. Commun. 283 (11) (2010) 2465–2471.
[173] A. Tomaello, C. Bonato, V. Da Deppo, G. Naletto, P. Villoresi, Link budget and background noise for satellite quantum key distribution, Adv. Space Res. 47 (5) (2011) 802–810.
[174] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M.J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, A. Forbes, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, Phys. Rev. A 88 (3) (2013) 032305.
[175] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, P. Villoresi, Experimental satellite quantum communications, Phys. Rev. Lett. 115 (4) (2015) 040502.
[176] Y.C. Tan, R. Chandrasekara, C. Cheng, A. Ling, Radiation tolerance of opto-electronic components proposed for space-based quantum key distribution, J. Modern Opt. 62 (20) (2015) 1709–1712.
[177] J.-P. Bourgoin, N. Gigov, B.L. Higgins, Z. Yan, E. Meyer-Scott, A.K. Khandani, N. Lütkenhaus, T. Jennewein, Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations, Phys. Rev. A 92 (5) (2015) 052339.
[178] S. Liao, W. Cai, W. Liu, L. Zhang, Y. Li, J. Ren, J. Yin, Q. Shen, Y. Cao, Z. Li, et al., Satellite-to-ground quantum key distribution, Nature 549 (7670) (2017) 43–47.

[179] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nat. Photonics 11 (8) (2017) 502–508.
[180] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, M. Takeoka, M. Fujiwara, M. Sasaki, Polarization-basis tracking scheme in satellite quantum key distribution, Int. J. Opt. 2011 (2011).
[181] T. Jennewein, C. Grant, E. Choi, C. Pugh, C. Holloway, J. Bourgoin, H. Hakima, B. Higgins, R. Zee, The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite, in: Emerging Technologies in Security and Defence II; and Quantum-Physics-Based Information Security III, Vol. 9254, International Society for Optics and Photonics, 2014, 925402.
[182] V. Sharma, S. Banerjee, Analysis of quantum key distribution based satellite communication, in: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2018, pp. 1–5.
[183] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, P. Villoresi, Feasibility of satellite quantum key distribution, New J. Phys. 11 (4) (2009) 045017.
[184] R. Bedington, T. Zhongkan, R. Chandrasekara, C. Cheng, T.Y. Chuan, K. Durak, A.V. Zafra, E. Truong-cao, A. Ling, D. Oi, Small photon entangling quantum system (SPEQS) enabling space based quantum key distribution (QKD), in: International Astronautical Congress, Jerusalem, Israel, 2015.
[185] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, et al., Direct and full-scale experimental verifications towards ground–satellite quantum key distribution, Nat. Photonics 7 (5) (2013) 387–393.
[186] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, et al., Long-distance free-space quantum key distribution in daylight towards inter-satellite communication, Nat. Photonics 11 (8) (2017) 509–513.
[187] J.G. Rarity, P. Tapster, P. Gorman, P. Knight, Ground to satellite secure key exchange using quantum cryptography, New J. Phys. 4 (1) (2002) 82.
[188] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature 589 (7841) (2021) 214–219.
[189] Quantropi, Inc., Quantropi QiSpace, 2015, (Accessed: 2022-Jul-10). URL https://lp.quantropi.com/qispace-trial.
[190] K. Takeda, A. Noiri, T. Nakajima, J. Yoneda, T. Kobayashi, S. Tarucha, Quantum tomography of an entangled three-qubit state in silicon, Nat. Nanotechnol. 16 (9) (2021) 965–969.
[191] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, M. Voznak, Quantum key distribution: A networking perspective, ACM Comput. Surv. 53 (5) (2020).
[192] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, A.K. Mishra, Quantum key distribution secured optical networks: A survey, IEEE Open J. Commun. Soc. 2 (2021) 2049–2083.
[193] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Modern Phys. 92 (2020) 025002.
[194] W. Li, V. Zapatero, H. Tan, K. Wei, H. Min, W.-Y. Liu, X. Jiang, S.-K. Liao, C.-Z. Peng, M. Curty, F. Xu, J.-W. Pan, Experimental quantum key distribution secure against malicious devices, Phys. Rev. Appl. (2021).
[195] F. Salahdine, N. Kaabouch, Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey, Phys. Commun. 39 (2020) 101001.
[196] M. Mozaffari, et al., A tutorial on UAVs for wireless networks: Applications, challenges, and open problems, IEEE Commun. Surv. Tutor. 21 (3) (2019).
[197] Z. Yin, M. Jia, N. Cheng, W. Wang, F. Lyu, Q. Guo, X. Shen, UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications, IEEE Trans. Intell. Transp. Syst. 23 (3) (2022) 2739–2751.
[198] N. Cheng, F. Lyu, W. Quan, C. Zhou, H. He, W. Shi, X. Shen, Space/aerial-assisted computing offloading for IoT applications: A learning-based approach, IEEE J. Sel. Areas Commun. 37 (5) (2019) 1117–1129.
[199] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, X.S. Shen, Software defined space-air-ground integrated vehicular networks: Challenges and solutions, IEEE Commun. Mag. 55 (7) (2017) 101–109.
[200] A.-V. Emilien, C. Thomas, H. Thomas, UAV & satellite synergies for optical remote sensing applications: A literature review, Sci. Remote Sens. 3 (2021) 100019.
[201] P.P. Ray, A review on 6G for space-air-ground integrated network: Key enablers, open challenges, and future direction, J. King Saud Univ. - Comput. Inf. Sci. (2021).
[202] G. Oligeri, S. Raponi, S. Sciancalepore, R. Di Pietro, PAST-AI: Physical-layer authentication of satellite transmitters via deep learning, 2020, arXiv preprint arXiv:2010.05470.
[203] M. von Rechenberg, P.H.L. Rettore, R.R.F. Lopes, P. Sevenich, Software-defined networking applied in tactical networks: Problems, solutions and open issues, in: 2021 International Conference on Military Communication and Information Systems (ICMCIS), 2021, pp. 1–8.
[204] A. Papa, T. de Cola, P. Vizarreta, M. He, C. Mas-Machuca, W. Kellerer, Design and evaluation of reconfigurable SDN LEO constellations, IEEE Trans. Netw. Serv. Manag. 17 (3) (2020) 1432–1445.
[205] L. Bertaux, S. Medjiah, P. Berthou, S. Abdellatif, A. Hakiri, P. Gelard, F. Planchou, M. Bruyere, Software defined networking and virtualization for broadband satellite networks, IEEE Commun. Mag. 53 (3) (2015) 54–60.
[206] L.F. Eliyan, R. Di Pietro, Dos and ddos attacks in software defined networks: A survey of existing solutions and research challenges, Future Gener. Comput. Syst. 122 (2021) 149–171.
[207] A. Kak, I.F. Akyildiz, Towards automatic network slicing for the internet of space things, IEEE Trans. Netw. Serv. Manag. (2021) 1.
[208] I.F. Akyildiz, A. Kak, The internet of space things/cubesats, IEEE Netw. 33 (5) (2019) 212–218.
[209] I.F. Akyildiz, A. Kak, The Internet of Space Things/CubeSats: A ubiquitous cyber-physical system for the connected world, Comput. Netw. 150 (2019) 134–149.
[210] ESA, How do you build a green satellite? 2021, (Accessed: 2022-Jul-10). URL https://blogs.esa.int/cleanspace/2016/10/24/how-do-you-build-a-green-satellite/.
[211] Z.Z. Kassas, J. Khalife, M. Neinavaie, The first carrier phase tracking and positioning results with starlink LEO satellite signals, IEEE Trans. Aerosp. Electron. Syst. (2021) 1.
[212] M. Scholl, (Draft) Introduction to Cybersecurity for Commercial Satellite Operations, National Institute of Standards and Technology (NIST), 2021.
[213] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, G. Araniti, Non-terrestrial networks in 5G & beyond: A survey, IEEE Access 8 (2020) 165178–165200, http://dx.doi.org/10.1109/ACCESS.2020.3022981.
[214] 3GPP, TR 38.821: Solutions for NR to support non-terrestrial networks (NTN), 2021, (Accessed: 2022-Jul-10). URL https://www.3gpp.org/ftp/Specs/archive/38_series/38.821/.
[215] 3GPP, 3GPP release 17, 2022, (Accessed: 2022-Jul-10). URL https://www.3gpp.org/release-17.
[216] 3GPP, 3GPP release 18, 2022, (Accessed: 2022-Jul-10). URL https://www.3gpp.org/release18.
[217] S. Kota, G. Giambene, 6G integrated non-terrestrial networks: Emerging technologies and challenges, in: IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2021, pp. 1–6.
[218] SAT5G, Satellite and terrestrial network for 5G - D6.1: Roadmap to satellite into 5G, 2021, (Accessed: 2022-Jul-10). URL https://www.sat5g-project.eu/wp-content/uploads/2019/04/761413_Deliverable_25_Roadmap-for-Satellite-into-5G.pdf.
[219] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, Security and privacy in 6G networks: New areas and new challenges, Digit. Commun. Netw. 6 (3) (2020) 281–291.
[220] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, Y.-D. Lin, Security and privacy for 6G: A survey on prospective technologies and challenges, IEEE Commun. Surv. Tutor. 23 (4) (2021) 2384–2428.
[221] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture, Tech. rep., National Institute of Standards and Technology, 2020.

Pietro Tedeschi is Senior Security Researcher at Technology Innovation Institute, Autonomous Robotics Research Center, Abu Dhabi, United Arab Emirates. He holds a Ph.D. in Computer Science and Engineering from HBKU-CSE, Qatar. He received his Master's degree with honors in Computer Engineering at Politecnico di Bari, Italy. His security research interests lie in UAVs, Wireless, IoT, Applied Cryptography.

Dr. Savio Sciancalepore is Assistant Professor at TU/e Eindhoven, Netherlands. He received his Master's and Ph.D. both from the Politecnico di Bari, Italy. His research interests include applied wireless and network security issues in Internet of Things and Cyber-Physical Systems.

Dr. Roberto Di Pietro, ACM Distinguished Scientist, is Full Professor of Cybersecurity at HBKU-CSE. His research interests include Distributed Systems Security, Wireless Security, OSN Security, and Intrusion Detection. In 2020 he received the Jean-Claude Laprie Award for having significantly influenced the theory and practice of Dependable Computing.