International Journal of Information Security (2021) 20:287–311
https://doi.org/10.1007/s10207-020-00503-w

REGULAR CONTRIBUTION

Cyber security in New Space

Analysis of threats, key enabling technologies and challenges

M. Manulis[1] · C. P. Bridges[2] · R. Harrison[1] · V. Sekar[1] · A. Davis[3]

Published online: 12 May 2020

Abstract
Developments in technologies, attitudes and investment are transforming the space environment, achieving greater accessibility for an increasing number of parties. New and proposed constellations will increase the in-orbit satellite population by the order of thousands, expanding the threat landscape of the space industry. This article analyses past satellite security threats and incidents to assess the motivations and characteristics of adversarial threats to satellites. The ground and radio frequency communications were the most favoured targets; however, the boom of satellites constellations in the upcoming years may shift this focus towards the space segment which must be addressed. Key technology advancements and open issues in the satellite industry related to security and operational requirements are also discussed.

Keywords New Space · Cyber security · Satellites · Constellations · COTS

1 Introduction

The space industry is a complex system of moving parts, changing dynamics and developing ideas. Emerging through the Cold War era, it was dominated by a handful of nations and state-level activity, developing large and expensive satellites with long operational lifetimes. Information was strictly on a need-to-know basis which aimed to hinder the military capabilities of enemies, laying a groundwork of obscurity in developmental practices. The practices surfacing during this time are typical of what is known as "Old Space".

Since this time, the boom of the consumer microelectronics industry, more rapid research and development practices and the lower costs of launch means that space is viewed now as a highly valued resource for business. This private sector interest has expanded the space market globally (estimated to be worth $269 billion as of 2017 [1]) and brought different players and projects to the table. The change in the economics of space to one which is profit-driven has prompted R&D to have a quicker turnaround with smaller agile teams, mirroring the IT industry rather than traditional aerospace or military outfits [2].

This agility pattern born from incorporating standard modules and components whilst making space travel cheaper and more widespread across industries is characterized by the term "New Space". This ecosystem, as Paikowsky [3] calls it, is also moving towards other trends such as large satellite constellations of the orders of hundreds and thousands, and small satellite (weighing 600 kg or less) production. In 2018, 328 small satellites were launched, six times as many as in 2012, with and half of them for commercial purposes [4]. Commercial-off-the-shelf (COTS) components are now commonplace in satellites and ground control systems, decreasing construction times and costs. Companies are tak-

Electronic supplementary material The online version of this article (https://doi.org/10.1007/s10207-020-00503-w) contains supplementary material, which is available to authorized users.

✉ M. Manulis
m.manulis@surrey.ac.uk

C. P. Bridges
c.p.bridges@surrey.ac.uk

R. Harrison
r.l.harrison@surrey.ac.uk

V. Sekar
venkkatesh.sekar@surrey.ac.uk

[1] Surrey Centre for Cyber Security, University of Surrey, Guildford, UK

[2] Surrey Space Centre, University of Surrey, Guildford, UK

[3] NCC Group, Manchester, UK

ing more risks with their satellites, leading to more innovative applications and technologies.

Major applications of New Space The academic sector is striving to push the innovative boundaries of New Space by exhibiting new technologies in space. Missions such as STRaND-1[1] demonstrated the feasibility of using smartphone electronics in satellites.

A surge of investment in the Earth observation market has been powered by the applications of satellite imagery and signals intelligence, namely business intelligence products [5], as well as environmental conservation efforts. Companies such as Planet[2] and HawkEye 360[3] are operating constellations of small satellites in low Earth orbit (LEO).

Global broadband services, another major applications emerging in New Space, aim to bring connectivity to rural and remote areas and provide fault-tolerant networks for critical services. Satellite broadband revenue has shown steady growth in the last five years, with more rapid growth predicted as proposed satellite constellations of the order of hundreds and thousands become operational [1,5], such as Starlink, OneWeb, Telesat and LeoSat.

Satellite geolocation services, providing precise time and position data to dedicated receivers, have been a steady addition to several industries, enabling applications including route planning, fleet management and time-critical purposes used in the financial and energy sectors. Many sectors to which Global Navigation Satellite Systems (GNSS) can be applied have developed the global ground equipment market. In 2016, GNSS equipment revenue made $84.6 billion of the total ground equipment revenue of $113.4 billion, which has been on a steady incline since 2012 [5].

The use of satellites in warfare has a leading role to play in the modern era, with 68% of munitions being guided by satellites in the 2004 Iraq war [6]. These systems have stricter security requirements and to employ features such as encryption, anti-jamming techniques and frequency hopping. The US military's use of commercial satellites has increased in recent conflicts and pushed further with legislation passed in the Bush era [7,8]. Small satellites are being increasingly used to support military functions, with USA, Russia and China launching 39, 20 and 17 small satellites, respectively, between 2012 and 2018 [4].

This paper therefore aims to provide an analysis of the New Space era in terms of the previous security threats, emerging security challenges and key technologies which are advancing and innovating the space and satellite industry.

Security challenge Being able to manipulate such remote objects as satellites provides a new challenge to the hacking community. Scarce documentation and source code provide the ultimate "black box" challenge. Combined with the "security through obscurity" mentality with which vendors develop these products, major vulnerabilities in satellite systems are being discovered. The security analysis of satellite user terminals in [9,10] brought to light numerous vendor's use of hard-coded credentials, insecure protocols and weak authentication mechanisms. This ageing mentality is not suitable for systems making use of cyber technologies, especially those which support critical infrastructure which are piquing the interest of the hacking community.

Security is now no longer an afterthought for terrestrial enterprises; standards, regulations and organizational security-driven mindsets have prompted the integration security practices both retrospectively and from a foundation level. An attack may not succeed using terrestrial methods and may be easier or more beneficial to target a satellite-based system which the organization uses. For instance, to negatively impact an economy may be more easily achieved by targeting satellites providing point-of-sale card services for many commercial entities [11].

Organization Section 2 provides an overview of satellite architectures of the space and ground segments. Section 3 presents security threats relevant to space systems, partly based on the analysis of previous satellite security incidents. Technologies which are enabling and enhancing the New Space industry are outlined in Sect. 4, and outstanding challenges for space and satellite security are identified in Sect. 5.

2 Satellite life cycle and space system architectures

This section presents an overview of the main life cycle phases for satellites and details the different space architectures.

2.1 Satellite life cycle

The duration of a satellite's operation is primarily mission-specific, but the life cycle of a satellite after its manufacture follows a standard structure of launch, commissioning, in-service and end of life.

Launch After stacking a launch vehicle with the satellites and launched into space from a designated facility. After reaching the intended position, the launch vehicle will deploy the satellites, which several operators may have shared.

Commissioning The satellite is positioned on its specific orbit in order for normal operations to occur called commissioning. The ground segment begins to monitor and control the satellite using Telemetry, Tracking and Command (TT&C)

[1] https://amsat-uk.org/satellites/tlm/strand-1/

[2] https://www.planet.com/

[3] https://www.he360.com/

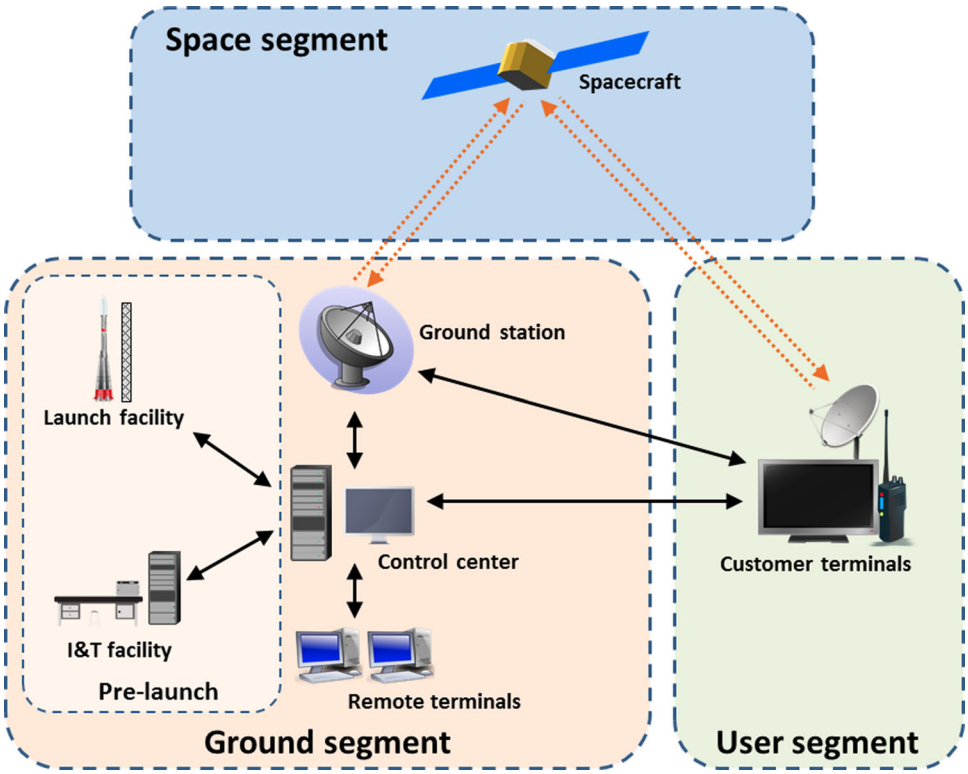


Fig. 1 Typical satellite architecture. Dotted orange arrows denote radio links; solid black arrows denote ground network links. Figure from [13]

systems, and the health of satellite subsystems is validated to prepare for in-orbit operations, typically over a two-month period.

In-service The satellite begins its designated mission until it is disposed of. The majority of the satellite's lifetime will be spent in routine operations, with the ground stations monitoring TT&C to maintain the satellite and operate the payload.

End of life At the end of its operation, commands to shut down the satellite are issued from the ground. The satellite is commanded to enter either into a higher "graveyard" orbit, or into a lower orbit for the satellite to burn up in the atmosphere.

2.2 Space and satellite systems

Space systems have a typical structure, consisting of a space segment and a ground segment, which communicate with each other via radio frequency (RF) signals (see Fig. 1). The space segment comprises the satellites or groups of satellites in orbit (as well as launch vehicles designed to release satellites into space). A satellite contains a payload, the equipment designed to carry out the satellite's function, and a bus, which houses the payload and remaining satellites systems. The main satellite systems include TT&C, command and data handling (C&DH) and attitude determination and control (ADCS). These systems are responsible for receiving and processing uplink and downlink signals, validating, decoding and sending commands to other subsystems, and controlling the stabilization and orientation of the satellite, respectively [12]. Communications with the satellites are achieved through RF waves, usually sent with frequencies in the MHz and GHz range. The communication channel from the Earth to the satellite is the uplink and, similarly, from the satellite to the Earth is the downlink. Table 1 lists the common RF frequency bands used in satellite communications. The ground segment encompasses all the terrestrial systems which receive or send RF signals, monitor and command satellites, and distribute payload and telemetry data to stakeholders. The principal ground segment elements include ground stations with corresponding TT&C capabilities, centres to manage mission operations and the payload, and the terrestrial networks which connect the various ground systems to each other and disseminate data collected from the payload.

Another element of the satellite architecture is the user segment, which can be seen as an extension of the ground segment for the end-users of a satellite-based service. This is the device or interface which can interact with satellite signals directly or with other ground segment systems or applications.

2.3 Space segment architectures

The shape of the space segment varies greatly depending on the purpose of the mission, the simplest being a single

Table 1 Satellite frequency bands

Name	Band
VHF	30–300 MHz
UHF	300–1000 MHz
L	1–2 GHz
S	2–4 GHz
C	4–8 GHz
X	8–12 GHz
Ku	12–18 GHz
K	18–27 GHz
Ka	27–40 GHz
V	40–75 GHz
W	75–110 GHz

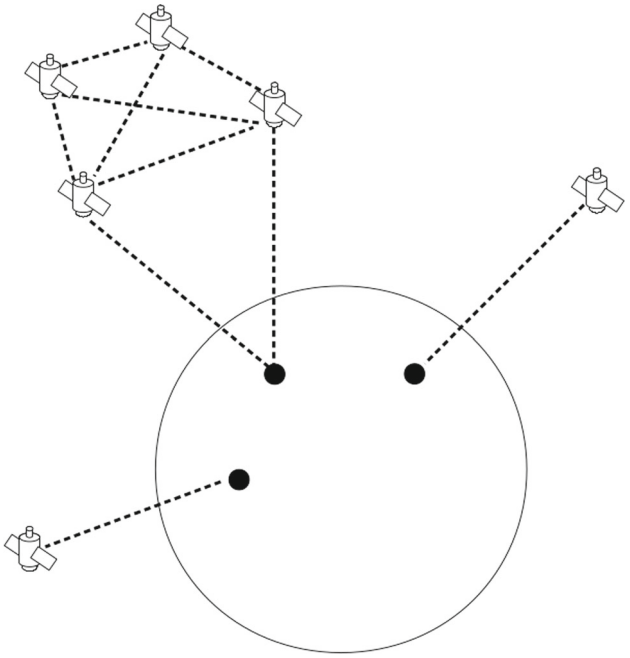


Fig. 2 Single satellite and satellite cluster orbiting Earth. Dotted lines represent communication links between satellites and between satellites and designated ground sites on Earth

satellite, characteristic of university, scientific or research missions.

A mission may make use of multiple orbiting satellites, clusters and constellations being the two main scenarios (see Figs. 2 and 3). A cluster usually contains a small number of satellites orbiting in close proximity to each other in some sort of formation. Satellite constellations usually consist of a large number of satellites in different orbital planes. Likely be controlled and coordinated by the same operator, the constellation will synchronize orbits and commands to create complimentary ground coverage to complete the mission objective.

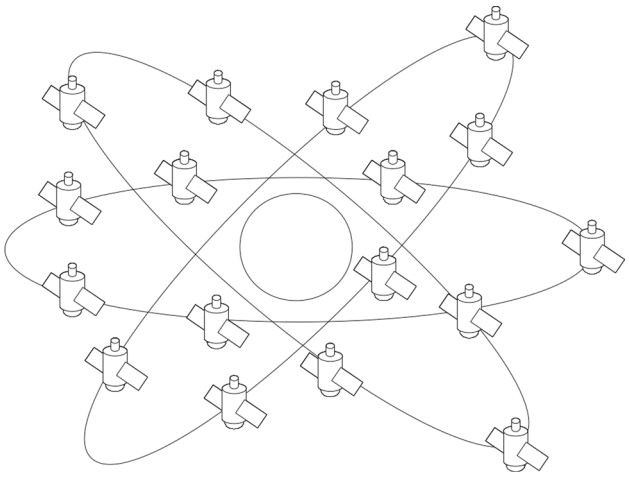


Fig. 3 Satellite constellation orbiting Earth. Solid lines represent satellite orbits

Satellites can communicate solely with the ground segment and can also pass data through inter-satellite links between satellites in the constellation or cluster.

2.3.1 Satellite constellations

Several new satellite constellations are operating in space. This section provides an overview of some current and proposed constellations. Information relating to constellation size, satellite mass and expected lifetime, and communication implementations is given in Table 2.

Planet Planet own and operate an earth-imaging constellation with the company mission to image the entire Earth's surface every 24 hours. Their 3U CubeSats known as "Doves" make use of the Ubuntu OS, Debian packages and Python modules and host a 90-mm aperture optical payload [14].

A ground station network of 11 sites supports Planet's flock of Doves. These ground stations, designed to be of a standard and reproducible COTS component build, are located across the globe. After a successful pass, imaging data and telemetry logs are uploaded to servers hosted in Amazon Web Services (AWS), a managed cloud provider, and their mission control software is also written in Python [15].

Imagery data are formatted with Digital Video Broadcasting—Satellite—Second Generation (DVB-S2) encoding scheme as the physical layer. Generic stream encapsulation (GSE) is applied to the data link layer, prior to being formatted as IP packets. This link is apparently encrypted and is used to downlink pictures and logs [14].

HawkEye 360 HawkEye 360 has a constellation of three satellites which fly in a cluster formation, named its Pathfinder mission, the primary purpose of which is to provide high-precision radio frequency interference (RFI) geolocation

Table 2 Satellite constellations

Company	Constellation Size	Satellite mass (kg)	Expected lifetime	Communication bands	Protocols
Planet	140	5	1–5 years	X-band	DVB-S2
				S-band u	GSE
				UHF TT&C	IP
HawkEye 360	3 (present)	12.75	2–7 years	S-band	Unknown
	18 (future)			X-band	
				UHF TT&C	
				S-band TT&C	
				S-band ISL	
Starlink	12,000	227	5–7 years	Ka-band	Unknown
				Ku-band	
				V-band	
				Optical ISL	
OneWeb	648	150	5 + years	Ka-band	Unknown
				Ka-band	
				V-band	
Leosat	108	1250	Unknown	Ka-band	DVB-S2
				Optical ISL	DVB-S2X

services. The Pathfinder mission serves as a proof-of-concept, laying the foundation for larger eighteen-satellite (six-cluster) constellation [16].

HawkEye 360 also make use of COTS components onboard their satellites, specifically using Linux operating systems, GNU radio+ software[4] and COTS software-defined radios (SDRs). They revealed that its satellite's SDR payload is based on the XilinxZynq 7045 SoC and uses analog devices 9361 transceivers [17]. Commercial ground station operator KSAT[5] was chosen by HawkEye 360 to provide primary ground segment support, with UHF/S-band TT&C stations located at HawkEye 360 headquarters in Virginia, USA.

Starlink SpaceX has plans to build an almost 12,000-satellite constellation to provide high-speed global broadband. Starlink satellites can perform orbit manoeuvres with krypton-powered Hall thrusters. Two prototype satellites, Tintin A & B, were launched in 2018, and a further 60 test satellites were launched in May 2019 [18,19].

Limited details have been released about the hardware and software designs of the satellites and ground segment systems, and communication protocols used. Starlink is also proposed to make use of optical inter-satellite links [20]; however, these have not been demonstrated with the 60 test satellites [21].

OneWeb Another player in the satellite broadband market is OneWeb. An initial test constellation of six satellites was launched in 2018, featuring an electronic propulsion system consisting of Hall thrusters powered by Xenon and the use of AES-256 encryption [22]. Unlike Starlink's vertically integrated approach, OneWeb has partnered with Airbus, Hughes and GMV for manufacturing, ground segment support and constellation management [22–24].

LeoSat LeoSat's constellation also aims to provide a high-speed data network with global coverage, targeted towards the business-to-business market. The constellation, to be developed by Thales Alenia Space [25], will be operated from two distributed ground operation centres [26]. Each satellite will have four optical inter-satellite links, acting as routers in space, in an attempt to remove the dependence on ground gateways to relay data.

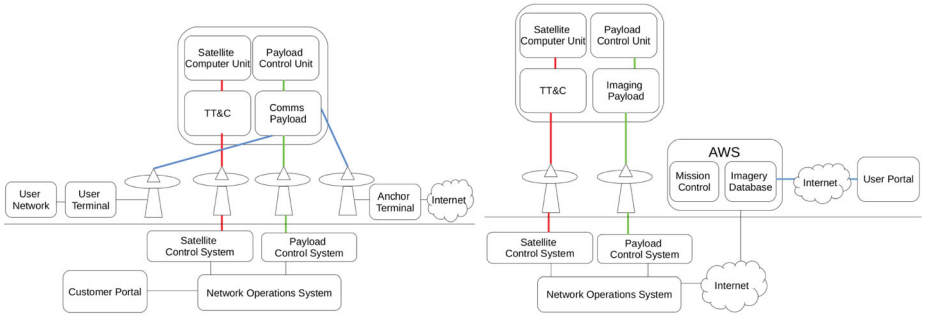
2.4 Ground segment architectures

The ground segment architecture varies greatly depending on the mission purpose, the service to be provided and the types of communication interfaces required. The user segment, whilst separate from the main ground segment, also influences its design.

TT&C and network operations can be separated from communications related to the service the satellite provides. Users can obtain data through a direct connection between a satellite and dedicated receiver device, or through a gateway ground station forwarding on data from its connection with a satellite to a user interface via terrestrial networks. Alternatively, data can be exchanged with the service provider

[4] https://www.gnuradio.org/

[5] https://www.kongsberg.com/ksat/



(a) Ground segment for communications satellites. **(b)** Ground segment architecture for web-based access e.g. Planet [75].

Fig. 4 Ground segment architectures. Red lines represent satellite TT&C communications, green lines represent payload control communications, and blue lines represent the link between two users of the communication service. Black lines represent terrestrial networking links

through feeder or hub stations, as discussed in the following examples.

Communications satellites Communication satellites are typically placed in geostationary orbits (GEO) which orbit at the same rate as the Earth at the same fixed point, but can also operate in LEO. They act as a relay between two parties wishing to communicate, commonly known as bent pipe architecture. The sending ground station transmits a message to the satellite on one frequency, which the satellite then passes onto the destination ground station at a different frequency which is then sent through the user's network (see Fig. 4a). These types of satellites enable communication between remote areas with limited terrestrial infrastructure.

Broadcast-only satellites For particular markets, the space and ground segment are constructed to offer broadcast-only services to users. Services such as direct-to-home (DTH) satellite television and GNSS rely on specific hardware for users to receive and use signals broadcast over a large area. In DTH broadcasting, TV programmes are uplinked to a satellite from an Earth station and then broadcasted over a wide region to be received by a user's personal dish at their home. In the case of radionavigation, GNSS satellites transmit positioning and timing information to dedicated GNSS receivers.

Web-based access Other architectures exist in which the satellite operator regulates the distribution of payload data from their satellites. In this case, users have no requirement for dedicated equipment to receive satellite signals, as the satellite operators release data themselves to their users through terrestrial capabilities (see Fig. 4b). Planet's Earth Observation (EO) imagery uses 11 ground stations built to a standard specification, all of which can command and control satellites and receive imagery data. These data are centrally processed by systems in the cloud, and access to imagery data is regulated by Planet and distributed through web application program interfaces (APIs) and browser-based applications [15].

3 Threats to space systems and security-related incidents

The space industry has been the victim of several attacks since its inception from a wide range of adversaries and for a multitude of reasons. This section explores the types of attacks which the space industry has faced, the motivation behind them and the sectors most at risk. An analysis of past security incidents on the space industry is also presented. The Consultative Committee for Space Data Systems (CCSDS) report titled "Security Threats against Space Missions" [27] presents an overview of threats against space missions, including illustrative examples of threats against various classes of missions. However, it is difficult to present a detailed threat model as it is strongly tied with the goals and security requirements of the target mission. In this section, hence, we explore the critical security threats and their feasibility of exploitation in New Space.

3.1 Ground segment

Compromising the ground station is ultimately the easiest way to control a satellite as it provides the equipment and software required to legitimately control and track it, and it uses existing and established terrestrial systems and attack vectors. The types of threats are generally the same during a satellite's life cycle. Types of attacks can include:

– Physical attacks, including compromising physical security measures, e.g. gaining unauthorized access to a ground station and other physical IT assets. A successful exploitation of a vulnerability through a physical attack might disable the ground station and directly affect the operation of the mission and the services provided. It might also aim to overtake the facility in order to take control of the spacecraft without technically attacking the systems. A NASA report, [28], detailed the theft of an unencrypted notebook computer and the consequent loss of International Space Station command and control algorithms.

- Computer network exploitation (CNE) is where an attacker is able to compromise the network to which a ground station is connected to. In the same vein as attacks on enterprise IT networks, attacks could feature exploitation of poorly configured or vulnerable technologies as well as phishing to again gain unauthorized access to ground control stations.
- Cloud infrastructure, presently, powers majority of the computing framework in the ground station. From data storage to data processing, the entire platform is pipelined to cloud solutions. For example, AWS ground station is a fully managed service that lets you control satellite communications, process data and scale your operations without having to worry about building or managing your own ground station infrastructure. Failure of the cloud infrastructure could have catastrophic effect on the ground station including denial of service (DoS) for the satellite receiver. Major cloud service providers including AWS and Google Cloud Platform (GCP) are known to have regular outages or disruptions among their networks due to both internal and external attacks [29,30]. These instances could hinder operations of satellite-based real-time systems.
- Data corruption/modification refers to the intentional or non-intentional alteration of data, whether being communicated or at rest. It can result in software failures or bugs, hardware failures, use of unauthorized software, or active attempts to change/modify data to deny its use. A corrupted spacecraft command could result in catastrophic loss if either no action occurred (e.g. command is discarded) or the wrong action was taken onboard a spacecraft.
- Supply chain attacks including leaking of software/tools/data sheets, open source research and use of common components, resulting in vulnerabilities and exploits which are incorporated into the supply chain.
- Unpatched/Outdated/Legacy COTS software deployed among the platform is a known attack surface. CVE (Common Vulnerabilities and Exposures)[6] is an actively maintained list of publicly disclosed vulnerabilities against COTS or open-sourced software. However, the deployed software needs to be continuously updated with the latest version which contains the fixes for the discovered vulnerabilities. Unpatched versions of the software expose the application with openly documented attack vectors available for exploitation.

3.2 Communications

Communications to and from the satellite are achieved through RF waves, usually sent with frequencies in the GHz range. TT&C and data communications can be compromised at any point in the satellite's life cycle, which may require the attacker to gather additional information and conduct attacks on the ground segment. The main attack methods to disrupt data communications are listed below.

Jamming Jamming is the act of overpowering a RF signal of a particular frequency with a higher power one of the same frequency, in order to disrupt communications between the ground station and satellite, or vice versa. Requiring an antenna, knowledge of the signal frequency and the appropriate power level to transmit, an attacker can transmit a continuous signal to deny legitimate communications. Alternative methods for jamming can be achieved through software vulnerabilities, discussed in Sect. 3.3. Key advances in the field can be seen through the Boeing EA-18G Growler air platform [31], an actively developed jamming infrastructure for electronic warfare. It is equipped with special payload—jamming pods, which are carried in the place of conventional weapons, in under-wing pylons. One of the systems that may be carried by EA-18G is AN/ALQ-218, supplied by Northrop Grumman[7]. It is a Tactical Jamming System (TJS) applicable at the beginning of the radio-electronic communication.

The jammer consists of two independent groups of receivers, primary and auxiliary. The primary receiver group consists of four channelized and four cued receivers, which operate in tandem to provide immediate signal acquisition, accurate parameter measurement, immediate updates and precision geolocation, employing geolocation techniques by means of GPS tracking, or the IP address of a given device. In turn, the auxiliary receiver group provides an extended range of frequencies, substitutes the primary receiver in long-term measurements, helps in the recognition of intra-pulse modulation and updating estimates for geolocation. The AN/ALQ-218 engages a unique combination of short, medium and long baseline interferometer techniques, i.e. a device responsible for measuring the interference of electromagnetic waves, with a patented passive algorithm to provide geolocation of emitters for cueing jammers and other built-in equipment such as electro-optical sensors, infrared radiation (IR) technology and on-board radar stations.

Eavesdropping Eavesdropping is the interception of data over a communication channel. For satellite and ground systems, this channel is an RF signal sent over the air, meaning that all communications are susceptible to interception. Data sent over RF signals are sometimes not encrypted or use low-grade encryption which can be overcome to retrieve the cleartext information.

The ELectronic INTelligence (ELINT) satellites are one of the tools used by military and security services in several

[6] https://cve.mitre.org/

[7] https://www.northropgrumman.com/

countries to eavesdrop on the information being transmitted through the air. Galactic Radiation and Background (GRAB), a US 80-kg satellite launched in 1962, was the first ELINT satellite launched and provided unprecedented information about the signals emitted by Soviet radars at a time when those two superpowers were Cold War adversaries and when information about activities inside the Soviet Union was almost impossible to obtain at that time. The ELINT satellites need enormous antennas to pick up radio signals, since they are located 36,000 km above the equator. The antenna on the US military communications satellite Mobile User Objective System (MUOS) is 28.6 m diameter when unfurled in orbit—the largest known publicly. But the secret eavesdropping satellites are reported in the media to have already had 50-m-wide antennas by 1994 and 90-m ones by 2006 [32].

Hijacking Many instances of satellite hijacking, reusing a satellite for another purpose, have been noted in recent history. This could be altering the legitimate signals or changing them completely. COTS products can also be used for this purpose [33].

Broadcast signal intrusion is a form communication hijacking, where broadcast signals of radio, television or satellite are hijacked. The mode of hijacking can be done, either by overpowering the original signal at the same frequency or directly breaking into the transmitter and replacing the signal. The Max Headroom Broadcast Signal Intrusion Incident [34] is one of the most known instances, where the attacker smothered the TV station's broadcast by sending a more powerful signal to the antenna atop their broadcast tower and distributed it over their satellite link and land-based microwave links.

Spoofing Spoofing is the art of transmitting a signal, appearing to be legitimate, but sending erroneous data for your own purposes. The spoofing of location data in global navigation satellite systems can have a significant impact. For instance, Global Positioning System (GPS) signals which provide accurate location and timing services can be spoofed with COTS components [35]. In fact, GPS systems aboard several ships reported that the ships were on land when in fact they were still in the Black Sea [36].

Extensive research has been carried out to find the parameters values required for a successful GPS spoofing [37]. The identified ranges provide benchmarks to successively avoid spoofing attacks. Cryptographic techniques designed to protect GPS spoofing are further discussed in Sect. 4.5. Other techniques that have been developed to tackle spoofing include utilizing other self-contained sensors, namely inertial measurement units (IMUs) and vehicle odometer output [38]. To detect a spoofing attack, the technique analyses GNSS and IMU or odometer measurements independently during a preselected observation window and cross-checks the solutions provided by GNSS and inertial navigation solution (INS)/odometer mechanization.

The legacy GPS signals include an encrypted binary code known as Y-code that is transmitted, with these signals only intended for military use. Without the encryption keys, it is virtually impossible for an adversary to generate the Y-code and, hence, virtually impossible to spoof a GPS receiver set to track Y-code. The Selective Availability Anti-spoofing Module (SAASM) [31] can track Y-code only when loaded with the currently valid decryption key, and the modules are tamper-proof to prevent reverse engineering by adversaries. SAASM receivers such as the NovAtel OEM625 are only available to government-authorized customers. By using the encrypted signal, the device provides greater signal accuracy in the event of GPS interference. Furthermore, the government is capable of disabling civilian satellite navigation signal so that the only remaining signal is reserved for users with the SAASM module.

3.3 Space segment

Once in orbit, a satellite has limited physical contact with humans, although that does not mean security threats are not present. Vulnerabilities in the software and hardware in use on the satellite can occur and can impact the satellite's operation and robustness of security controls. In the case of using SDRs and digital signal processing software to provide radio functionality, insufficient checks in radio frame processing and sending malformed data packets could lead to buffer overflows and create denial-of-service conditions to jam communications [39]. This type of jamming is significantly more stealthy as it is triggered by sending only a small number of packets and also does not require sending a continuous RF jamming signal. Since satellites are deployed on missions requiring high dependability, they are equipped with embedded reliable operating systems (cf. Sect. 4.1), which provide significant security guarantees against memory-abuse attacks [40].

Depending on the complexity of the satellite and ground control systems and the security measures (or lack thereof) in place, taking control of a satellite to manipulate its system and/or orientation of orbit can be a difficult task. Requiring significant skill and knowledge to breach the TT&C links, and chaining several of the previously mentioned satellite attacks, other areas such as software vulnerabilities and replaying of recorded transmissions can contribute to achieving control. Even agencies such as NASA and government organizations are not immune to threats such as these, with several examples of satellites being under the control of attackers [41].

3.4 Regulatory requirements

Guidelines established by the Committee on National Security System (CNSS) have been used for years to regulate security protections on satellite communications used in national security missions. The CNSS Policy 12 (CNSSP-12) [42] strives to implement security practices into the ground and space systems at the design phase, rather than attempting to fit security in afterwards. It enforces the use of techniques such as authentication, NSA-approved end-to-end encryption and pseudorandom bit streams to achieve confidentiality and integrity and to remove predictability in messages.

Although commercial satellite systems used in national security missions and interfacing with government systems must also adhere to CNSSP-12, commercial and private spacecraft falling outside of this are not required to gain a formal accreditation of cyber security [43]. However, some enterprises are using the principles of CNSSP-12 to prioritize security requirements. As examples, the LeoSat constellation is trying to be "as close to CNSSP-12-compliant as possible" by incorporating encryption over all data sent over its network [44] and the Starlink constellation will feature "End-to-end encryption encoded at firmware level" [45].

3.5 Review and analysis of satellite incidents

For our analysis, we have prepared a timeline of incidents involving the space industry from various sources including academic literature, governmental agencies and news articles from the public domain between 1977 and 2019[8]. These incidents were categorized in terms of:

- The segment under attack or exploited
- The type of target, i.e. government, commercial, civilian and military
- The type of incident, e.g. jamming, spoofing, CNE, hijacking, etc.
- The motivation for the incident, e.g. state espionage, hack and leak, criminal activity, etc.

It should be noted that since these incidents are from public domain sources, certain limitations are placed on this analysis. Incidents may have been under- or miss-reported as incidents may have not been detected, or over confusion about what has happened, or for national security concerns in sectors such as military or government.

Table 3 shows a breakdown of the number of incidents with respect to the sector and segment which were targeted, and the type of technique used. The ground segment is the most targeted sector from the incidents examined, followed by RF data communications. This is anticipated due to the familiarity of tried and tested techniques on the ground segment by attackers and the exposure of RF communications across the world. The space segment, whilst having a smaller frequency of reported incidents, is still being targeted despite having several difficulties to conduct attacks.

Table 3 Segment and sector analysis of satellite security incidents

	Category	Frequency
Segment	Ground	83
	Space	8
	Data communications	38
	Unknown	2
Sector	Government	91
	Commercial	28
	Civilian	11
	Military	11
Incident type	Jamming	19
	Eavesdropping	3
	Spoofing	3
	Control	4
	CNE	30
	Hijacking	16
	Phishing	3
	Internet hijacking	1
	Denial of service	3
	Theft/loss	48
	ASAT incident	3

The majority of reported incidents were focused on governmental assets. Twenty-eight incidents targeted commercial organizations, over twice as many as the civilian or military sectors. Due to the secrecy of military operations, incidents may not have been reported publicly, and the frequency of military incidents may in fact be higher.

Incidents concerning the theft or loss of space industry-related assets and CNE activities were among the highest reported, expected due to the terrestrial-based nature of these techniques. Jamming and hijacking incident frequency follow behind and were the most popular to abuse and disrupt the RF communications segment. Other types of incidences were reported, such as eavesdropping, control, spoofing and phishing, but occurrences were limited to between 1 and 4 times.

The motivation of space and satellite incidents was also explored, and Fig. 5 shows the number of incidents for each type of motivation or intent. State espionage incidences made primary use of ground segment techniques. Common mistakes are being made in this segment as CNE activities hold a significant lead over data communications and space segment techniques. CNE and phishing techniques were also

[8] Timeline available from https://tinyurl.com/yxf5nzws

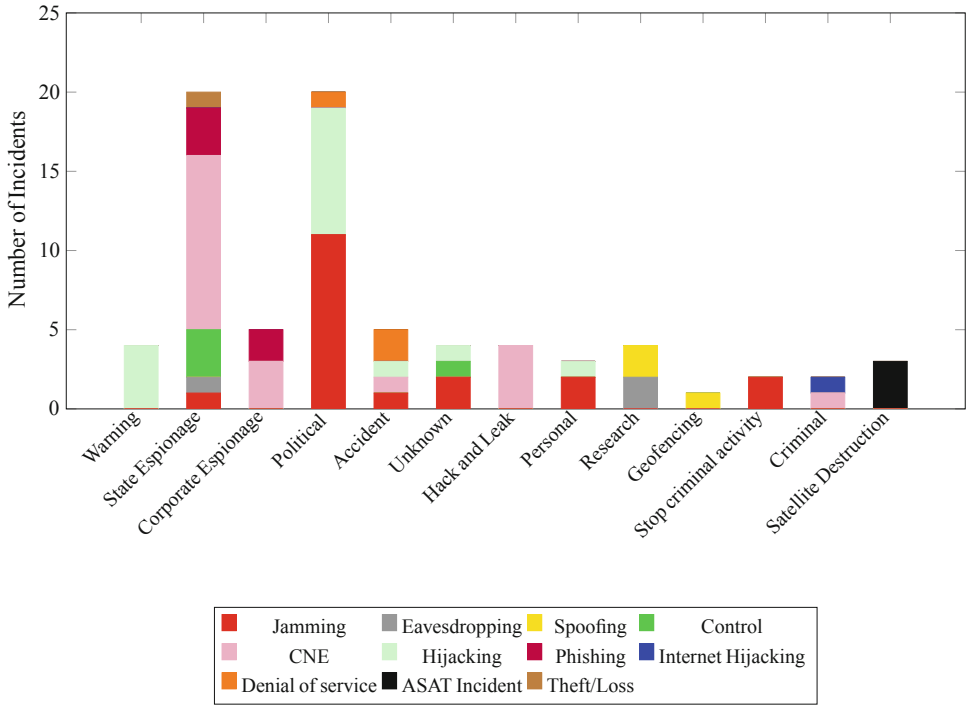


Fig. 5 Motivation of satellite incidents and a breakdown of the techniques used

dominant in incidents motivated by corporate espionage and hack and leak attacks.

Politically motivated incidents were usually carried out through RF jamming or signal hijacking, aiming to either stop or alter satellite TV and radio broadcasts with political messages. Signal jamming and hijacking were also noted to be accidental and from personal use, e.g. GPS jamming to avoid employer asset tracking, or in some cases for unknown motivations. Some instances of signal hijacking were used to convey warnings to the public over satellite TV ,and jamming was also used in attempts to stop criminal operations using satellite phones.

Three anti-satellite (ASAT) incidents (two tests and one planned mission) were intended to destroy a state's own orbiting satellites.

Criminal organizations exploit the ground and data communication segments, using CNE to gather information to sell onto other states. Another incident did not attack satellite systems directly, rather it used satellite Internet connections to find valid subscriber IP addresses to infect other servers [46]. As the ingenuity and innovation of the New Space era increase, so does that of adversaries.

A number of space and satellite industry incidents were also grouped in ten-year period in Fig. 6, which also shows the number of operational satellites between 1958 and 2018 from [47]. This figure shows an increase in the number of incidents reported in this ten-year period since 1977 and an increasing rate of satellites in operation. Both of these data sets show a substantial leap since the widespread adoption of the Internet in organizational IT practices in the early 2000s and beginning of the New Space age. Whilst there are competing factors to determine the success of malicious incidents, e.g. increases in computing power, new attack techniques and tools and the adoption of consistent security cultures, this increasing trend could be carried on in future decades if the space industry does not make security a priority.

4 Key enabling technologies in New Space

For decades, the designs of military, government and commercial satellite systems from space-capable nations have been on the most part, proprietary. This is in part due to the nature of the tasks these satellites were performing, those related to national security and sending sensitive data, or to protect satellite operator's intellectual property, although academic institutions generally detail the hardware and software in use in their satellite experiments. This section analyses key technologies of the New Space era.

4.1 Space segment

CubeSats One of the notable developments in satellites in New Space is the CubeSat specification[9]. Developed by California Polytechnic State University and Stanford University in 1999, the CubeSat specification encourages interest and skill development of small satellite manufacture and design

[9] http://www.cubesat.org/

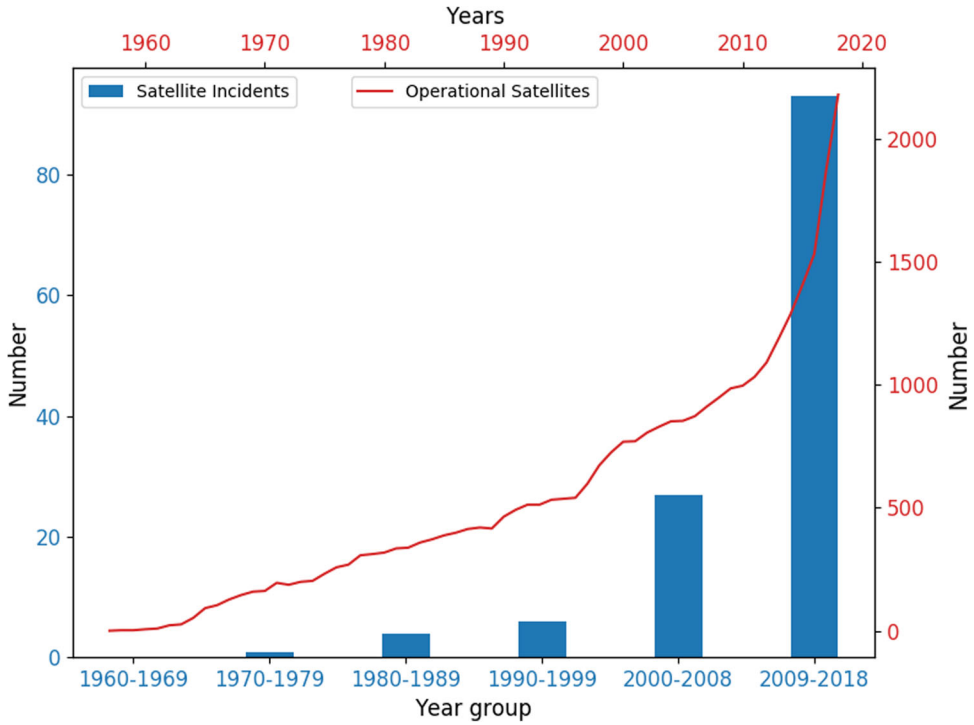


Fig. 6 Number of satellites attacks per year group is plotted on the bottom and left axes, and the number of operational satellites between 1958 and 2018 is plotted on the top and right axes

Table 4 Small satellite classifications

Classification	Mass (kg)
Minisatellite	100–500
Microsatellite	10–100
Nanosatellite	1–10
Picosatellite	0.1–1
Femtosatellite	0.01–0.1

whilst reducing costs and time efforts. The specification stipulates fixed dimensions of 10 cm × 10 cm × 11.35 cm and a total mass of 1.33 kg for the base unit (1U). CubeSats can be increased in size and mass by an order of units; common sizes are 3U and 6U, and even 20U in [16]. Other classifications for small satellites exist based upon their mass, as given in Table 4. 1U CubeSats belong to the picosatellite category.

CubeSats are steadily becoming a part of global computing infrastructure, where components need to be protected from adversarial physical access. Sensitive computation often has to be performed in a trusted execution environment (TEE), which, in turn, requires tamper-proof hardware. If the computational fabric can be tampered with, the correctness of the computation cannot be trusted. A recent study [48] has demonstrated this approach, providing a practical hardware security module solution for space and using them as a root of trust for a certificate authority (CA). CubeSats have also been used to demonstrate quantum key distribution (QKD) [49], a series of post-quantum secure cryptographic techniques for sharing a secret key among two parties (cf. Sect. 4.5).

COTS components, open source and GPL-licensed products The space industry has taken advantage of the global boom of affordable and powerful commercial electronics. The use of COTS components in academic endeavours is commonplace due to the limited budgets of research projects, but it has also provided a platform to examine and exhibit these technologies in-orbit. It seems a likely conclusion that satellite start-ups originating from university students will continue COTS practices to build upon their academic experience. In addition, the time and cost savings are a strong driver for COTS use across the entire commercial sector.

Details of satellites designed and constructed by *academic* institutions with COTS components in mind are prevalent. Many of these constructions utilize field programmable gate arrays (FPGAs), system-on-chip (SoC) components and microcontrollers. These satellites also make use of the open-source real-time operating system such as "XilKernel" [50], FreeRTOS [51]. Other open-source software and hardware designs specifically for space and ground systems include KubOS[10], UPSat[11] and EQUiSat[12].

In recent years, some *companies* have been more forthcoming about their satellite architectures, mainly those which implement COTS technologies. Section 2.3.1 details the information known about the construction of Planet and HawkEye 360's satellites. Planet also released an open-

[10] https://www.kubos.com/kubos/

[11] https://gitlab.com/librespacefoundation/upsat

[12] https://brownspace.org/equisat/

source radio solution[13] which has been deployed in each of its satellites, providing both hardware and software tools.

The trend towards use of COTS software and hardware is driven by several factors, including significantly lower procurement cost. COTS products are often highly complex, some of them involving tens of millions of lines of code, so that no one knows their content and behaviour in detail. Legacy systems make up the vast bulk of the code base, and all new systems become legacy when they come on line. With this complex system, COTS products are essentially a black box to their users. The US government provides a list [52] of risks associated with employing COTS software and mitigation techniques to avoid them. The usage of COTS products, thus, needs to be met with vigorous security analysis through black-box testing mechanisms (e.g. fuzzing, boundary value analysis, equivalence partitioning) using COTS tools [53] or be checked for compliance with known security guidelines like STIG (Security Technical Implementation Guides)[14] and OWASP Top Ten[15] for software and FIPS 140-3 [54] for hardware before being deployed in use.

Software-defined radios (SDRs) One of the major technology advancements made in the New Space era is SDRs, which "represent a radio that has software control over some functions, and still being partly implemented in analog electronics" [55]. Functionality traditionally implemented in hardware—filters, modulators, mixers—is now moving to software. This technology affords space systems with flexibility and reconfigurability, whilst also removing the need for dedicated hardware to save space on satellite buses. SDRs such as RTL-SDR, USRP and LimeSDR are commonly available for purchase.

This move to SDRs shows a shift between the technologies in Old Space and New Space. For Old Space, radio communications were achieved through traditional dedicated radio hardware. The relationship between satellite hardware, software and the Open Systems Interconnection (OSI) model, which abstracts communications into seven separate layers, typically falls into the one shown on the left side of Fig. 7. Hardware is used for the physical and data link layers, with software covering the other five layers and optionally the data link layer. SDRs implement functions that originally resided in hardware, but now in software, encapsulating the physical, data link and network layers, demonstrated in the right side of Fig. 7. More parts of the communications stack consist of software instead of hardware, reducing satellite reliance on hardware but opening the system to software threats. Traditional radio components have in-built limitations, such as specific frequencies and filter ranges. Trusted hardware functions are now in software, so future implementations must consider how to trust software to behave as intended and in a secure manner.

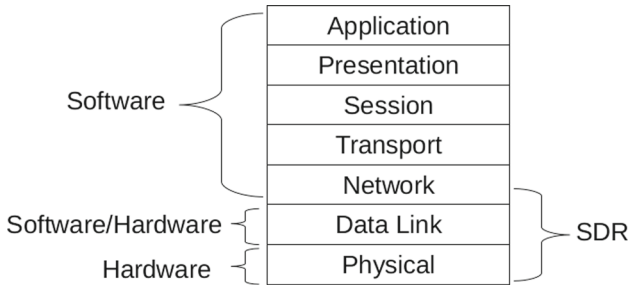


Fig. 7 OSI communication model for satellites showing relationship to SDR technology

Authentication of signals is a critical aspect of secure communication. Most mechanisms of authentication (e.g. digital signatures and certificates) exist above the physical layer, though some (e.g. spread-spectrum communications) exist at the physical layer often with an additional cost in bandwidth. The use of SDRs at physical layer has provided low-cost authentication solutions using various software techniques like fingerprint embedding where a low-power secret modulation is superimposed over the message waveform which serves as an authentication tag [56,57].

Although SDRs provide significant advantages over hardware techniques, they introduce protocol-independent software vulnerabilities into the system. In the process of securing SDRs, several integrated components have been proposed. A survey paper [58] on the security of SDRs discusses the threat model SDR faces and architectures proposed to mitigate them. Notably, a secure SDR architecture proposed [59] is composed of an automatic and calibration unit (ACU), a radio security module (RSM) and a location component based on a GNSS receiver (cf. Fig. 8). The ACU controls the output spectrum to be compliant with the local spectrum regulations. The SDR stores the information (e.g. spectrum configuration files) on the spectrum regulations in various spectrum jurisdictions in the world. The GNSS receiver in-built provides the location of the SDR at any given time; the ACU uses the location and the spectrum configuration files to determine the correct spectrum regulations.

The ACU represents a protection technique against security threat if the SDR services are related to transmission and communication of signals. Even if a malicious waveform is activated in the SDR node, the ACU can prevent it from transmitting in unauthorized bands. The RSM is responsible for download, activation and execution of the software modules. With the potential harm that malicious SDR code could cause, the veracity of the RSM functions is critical; therefore, these functions must be implemented with a suitable level of trust.

[13] https://github.com/OpenLST

[14] https://public.cyber.mil/stigs/

[15] https://owasp.org/www-project-top-ten/

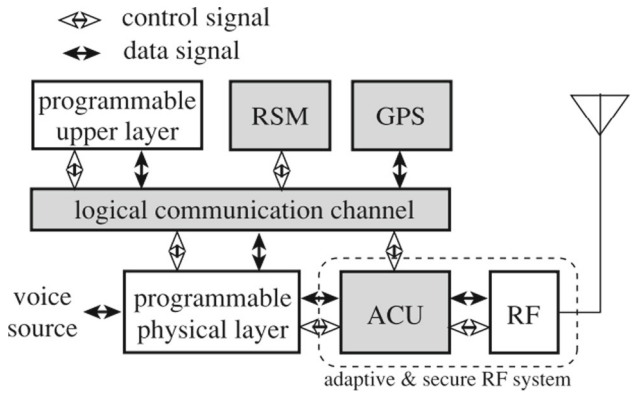


Fig. 8 ACU- and RSM-based SDR hardware architecture [59]

A popular digital signal processing software used with SDRs is GNU radio, which provides standardized signal processing blocks to implement radio communications with SDRs, either with real RF hardware or in a simulated environment. It has been used widely in academic circles (for instance in [60–63]) with some confirmed usage in the commercial sector [17,64].

SDR usage is becoming more widespread with significant numbers of "How To" guides on satellite eavesdropping with SDRs available on the Internet, e.g. [65,66] detail how to obtain weather satellite imagery using SDRs, [67] provides commentary on using an SDR to listen on transmissions from spacecraft travelling to the International Space Station (ISS), and a tutorial for decoding messages from the satellite communications provider Inmarsat is available from [68].

4.2 Ground segment

Automation and autonomy Autonomy has made great strides in the past few decades with autonomous vehicle prototypes in action and great leaps made in robotics. Autonomous operations are those in which a system performs self-regulating and self-controlling actions and have been attempted to be implemented in the ground segment since the late 1980s [69]. Strides have been taken to provide autonomy in space rovers—NASA's Curiosity rover employed autonomy in areas such as navigation and sample selection [70,71].

The ability of a ground station and mission control centre to command, control and receive payload transmissions for satellites without the need for human interaction is a desirable one. Automation helps to reduce costs but also enable scalable and complete management of potentially large numbers of satellites belonging to a constellation [72].

Experimentation of autonomous ground station and on-orbit operations has been developing, with examples provided in [72–75], reporting successful demonstrations of autonomous operations. Autonomy has also expanded to commercial interests with SpaceX releasing Starlink constellation information which states that satellites are "capable of tracking on-orbit debris and autonomously avoiding collision" [76].

Commercial interests, such as Planet, have already incorporated automated procedures in both their software and firmware development and in the satellite commissioning stages, which are expanded upon in [14]. Initially, a ground-based software process, Planet, moved to on-board commissioning software due to the unscalability of their original process for an entire constellation. Forty-seven out of 88 of its satellites were able to complete the commissioning process completely automated. Out of the 150 calibration manoeuvres for ADCS across all satellites, 110 were fully automated. Whilst not a perfect run, these automated operations allowed satellites to be commissioned by teams of 1–2 operators, reducing their involvement and increasing the efficiency of the entire process.

Cloud computing Cloud computing is a strong candidate to provide part of ground segment infrastructure, moving processing and storage away from personal computers to large data centres, accessed over the Internet. Cloud computing affords greater flexibility and availability with multiple sites for redundancy and provides an independence from location or device-type restrictions [77]. Planet's imagery data and mission control software are hosted in the cloud and customer's access imagery through web-based protocols.

From an education and amateur standpoint, networks such as the Satellite Network Open Ground Stations (SatNOGS)[16] and Global Educational Network for Satellite Operations (GENSO)[17] (no longer actively maintained), provide software and hardware details to begin tracking satellites with the use of cloud computing architecture. These implementations use client software to operate the ground station after receiving instructions through their network, with telemetry data available for access over the Internet.

Some ground station operators such as KSAT [78], who provide these capabilities for Earth-i and HawkEye 360 [79,80], have already adopted cloud-based technologies to manage customer's scheduling needs through browser-based applications [81]. RBC signals, a satellite ground station network operator, confirmed that it had plans to implement cloud-based mission control software developed by KubOS [82].

Even Amazon is transitioning into the space arena after success in ecommerce and cloud platforms, providing ground stations as a service[18]. Space sector companies such as DigitalGlobe, BlackSky, Spire Global, Capella Space and Open Cosmos are reported to be its first customers [83].

[16] https://satnogs.org/

[17] https://www.esa.int/Education/How_GENSO_work

[18] https://aws.amazon.com/ground-stat

Whilst cloud providers can guarantee some measurable non-functional performance metrics, e.g. service availability or throughput, there is lack of adequate mechanisms for guaranteeing certifiable and auditable security, trust and privacy of the applications and the data they process. For example, there exists a fragile transparency in the trustworthiness of remote satellite imagery from cloud providers because of conflicting policies between them and governments on grounds of international security [84]. Object Management Group[19] provides a list [85] of cloud security standards and certification to be expected from the providers before moving to a service. In addition to the general standards and frameworks, there are others that operate at country or regional levels or that apply to specific industries (e.g. PCI DSS) or to specific types of data (e.g. HIPAA, GDPR). It is impertinent that cloud customers continually review service provider security controls and standards to ensure they are properly defined and enforced as this is the sole security guarantee from a cloud provider.

Edge computing An abstraction of cloud computing, edge computing [86], leverages processing within a closer local network to perform operations typically performed in cloud services. This brings applications and data to a closer location to the user, reducing latency in networks.

Edge computing has been used with Internet of things (IoT) devices, especially sensors which provide readings for processing to nearby edge devices. System decisions can then be made based upon readings and then data sent to the cloud afterwards. An example of this is smart cities where sensors readings across cities provide edge devices the data to make decisions to influence transportation, energy and crime [87].

IoT devices, edge computing and satellites have already become intertwined. The Australian-based company Fleet provides a gateway device containing an edge server, satellite modem and antenna which connects to IoT devices. This gateway collects, processes and analyses sensor data and uses their satellite communications network to send only the relevant information to a business's central cloud infrastructure [88].

4.3 Space protocols and their security

Satellite communication links often suffer from higher error rates and latencies than terrestrial cabled networks and, in the case of LEO satellites, only have a small window of time to communicate whilst in range of a ground station. Communication protocols have often been lightweight to lower the resource requirements of satellites.

The CCSDS has created a set of protocols for telemetry, telecommand and OSI model layers (application, transport, etc.). Adapted to support protocols from the IP suite, CCSDS is making data communications more accessible and familiar for new enterprises in the space industry [89]. The implementation and demonstration of these protocols have been noted in over a thousand missions listed on the CCSDS website at [90], with several commercial telecommunication satellites using CCSDS command and control capabilities.

Surveys on satellite communication protocols are presented in [91,92] which summarize current protocols in use. This section aims to provide a more extensive overview into their security.

Physical One of the most widely used satellite services is satellite TV. The majority of satellite TV broadcasts is achieved using DVB[20] protocols, i.e. DVB-S, DVB-S2, DVB-SH. These physical (and data link) layer protocols standardize methods to broadcast television signals globally, and encryption can be applied on top of these transmissions. The conditional access system (DVB-CA) defines a common scrambling algorithm (DVB-CSA) and a physical common interface (DVB-CI) for accessing encrypted content. DVB-CA providers develop their wholly proprietary conditional access systems with reference to these specifications. Cryptanalysis of the common scrambling algorithm [93–95] provides intuition for the vulnerability of the algorithm to several generic attacks. However, no feasible attack against the protocol with considerable advantage has been published yet. Constellation companies Planet and LeoSat propose to use DVB protocols for imagery downlinks [14] and "both earth-to-satellite and satellite-to-earth links" [26] respectively.

Optical communications A recent development in satellite communications is the use of optical communication payloads using visible light communications (VLCs). These can provide higher data rates whilst steering clear of radio frequency electronic warfare activities such as jamming and avoiding exhausting the RF spectrum. Whilst affected by cloud coverage, making them less fitting for ground to space links, they are suitable for inter-satellite links.

Already large optical payloads have been demonstrated in satellites such as Artemis, Spot-4, Envisat Adeos-II, OICETS, Kodama, DAICHI and SDS-1 at extremely high wireless data rates [96]. NASA's Laser Communication relay [97] aims to discover whether optical communication transceivers can be built with similar mass and power requirements to a traditional RF system. Broadband constellation plans such as Starlink and LeoSat aim to use laser communications for inter-satellite links to reduce latencies in their networks.

Optical communication can be secured by quantum cryptographic techniques using QKD (cf. Sect. 4.5). A less secure

[19] https://www.omg.org/

[20] DVB, https://www.dvb.org/

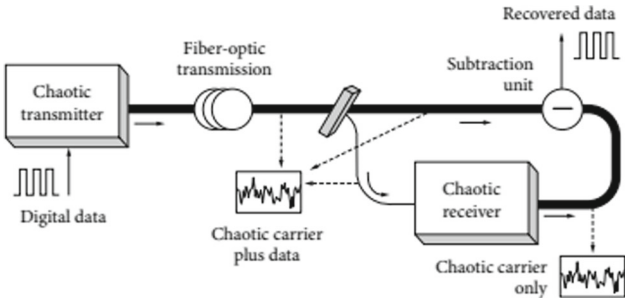


Fig. 9 An optical communication system based on chaos encryption [101]

but significantly studied in the literature method of securing communication is chaotic encryption [98–100]. It can be realized by encoding the message using chaotic carriers. The objective of chaos hardware encryption is to encode the information signal within a chaotic carrier generated by components whose physical, structural and operating parameters form the secret key. Once the information encoding has been carried out, the chaotic carrier is sent by conventional means to a receiver. Decoding of the message is then achieved directly in real time through a so-called chaos synchronization process [101]. However, chaotic cryptosystems have proven to be insecure because of the inadequacy of logistic maps used for encryption [102] (Fig. 9).

Data link Educational and small satellites have been noted to use various simplistic data link protocols, some of which were originally designed for amateur packet radio such as AX.25[21], offering data frame processing and fault detection, but not error correction. Other data link protocols such as the unified space link protocol (USLP), new satellite data link protocol (NSLP), low-altitude multiple satellite data link control (LAMS-DLC), Proximity-1 and Nanolink, detailed in [91], provide similar data framing services and varying degrees of error correction and reliability procedures, but no built-in security.

Low-impact educational missions do not immediately prompt for more complex and security-driven protocols; however, commercial enterprises such as Planet also reported using the AX.25 protocol [103]. These organizations often have greater needs for confidentiality and privacy, for which these types of lightweight protocols may not be suitable.

The CCSDS Space Data Link Security (SDLS) protocol [104] extends its data link protocols to incorporate confidentiality services through encryption of the frame data, authentication and integrity through authenticated and non-authenticated message authentication codes (MACs), respectively, and anti-replay protection through the use of sequence numbers. The scheme is designed and analysed in adherence to the security concerns mentioned in ISO 7498-2 [105]. The protocol, overall, attempts to offer confidentiality, integrity and/or authenticity of the transmitted data. However, it fails to provide guarantee against DDoS by jamming, traffic flow analysis and data substitution attack if the encryption does not use authentication.

Networking and transport Network protocols such as the Space Packet Protocol (SPP) and Delay Tolerant Network Bundle Protocol (DTN BP) allow for asynchronous data transfers, suitable for data transmission delays found in satellite communications. Broadband services commonly use IP protocols. Reliability services emerge through transport protocols. The space communications protocol specification-transport protocol (SCPS-TP) based upon TCP and Licklider Transmission Protocol (LTP) which can run over UDP or the data link offer such services. The TP stack was actually designed as a part of SCPS protocol suite, with an SP security layer, FP file transfer and NP network protocol intended to replace IPSec, FTP and IP, respectively. However, with the evolution of the Internet and supporting protocols, these other SCPS layers have become irrelevant. TCP has historically been deemed ill-fitting for space due to its bad performance [106]; however, these newer space-related protocols are designed to balance the high error rates and latency issues which lower TCP performance. Alternatively, TCP performance enhancing proxies (PEPs) are widely used to overcome the limitations of TCP over satellite links. This is known as TCP splitting [107], where each overlay hop between each PEP is considered as a new TCP connection.

IPSec provides authentication and encryption of data packets to provide secure encrypted communication between two computers over an IP network. However, TCP PEPs are not compatible with IPSec [108] as PEPs need to analyze the headers of TCP segments and IP packets between two ends to route the packets through suitable PEPs. Since IPSec tunnels mask the content of the IP packets, in particular the source and destination of data, it is impossible to implement a PEP through a IPSec tunnel. Several solutions [109–111] have been proposed to circumvent this issue by either adding additional information to the packet or selective usage of the IPSec protocol.

The CubeSat Space Protocol (CSP)[22] provides a simple design to achieve networking and transport services, which also compatible with several different physical and data link protocols. CSP includes encryption and integrity features with the use of the XTEA [112] algorithm for encryption of packets and HMAC-SHA1 [113] for message authentication. Although these algorithms have known cryptographic weaknesses [114–116] that undermine these security features, they are preferred for their lightweight operation on CubeSat's embedded systems.

[21] AX.25.net, http://www.ax25.net/Default.aspx

[22] https://github.com/libcsp/libcsp

For securing communications for the CCSDS Space Packet protocol, in [117], the use of encryption and digital signatures is prescribed to increase security. The encryption lies solely on the application data and not the header of packets, and the digital signature or an integrity check value (ICV) is appended to the end of the encrypted data. Some drawbacks appear with this implementation namely that the header remains in cleartext; this solution offers no anti-replay protection, and it may be possible to differentiate between encrypted and unencrypted packets from the header.

Application Whilst application layer protocols are usually mission dependent, we note some file transfer protocols that are currently in use: CFDP [118] developed by CCSDS and Saratoga [119] developed by SSTL[23]. Whilst Saratoga is designed to operate over IP and is suitable for short LEO satellite passes, CFDP combines functionalities from both the application and transport layers to ensure reliable file delivery over multiple types of link with minimal resource consumption.

Application layer security controls can be applied to the communication stack; however, security considerations provided at lower protocols, at the network, data link or physical layers, may be sufficient for some missions. [117] lists the transport layer security protocol and X.509 certificates [120] as a way to implement encryption and authentication controls, though the verification of certification chains renders this protocol unsuitable for space owing to long latency times whilst handshaking [121].

4.4 User segment

The user segment deals with the applications of satellite systems. Applications such as navigation, TV and communications often require dedicated hardware. Other systems use the data that these dedicated receivers collect to serve a specific product or application. For satellite TV transmissions, a dish and set-top box must be installed to receive the particular channels provided and perform subsequent tuning and decoding of transmissions for viewing. For navigation purposes, a GNSS receiver acquires signals from a constellation to determine the location of the receiver. Applications use data from GNSS receivers in mobile phones or satellite navigation devices to plan routes, e.g. Waze[24].

Alternatively, instead of consumers having the ability to receive satellite signals themselves, a satellite operator may collect all data themselves and then distribute it via terrestrial networks. Earth observation, signal intelligence, metrological and scientific applications typically make use of this. This way, customers do not need to install or buy hardware to get access to the data. Access to the data is managed by the operator, and key technologies include web APIs and customer web portals, often cloud-based, or dedicated installable software. Planet and HawkEye 360 provide various apps and APIs to access imagery and signal mapping data for customers. Scientific data may be free to access and download from the web, e.g. datasets from the International Satellite Cloud Climatology Project (ISCCP) are accessible from their website [122].

4.5 Cryptography for New Space

Novel cryptographic mechanisms are emerging in the satellite industry. Navigation message authentication (NMA) is an authentication mechanism to provide authenticity and integrity of the navigation data to the receiver. NMA can use both or either of the symmetric/asymmetric key encryption approaches to achieve this goal.

The Chips Message Robust Authentication (CHIMERA) [123] is a hybrid NMA and spreading code authentication mechanism proposed for GPS signals. It achieves NMA using asymmetric elliptic curve digital signature algorithm (ECDSA) P-224, a well-established standard. However, CHIMERA requires receivers to have occasional access, via-non-GPS channels, to provide authenticated GPS public keys and a public key infrastructure (PKI) to verify the authenticity of the key provided.

The Galileo GNSS, as part of message authentication of its public open service, will incorporate the established Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol [124] with a novel single one-way chain of cryptographic keys shared by all satellites. The TESLA protocol has low computational and communication overhead and can also support one-to-many transmissions, making it a suitable choice for GNSS. The TESLA protocol uses MAC to prove the origin and identity of a message. The key to compute the MAC, belonging to a chain generated by a one-way function, is sent some time after the message and the MAC.

In the Galileo Open Service implementation [125], different keys are transmitted to user receivers from different satellites, but the keys are still from the same chain. The keys are transmitted in the reverse order of their computation from the chain. Hence, using the one-way function, the receiver can verify that each chain key is from the same chain as the root key by recomputing the chain. However, it is impossible to predict future keys by adversaries as it is computationally hard to invert an one-way function. Cryptanalysis of the architecture shows that with current proposed parameters, combined with the use of efficient hashing hardware, it can lead to a feasible attack with significant collision probability [126]. Whilst increasing robustness of transmissions against data losses and in difficult visibility conditions, it also allows cross-authentication of neighbouring satellites.

[23] Surrey Satellite Technologies Ltd, https://www.sstl.co.uk/

[24] https://www.waze.com/

The symmetric key encryption style of TESLA eliminates the PKI requirement posted by CHIMERA. However, the main disadvantage of the scheme arises from their security condition; it requires a coarse time synchronization between the sender and the receiver. Without this assurance, the receiver cannot be certain that the navigation message has not been generated by a spoofer who received the valid signing key from the satellite signal.

Variants of TESLA protocol include μTESLA [127], *inf*-TESLA [128] and multi-level μTESLA [129] which have been proposed for wireless sensor networks to overcome the disadvantages of the TESLA protocol. Still, performance analysis has not been performed for them with respect to GNSS satellite links.

QKD allows two parties to establish a secret key with unconditional post-quantum security by making use of the fundamental laws of quantum mechanics. QKD occurs in two phases, namely the quantum phase, where quantum superimposed signals are exchanged between the two parties establishing the raw key for each party. The second phase is the classical phase, where interactive key exchange protocols are used to distil two identical strings from the raw key [130].

Optical communication networks provide ideal channels for exchange of quantum photons. However, glass in the optic fibres tends to absorb the photons, increasing the error rate of the transmitted signals. Since security bound for quantum security provides a maximum error rate of 11% for transmission [131], the use of optic fibres is limited to a distance of few hundred kilometres for appreciable security.

On the other hand, by using satellites equipped with high-quality optical links, satellite-QKD can achieve ultra-long-distance quantum communication in the 1000 km range. Hence, optical free space links are currently the most promising channel for large-scale quantum communication by use of satellites and ground stations. The usage of a satellite terminal in space makes it possible to develop quantum communication networks on a global scale [132]. Significant experimental efforts have been devoted to investigating the feasibility of satellite-based quantum communications. NanoBob [133], QEYSSat [134] and NanoQEY [135] are some key advances in quantum research to establish a practical satellite QKD system.

5 Open challenges for space and satellites

In this section, the challenges for satellite and ground segments are discussed. The security and usability of a system are often a delicate balance and require careful consideration to achieve a desired level of service for the end user. These open challenges have been categorized into two streams, security and privacy related, and data throughput and energy consumption, to reflect these conflicting needs.

Lightweight authentication and secure communications

- Most of the satellite communication protocols are designed to be lightweight to reduce power and memory requirements and increase the speed of transmissions. Broadband constellations are aiming to provide services with high data rates and low latencies. Adding security into protocols introduces an overhead into the communication stack, increasing power consumption and memory usage. Depending on the mission, this overhead may not be tolerable, so security and missions needs must be weighed in the design and decision-making process to create an acceptable risk level for the mission.
- The use of security controls also facilitates another risk factor. An attack which aims to drain a satellite's power, e.g. creating lots of resource consumption, may lead to the satellite to turn off security controls to prioritize power-saving efforts. This makes the satellite more vulnerable to other attacks such as gaining unauthorized access or eavesdropping on cleartext communications.
- Protocols for space missions are largely mission dependent. Whilst there has been attempts to document and recommend certain communication protocols, there is no consensus in the space industry in how to best implement secure communications and authentication, or which missions warrant the need for higher or lower security requirements. Security is often added as an afterthought in the protocols used in space, and some current options utilizing existing terrestrial techniques are not suitable for satellites. Even in satellite systems which use encryption, maintaining unencrypted connection for emergency situations such as satellite tumbling is important. However, communications would be in cleartext, able to be retrieved by eavesdropping on the connection.
- Physical layer security achieved through information-theoretic models provides computationally unbounded security as opposed to cryptographic protocols with computational security [136]. Reusing the physical layer features can decrease additional energy cost for security as embedded systems like CubeSats cannot afford the additional silicon area, power consumption and code space needed to perform the expensive mathematical calculations of cryptographic methodologies. Physical transmission techniques achieve security by exploiting the unpredictable features of wireless channel through artificial noise [137], jamming [138], beamforming [139], etc. However, performance analysis methods for satellite links are needed that consider realistic legitimate and eavesdropper system assumptions and non-asymptotic coding lengths before practical consumption [140].

Key management

- Scalability—Whilst it may be a straightforward task to manage the keys of a single or small cluster of satellites, large satellite constellations require a large number of keys, making scalable key management an open issue. Constellations aiming to provide high data rates, such as broadband services, will also encompass a large network of ground stations, each with their own keys. [141] presented that to provide maximum throughput for the Telesat, OneWeb and Starlink constellations, there would need to be 42, 71 and 123 ground station locations, respectively, with a varying number of antennas per station for their proposed constellation size. Whilst maximum throughput may not be the desired level, these projects will still require vast ground segment support, presenting a larger attack surface and demanding scaled and consistent security controls over all ground segment interfaces. Satellite TT&C and payload systems may require separate keys for when the user segment communicates directly with the satellite. Separate keys for TT&C, payload management and user interactions with a payload may be required. If a separate key for the payload is compromised, the TT&C keys remain unknown and this command and control link is not compromised. Inter-satellite links also add more complexity to the situation. To provide confidentiality of each inter-satellite link (ISL), a satellite requires to have another set of keys to communicate with each of its neighbours, separate from ground-to-Earth and Earth-to-ground links. All these competing key requirements compound the issue of scalable key management further.
- Group dynamics—another challenge relates to the dynamics of satellites entering and leaving a constellation. For the satellites entering and leaving the constellations, keys must be issued and revoked respectively for TT&C, payload management and for user interactions. ISLs also complicate this as it is necessary for satellite neighbours to update their keys when changes in the constellations occur. Keys will have to be issued and revoked in a flexible manner to allow for changes in constellation group dynamics.
- Key protection—transportation, satellite stacking and delayed launches provide ample opportunities to compromise satellites and their keys, as it is not possible to keep eyes on the satellite constantly. Launch failures may scatter components over a large area, which may not have been destroyed due to their radiation hardening. Sensitive information, such as cryptographic keys, may be recoverable from these components. Reliability of hardware keys under active security threats leads to the development of physical unclonable functions (PUFs) [142] and true random number generators (TRNGs) to generate cryptographic keys and IDs used for device authentication, cloning prevention, generating session keys, etc. Trusted Platform Module (TPM) [143] is an international standard to design secure hardware with integrated cryptographic keys. Device Identifier Composition Engine (DICE) [144] and SpaceTEE [48] are hardware security designs for embedded systems which offer key protection through tamper-proof hardware.
- Quantum key distribution—whilst significant advances [133–135] have been made in satellite-based quantum key derivation, there are still various technical challenges which need to be addressed. Reducing quantum signal capable satellite size without compromising accuracy, higher orbit for satellites processing quantum signal for increased global coverage and analysis of discrete variable and continuous variable QKD using metrics such as relative secret key rates, communication overheads and computing resource requirements for error correction codes are some key areas which need to be addressed to enhance an accurate signal transmission and continuous global quantum network.

Software/firmware updates Satellites manufactured in Old Space usually had long development times to guarantee that these systems would not fail. Satellites were launched which had antiquated technology aboard, which could be vulnerable to serious threats. Hardware upgrades or replacements were rarely made, and high operational quality verification of software and firmware changes delayed their installation on the space segment.

New Space has brought agile development and operational processes. The use of FGPAs and SDRs makes it possible to re-program hardware and software in orbit easily. However, updates to software, firmware, hardware, cryptographic keys and insecure algorithms may introduce vulnerabilities, either inadvertently through a legitimate transmission of the update, or through an attacker using this circumstance to purposefully inject flaws into the satellite. In the case of the space probe Phobos 2, a software update inadvertently caused the spacecraft to lose its lock on the Sun which drained power and ceased communications [145]. Being able to use techniques such as software attestation, where software is able to prove its identity and that a system is trustworthy, may be one way to resolve this issue.

Reliable software Real-time On-board Dependable Operating System (RODOS) [146] is a real-time operating system for embedded systems and was designed for application domains demanding high dependability. A reliable secure operating system must offer trusted or reliable execution of software components, memory safety, fault tolerance against both hardware and software failures and to perform in nominal mode with respect to external and internal per-

turbations. FreeRTOS achieves memory safety through an inbuilt software model checker called CBMC[25]. The program effectively reasons every execution path through a program on every input searching for assertion or memory violation. MINIX3 [26] and Kaspersky OS[27] achieves reliability through microkernel architecture, where only a minimal set of abstractions run at the highest privilege level and reincarnation servers, which replaces a fresh copies of non-responsive or crashed drivers at user space. However, critical features like live updates, crash recovery of stateful services and virtualization are still being developed and the operating systems must be repurposed and analysed for space-based mission and threats before practical use.

Secure positioning of satellites In addition to command and control of a satellite, TT&C operations also include satellite ranging where the distance between the Earth and satellite is measured. These measurements help to verify a satellite is on the correct orbit and is in the expected position, and if not, commands to alter this can be sent. In the case of a mega-constellation, due to its size, this process happens on a much larger scale and it be may be easier for an attacker to place a malicious satellite into the constellation unnoticed.

Satellites are becoming more interconnected and making use of Internet protocols similar to IoT devices. Being able to measure the position of IoT devices compliments several IoT applications, but also offers assurances that you are communicating with the correct device. This idea is important for satellite constellations as well—you want to make sure the satellite you are communicating with is the one you think it is. A rogue satellite attempting to appear legitimate, whilst communicating with the ground or other satellites correctly, cannot occupy the same physical space of another legitimate satellite, so satellite ranging and positioning can be included as part of verifying a satellite's identity.

Distance bounding mechanisms have been proposed as a way to achieve secure positioning in wireless networks [147], and satellite ranging from TT&C makes use of similar concepts. Satellite constellations could potentially make use of not only measurements from ground stations, but also from other constellation satellites through the use of their ISLs, but also maybe satellites in higher orbits such as GEO; however, further work is required to explore this issue.

Routing in ISLs The use of ISLs provides communication routes which do not rely solely on ground infrastructure, but also give rise to questions over when, where and how routes are calculated. A constellation operator must decide whether routes are static or dynamic, be calculated on-demand or pre-computed, and implemented on a centralized, decentralized or distributed platform [148]. Each of these options has operational advantages and limitations and which also impact security requirements. Centralized static routes offer fixed communication paths administered by a single authority which may provide more control over the routes but is a single point of failure with fault tolerance and network congestion issues. Distributed on-demand routing splits computations among different nodes when required which increases fault tolerance. However, it also increases the attack surface of the routing procedure as more nodes are required and an attack may be easier to propagate through a network. Several protocols for ISL routing are discussed in [149] which may offer suitable implementations for both single- and multi-layer constellations. However, more work is required to address aspects such as network resilience after satellite destruction, flexible space networking mechanisms and optimal ground segment coverage.

Distributed control As mentioned earlier, when it comes to large constellations, scalability is an ongoing challenge, not only for the space segment but also for the ground. Large constellations will likely not be able to be managed from one single site. Operations may have to be distributed over several sites, requiring coordination between sites and handover from one to the next. In addition to these aspects, establishing standardized ground station builds and security practices also compounds this issue.

Fault tolerance The space environment is a harsh one with severe thermal, radiation and vibration extremes which can affect satellite components. Radiation in particular can have a devastating effect on satellites and is why many components are radiation-hardened. Single-event upsets (SEUs), where ionizing radiation causes a change of state in a components, can cause bits to be flipped, damaging data stored on the satellite. Keys stored on the satellite may be altered due to flipped bits and render satellites unable to communicate with the ground using encryption. If cost is a factor, then regular COTS components may be favoured over their radiation-hardened counterparts. New fault-tolerant cryptographic mechanisms, e.g. [150], will be required to account for these types of challenges in the space environment.

Intelligence gathering Deducing information concerning a satellite or constellation's operation may be possible without having to view the payload data. A satellite's power consumption and orbit, as well as observations from telescopes and sensors, may be used to determine mission objectives. This may be of concern to satellites attempting to remain as covert as possible and impacts the privacy of satellite operations. For example, powering on a payload when in the vicinity of a particular region could indicate imaging or signals intelligence purposes.

Companies must register the frequencies on which their satellites operate and their orbital slots with the International

[25] https://www.cprover.org/cbmc/

[26] http://www.minix3.org/

[27] https://os.kaspersky.com/

Telecommunications Union (ITU)[28], United Nations organizations which has jurisdiction over global space activities. National organizations such as the Federal Communications Commission (FCC) in the USA also regulate spectrum usage in a national capacity. This publicly available information provides ample opportunity to listen and record RF signals in the hopes of reverse-engineering message formats. An integral part of the state sector space industry is information gathering about other nations and the physical nature of RF means this challenge is not going away.

Ground segment Attacks on the ground segment are prolific throughout the space industry's history, as seen in Sect. 3. It remains one of the easiest segments to attack, owing to the use of commonplace technologies across several industries and in consumer electronics, and to tried and tested CNE attacks which are successful in all sectors.

Network and application security, user awareness and organizational security culture are ongoing problems. Phishing campaign which installed backdoor Trojan programs is a common attack vector to gain a foothold into a network and may have played a part in other satellite compromises [151,152].

Details on open-source components are publicly available which is an advantage to an attacker in finding security vulnerabilities. Global manufacturing capabilities for COTS components provide increasing opportunities for malicious actors to alter components in the supply chain. It is therefore paramount to establish confidence in the supply chain and trust overall to ensure that satellites, ground stations and user devices are designed, built and managed by parties who are held to high security standards.

Several New Space organizations are start-ups, founded by groups of graduates with experience of developing small satellites in academic institutions. Companies such as Kepler Communications[29], IceEye[30] and Astrocast[31] hoping to tackle the New Space market are university spin-offs. University missions are a starting point for many future start-ups and are typically not designed with security in mind due to the low impact of the satellite being in-orbit. There is a risk that start-ups may continue under this same mindset, without security ingrained into design and operating practices, which could become a bigger issue government and military contracts are won.

Signal Manipulation As discussed in Sect. 3, RF communication can be manipulated. Devices and techniques such as GPS jammers and spoofers, and broadcast TV/radio signal hijacking have made signal disruption an easier undertaking. The rise in COTS and SDR products available at affordable prices and the reduction of necessary specialist knowledge have increased the ease of such attacks. Also, optical communications, whilst providing an alternate means of communication to RF, are vulnerable to manipulation through optical dazzling [153], where a target is rendered blind from a more intense source direct radiation. This is the equivalent to jamming and prevents the transmission of legitimate signals, but is reversible and temporary.

Techniques and technologies aiming to prevent these types of signal manipulation have been used in the military and government sectors and are now moving to commercial satellite systems. They include techniques such as spread-spectrum and frequency hopping, which are applied at the physical layer to make signals appear noisy or switch their frequency usage with pseudo-random sequences [154].

Intrusion detection and prevention Terrestrial-based networks employ intrusion detection and prevention systems (IDS/IPS) to monitor and respond to threats. In the New Space era, a new, similar technology will be required for satellites to observe and tackle potential attacks on-board satellites such as data protocol and RF-based attacks. This brings up questions over competing power and memory requirements and scalability issues and introduces more hardware and software, which could be vulnerable. An IDS or IPS may appear to be an easy and cheaper way to implement security for satellite operators but should not be a replacement for secure design and development of satellite systems.

User segment interface Applications of New Space satellite systems provide new ways for users to interact with these services. Whether interacting directly with a receiver or accessing a service through software or web portals, several challenges arise on how to deliver these services in a secure manner. Authorization and access control play a large part in securing a system. For dedicated receivers, e.g. satellite phones, access to the service or data should not rely solely on access to the device itself. Similarly for software or web-based solutions, just because a system expects a particular format for a user to interact with it does not mean that it cannot be abused, especially if these types of systems support on-demand services to reconfigure payloads or direct satellites. Verification of a user's identity and their level of access do not always go hand-in-hand when designing any system and a major challenge is ensuring robust enough authentication and authorization controls whilst minimally impacting usability.

6 Conclusion

Key advancements are being made in the space and satellite industry. Private sector investment in existing companies and

[28] https://www.itu.int/en/Pages/default.aspx

[29] https://www.keplercommunications.com/company/about

[30] https://www.iceye.com/

[31] https://www.astrocast.com/

new start-ups is driving innovation and ingenuity, in technology and also the applications of satellites. Satellite applications have a diverse nature and cross boundaries of state, military, commercial and civilian sectors. A review of past attacks on the space industry revealed attacks mainly focused on the ground segment or electronic warfare activities, for espionage and political activities. However, constellations of thousands of satellites are planned for launch in the upcoming years, making commercial satellites a much more attractive target by adversaries with a multitude of motivations and capabilities.

Advancements in technologies such as COTS components, SDRs and cloud computing were discussed, and their resulting impact on security of the industry. Many challenges and open design problems relating to both security and operational requirements are still to be resolved. An overview of issues facing secure communication practices, privacy, supporting terrestrial systems and the user segment is provided.

Funding This research has been funded by the NCC Group.

Compliance with ethical standards

Conflict of Interest All authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

References

1. Bryce Space and Technology: State of the Satellite Industry Report 2018. Resreport (2018). https://brycetech.com/downloads/SIA_SSIR_2018.pdf. Accessed 17 April 2019
2. Sweeting, M.N.: Modern small satellites-changing the economics of space. Proc. IEEE **106**(3), 343–361 (2018)
3. Paikowsky, D.: What is new space? the changing ecosystem of global space activity. New Space **5**(2), 84–88 (2017)
4. Bryce Space and Technology: Smallsats by the Numbers 2019. Technical report (2019). https://brycetech.com/download.php?f=downloads/Bryce_Smallsats_2019.pdf. Accessed 02 April 2019
5. Bryce Space and Technology: State of the Satellite Industry Report 2017. Resreport (2017). https://brycetech.com/downloads/SIA_SSIR_2017.pdf. Accessed 17 April 2019
6. Parliamentary Office for Science and Technology: Postnote: Military users of space. https://www.parliament.uk/documents/post/postpn273.pdf. Accessed 16 May 2019
7. Forest, B.D.: An Analysis of Military Use of Commercial Satellite Communications. Master's thesis, Naval Postgraduate School (Sep 2008)
8. White House: U.S. National Space Policy (Aug 2006). https://fas.org/irp/offdocs/nspd/space.pdf. Accessed 25 May 2019
9. Santamarta, R.: A Wake-up Call for SATCOM Security. Technical White Paper (2014). https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf. Accessed 23 May 2019
10. Santamarta, R.: Last Call for SATCOM Security. Technical White Paper (Aug 2018). https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf. Accessed 23 May 2019
11. Falco, G.: Cybersecurity principles for space systems. J. Aerosp. Inf. Syst. **16**(2), 61–70 (2019)
12. Space mission analysis and design. Space technology library; v.8, Microcosm ; Kluwer Academic, Torrance, Calif.: Dordrecht; London, 3rd ed./edited by james r. wertz and wiley j. larson. edn. (1999)
13. Swpb: Simplified diagram of segments of a satellite system. https://commons.wikimedia.org/wiki/File:Ground_segment.png (2016). https://commons.wikimedia.org/wiki/File:Ground_segment.png. Accessed 16 May 2019
14. Zimmerman, R., Doan, D., Leung, L., Mason, J., Parsons, N., Shahid, K.: Commissioning the world's biggest satellite constellation. In: 31st Annual AIAA/USU Conference on Small Satellites. No. SSC17-X-03 in Year in Review (2017). https://digitalcommons.usu.edu/smallsat/2017/all2017/. Accessed 17 Apr 2019
15. Kyle Colton, B.K.: Supporting the Flock: Building a Ground Station Network for Autonomy and Reliability. In: 30th Annual AIAA/USU Conference on Small Satellites. No. SSC16–IX–05 (2016)
16. CaJacob, D., McCarthy, N., O'Shea, T., McGwier, R.: Geolocation of RF emitters with a formation-flying cluster of three microsatellites. In: 30th annual AIAA/USU conference on small satellites. No. SSC16-VI-5 in Next on the Pad (2016). https://digitalcommons.usu.edu/smallsat/2016/all2016/. Accessed 17 Apr 2019
17. Sarda, K., Roth, N., Zee, R., CaJacob, D., Orr, N.G.: Making the Invisible Visible: precision RF-Emitter Geolocation from Space by the HawkEye 360 Pathfinder Mission. In: 32nd Annual AIAA/USU Conference on Small Satellites (2018)
18. Graham, W.: SpaceX launches Falcon 9 with PAZ, Starlink demo and new fairing (Feb 2018). https://www.nasaspaceflight.com/2018/02/spacex-falcon-9-paz-launch-starlink-demo-new-fairing/. Accessed 14 Jun 2019
19. SpaceX: Starlink Mission (May 2019), https://www.spacex.com/news/2019/05/24/starlink-mission. Accessed 14 Jun 2019
20. Space Exploration Holdings LLC: SpaceX Non-Geostationary Satellite System—Attachment A. http://licensing.fcc.gov/myibfs/download.do?attachment_key=1158350 (Nov 2016). Accessed 30 May 2019
21. Henry, C.: SpaceX to Launch 'Dozens' of Starlink Satellites Next Week, More to Follow (May 2019). https://www.space.com/spacex-starlink-satellites-launching-may-2019.html. Accessed 14 Jun 2019
22. OneWeb: OneWeb Satellites. https://onewebsatellites.com/about-us/. Accessed 26 Feb 2019
23. Hughes Network Systems: Hughes Ships First Gateways for the Ground Network to Support OneWeb's Low Earth Orbit

Constellation (Mar 2018). https://www.prnewswire.com/news-releases/hughes-ships-first-gateways-for-the-ground-network-to-support-onewebs-low-earth-orbit-constellation-300612885.html. Accessed 14 Jun 2019
24. GMV: OneWeb awards GMV the Contract to Develop OneWeb's Satellite Constellation Command and Control (Dec 2016). https://www.gmv.com/en/Company/Communication/News/2016/12/satelites_oneweb.html. Accessed 14 Jun 2019
25. Thales Alenia Space: Optical communications (2017). https://artes.esa.int/sites/default/files/PM02TASFRESAWS-July_12th_2017_final.pdf. Accessed 15 Jun 2019
26. LeoSat: LeoSat Non-Geostationary Satellite System—Attachment A. licensing.fcc.gov/myibfs/download.do?attachment_key=1158225. Accessed 15 Jun 2019
27. Book, G.: Security threats against space missions
28. Martin, P.K.: NASA Cybersecurity: An Examination of the Agency's Information Security. Testimony before the Subcommittee on Investigations and Oversight (Feb 2012). https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf. Accessed 23 May 2019
29. Google cloud networking incident #19020. https://status.cloud.google.com//incident/cloud-networking/19020, Accessed 24 Feb 2020
30. Nichols, S.: Aws's s3 outage was so bad Amazon couldn't get into its own dashboard to warn the world (Mar 2017). https://www.theregister.co.uk/2017/03/01/aws_s3_outage/. Accessed 24 Feb 2020
31. Bielawski, R.: Space as a new category of threats to national security. Saf. Def. **5**(2), 1–7 (2019)
32. Society, R.A.: Eavesdropping from space. https://www.aerosociety.com/news/eavesdropping-from-space/. Accessed 24 Feb 2020
33. Franceschi-Bicchierai, L.: This 1000 USD device lets hackers hijack satellite communications. https://motherboard.vice.com/en_us/article/xywjpa/this-1000-device-lets-hackers-hijack-satellite-communications. Accessed 12 Feb 2019
34. Knittel, C.: The mystery of the creepiest television hack. https://www.vice.com/en_us/article/pgay3n/headroom-hacker. Accessed 24 Feb 2020
35. Kand, W., Chen, S., Pan, A.: Is Your Timespace Safe?—Time and Position Spoofing Opensourcely. In: BlackHat EU 2015 (2015). https://www.blackhat.com/docs/eu-15/materials/eu-15-Kang-Is-Your-Timespace-Safe-Time-And-Position-Spoofing-Opensourcely-wp.pdf. Accessed 14 July 2019
36. Lied, H.: Gps freaking out? maybe you're too close to putin. https://web.archive.org/web/20170925202637/https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/. Accessed 12 Feb 2019
37. Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B., Capkun, S.: On the requirements for successful gps spoofing attacks. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, pp. 75–86. CCS '11, Association for Computing Machinery, New York, NY, USA (2011). https://doi.org/10.1145/2046707.2046719
38. Broumandan, A., Lachapelle, G.: Spoofing detection using GNSS/INS/Odometer coupling for vehicular navigation. Sensors **18**(5), 1305 (2018). https://doi.org/10.3390/s18051305
39. Hitefield, S.: Exploiting Vulnerabilities in Software Radios. In: GRCon 2016 (2016). https://www.youtube.com/watch?v=bN4IN4EGhDg
40. Lee, M., Choi, G., Park, J., Cho, S.J.: Study of analyzing and mitigating vulnerabilities in UC/OS real-time operating system, pp. 834–836 (07 2018)
41. U.S. Government: Report to Congress of the U.S.-China Economic and Security Review Commission (2011). https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf. Accessed 12 Feb 2019
42. Committee on National Security Systems: Cyber Security Policy for Space Systems Used to Support National Security Missions (Feb 2018). https://www.cnss.gov/CNSS/openDoc.cfm?FLUClyvgO4ap6BbupiliBw==. Accessed 14 July 2019
43. Sims, E.M., Braun, B.M.: Navigating the Policy Compliance Roadmap for Small Satellites (Nov 2017). https://aerospace.org/sites/default/files/2018-05/SmallSatRegulations_0.pdf. Accessed 14 Jun 2019
44. Russell, K.: Evolving Cybersecurity in the NewSpace Era (Apr 2018). http://interactive.satellitetoday.com/via/april-2018/evolving-cybersecurity-in-the-newspace-era/. Accessed 14 Jun 2019
45. Musk, E.: Twitter.com: End-to-end encryption encoded at firmware level. https://twitter.com/elonmusk/status/967728299282595840?lang=en. Accessed 08 Feb 2019
46. Kaspersky: Satellite Turla: still alive and hiding in the sky. https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf. Accessed 15 May 2019
47. JSR: Number of active satellites from 1957 to 2018. Statista Inc., https://www.statista.com/statistics/897719/number-of-active-satellites-by-year/. Accessed 09 July 2019
48. Michalevsky, Y., Winetraub, Y.: Spacetee: Secure and tamper-proof computing in space using cubesats. CoRR arXiv:1710.01430 (2017). http://arxiv.org/abs/1710.01430
49. Grieve, J.A., Bedington, R., Tang, Z., Chandrasekara, R.C., Ling, A.: Spooqysats: cubesats to demonstrate quantum key distribution technologies. Acta Astronaut. **151**, 103–106 (2018). https://doi.org/10.1016/j.actaastro.2018.06.005
50. Hanafi, A., Karim, M., Latachi, I., Rachidi, T., Dahbi, S., Zouggar, S.: FPGA-based secondary on-board computer system for low-earth-orbit nano-satellite. In: International Conference on Advanced Technologies for Signal and Image Processing, pp. 1–6 (May 2017)
51. Bartram, P., Bridges, C., Bowman, D., Shirville, G.: Software defined radio baseband processing for ESA ESEO Mission. In: 2017 IEEE aerospace conference. IEEE (2017). http://epubs.surrey.ac.uk/813289/. Accessed 15 May 2019
52. Cybersecurity, Agency, I.S.: Security considerations in managing cots software. https://www.us-cert.gov/bsi/articles/best-practices/legacy-systems/security-considerations-in-managing-cots-software. Accessed 26 Feb 2020
53. Cybersecurity, Agency, I.S.: Black box security testing tools. https://www.us-cert.gov/bsi/articles/tools/black-box-testing/black-box-security-testing-tools. Accessed 26 Feb 2020
54. Security requirements for cryptographic modules: technical teport (2019). https://doi.org/10.6028/nist.fips.140-3
55. Center for Software Defined Radio: Software Defined Radio Terms, Trends and Perspectives. resreport (Jan 2007)
56. Paul, L.Y., Baras, J.S., Sadler, B.M.: Physical-layer authentication. IEEE Trans. Inf. Forensics Secur. **3**(1), 38–51 (2008)
57. Verma, G., Yu, P., Sadler, B.M.: Physical layer authentication via fingerprint embedding using software-defined radios. IEEE Access **3**, 81–88 (2015)
58. Baldini, G., Sturman, T., Biswas, A.R., Leschhorn, R., Godor, G., Street, M.: Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead. IEEE Commun. Surv. Tutor. **14**(2), 355–379 (2012)
59. Sakaguchi, K., Lam, C.F., Doan, T., Takada, J.I., Araki, K.: ACU and RSM based radio spectrum management for realization of flexible software defined radio world. IEICE Trans. Commun. **86**(12), 3417–3424 (2003)
60. Maheshwarappa, M.R., Bridges, C.: Software Defined Radios for Small Satellites. In: 2014 NASA/ESA Conference on Adaptive Hardware and Systems (AHS). pp. 172–179 (07 2014)

61. Pinto, F., Afghah, F., Radhakrishnan, R., Edmonson, W.: Software Defined Radio implementation of DS-CDMA in inter-satellite communications for small satellites. In: 2015 IEEE WiSEE, pp. 1–6 (Dec 2015)
62. Velasco, C., Tipantuña, C.: Meteorological picture reception system using software defined radio (SDR). In: 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), pp. 1–6 (Oct 2017)
63. Pei, Y., Chen, H., Pei, B.: Implementation of GPS Software Receiver Based on GNU Radio. In: Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC). pp. 1–3 (July 2018)
64. Janicik, J., Wolff, J., Friedman, A.: Cybersecurity in Modern Spacecraft Operations. In: Proceedings of the 28th Annual AIAA/USU Conference on Small Satellites,. No. SSC14-P4-5 in Poster Session (2014). https://digitalcommons.usu.edu/cgi/viewcontent.cgi?filename=0&article=3128&context=smallsat&type=additional
65. Dillon, H.: Receiving weather satellite images with Softrock. http://www.alternet.us.com/?p=1398. Accessed 30 Jan 2019
66. Baguley, R.: Full Earth Disc Images From GOES-17 Harvested By SDR (2019). https://hackaday.com/2019/05/03/full-earth-disc-images-from-goes-17-harvested-by-sdr/. Accessed 14 Jun 2019
67. Maloney, D.: Eavesdropping On Cosmonauts With An SDR (Mar 2019). https://hackaday.com/2019/03/28/eavesdropping-on-cosmonauts-with-an-sdr/#more-350387. Accessed 14 Apr 2019
68. rtl-sdr.com: RTL-SDR Tutorial: decoding Inmarsat STD-C EGC Messages (Aug 2015). https://www.rtl-sdr.com/rtl-sdr-tutorial-decoding-inmarsat-std-c-egc-messages/. Accessed 15 May 2019
69. Chweh, C.: Autonomy in space. IEEE Intell. Syst. Their Appl. **13**(5), 78–80 (1998)
70. NASA.gov: Mars exploration rovers—mobility. https://mars.nasa.gov/mer/mission/technology/autonomous-planetary-mobility/. Accessed 08 May 2019
71. Webster, G., Brown, D., Cantillo, L.: Nasa mars rover can choose laser targets on its own. https://mars.nasa.gov/news/nasa-mars-rover-can-choose-laser-targets-on-its-own/. Accessed 08 May 2019
72. Obata, T., Nakasuka, S., Aoyanagi, Y., Matsumoto, T., Shirasaka, S.: On-Orbit Demonstrations of Robust Autonomous Operations on CubeSat. In: 32nd Annual AIAA/USU Conference on Small Satellites. No. SSC18-WKX-02 in A Look Back: Lessons Learned (2018)
73. Kennedy, A.K., Cahoy, K.L.: Initial Results from ACCESS: An Autonomous CubeSat Constellation Scheduling System for Earth Observation. In: 31st Annual AIAA/USU Conference on Small Satellites. No. SSC18-X-03 in Ground Systems (2017)
74. Ogilvie, A., Allport, J., Hannah, M., Lymer, J.: Autonomous Satellite Servicing Using the Orbital Express Demonstration Manipulator System. In: 9th International Symposium on Artificial Intelligence, Robotics and Automation in Space (01 2008)
75. NASA: Cubesat Proximity Operations Demonstration (Mar 2016). https://www.nasa.gov/sites/default/files/atoms/files/cpod_fact_sheet-7march2016.pdf. Accessed 29 May 2019
76. SpaceX: Starlink mission overview (May 2019). https://www.spacex.com/sites/spacex/files/starlink_press_kit.pdf. Accessed 08 Feb 2019
77. Tepe, A., Yilmaz, G.: A survey on cloud computing technology and its application to satellite ground systems. In: 2013 6th International Conference on Recent Advances in Space Technologies (RAST), pp. 477–481 (June 2013)
78. Kongsberg: KSAT. https://www.kongsberg.com/ksat/. Accessed 01 April 2019
79. Earth-i: Earth-i to use KSAT's Ground Stations to Receive First Commercial Full-Colour Video From Space (Dec 2017). https://earthi.space/press/earth-i-use-ksats-ground-stations-receive-first-commercial-full-colour-video-space/. Accessed 01 April 2019
80. HawkEye 360: HawkEye 360 Selects Norway's Kongsberg Satellite Service (KSAT) to Provide Ground Station Services for Pathfinder Mission (Apr 2018). https://www.he360.com/hawkeye-360-selects-norways-kongsberg-satellite-service-ksat-to-provide-ground-station-services-for-pathfinder-mission/. Accessed 01 April 2019
81. Thrana, S.A.: Innovative NewSpace Ground Segment—Global Coverage Available through the Cloud. In: 30th Annual AIAA/USU Conference on Small Satellites. No. SSC16–VII–07 (2016)
82. Signals, R.: RBC Signals Announces New Integration Agreement with Kubos. http://rbcsignals.com/rbc-signals-announces-new-integration-agreement-with-kubos/. Accessed 29 May 2019
83. Shah, S.: AWS Ground Station first customers include DigitalGlobe, BlackSky and Spire (Nov 2018). https://www.computing.co.uk/ctg/news/3067137/aws-ground-station-first-customers-include-digitalglobe-blacksky-and-spire. Accessed 01 April 2019
84. Witjes, N., Olbrich, P.: A fragile transparency: satellite imagery analysis, non-state actors, and visual representations of security. Sci. Pub. Policy **44**(4), 524–534 (2017). https://doi.org/10.1093/scipol/scw079
85. Council, C.S.C.: Cloud security standards: what to expect and what to negotiate version 2.0. https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf. Accessed 26 Feb 2020
86. Wikipedia.com: Edge computing. https://en.wikipedia.org/wiki/Edge_computing. Accessed 25 Jun 2019
87. Musa, S.: Smart City Roadmap. https://www.academia.edu/21181336/Smart_City_Roadmap. Accessed 25 May 2019
88. Fleet Space Technologies: Fleet Portal. https://www.fleet.space/portal. Accessed 15 May 2019
89. The Consultative Committee for Space Data Systems: Overview of Space Communications Protocols. techreport 130.0-G-3, The Consultative Committee for Space Data Systems (Jul 2014). https://public.ccsds.org/Pubs/130x0g3.pdf
90. The Consultative Committee for Space Data Systems: CCSDS Missions. https://public.ccsds.org/implementations/missions.aspx. Accessed 30 May 2019
91. Davoli, F., Kourogiorgas, C., Marchese, M., Panagopoulos, A., Patrone, F.: Small satellites and CubeSats: survey of structures, architectures, and protocols. Int. J. Sate. Commun. Netw. (09 2018)
92. Burleigh, S.C., Cola, T.D., Morosi, S., Jayousi, S., Cianca, E., Fuchs, C.: from connectivity to advanced internet services: a comprehensive review of small satellites communications and networks. Wirele. Commun. Mob. Comput. **20192019**, 1–17 (2019)
93. Weinmann, R.P., Wirt, K.: Analysis of the DVB common scrambling algorithm. In: Chadwick, D., Preneel, B. (eds.) Communications and Multimedia Security, pp. 195–207. Springer, Boston (2005)
94. Simpson, L., Henricksen, M., Yap, W.S.: Improved cryptanalysis of the common scrambling algorithm stream cipher. In: Proceedings of the 14th Australasian Conference on Information Security and Privacy, pp. 108–121. ACISP '09, Springer, Berlin (2009). https://doi.org/10.1007/978-3-642-02620-1_8
95. Tews, E., Wälde, J., Weiner, M.: Breaking DVB-CSA. In: Armknecht, F., Lucks, S. (eds.) Research in Cryptology, pp. 45–61. Springer, Berlin (2012)
96. Muri, P., McNair, J.: A survey of communication sub-systems for intersatellite linked systems and cubesat missions. J. Commun 7 (04 2012)

97. NASA: Laser Communications Relay Demonstration (LCRD) Overview. https://www.nasa.gov/mission_pages/tdm/lcrd/overview.html. Accessed 30 May 2019
98. Liu, Jm, Chen, Hf, Tang, S.: Synchronized chaotic optical communications at high bit rates. IEEE J. Quantum Electron. **38**(9), 1184–1196 (2002)
99. Heil, T., Mulet, J., Fischer, I., Mirasso, C.R., Peil, M., Colet, P., Elsasser, W.: On/off phase shift keying for chaos-encrypted communication using external-cavity semiconductor lasers. IEEE J. Quantum Electron. **38**(9), 1162–1170 (2002)
100. Jiang, N., Zhao, A., Xue, C., Tang, J., Qiu, K.: Physical secure optical communication based on private chaotic spectral phase encryption/decryption. Opt. Lett. **44**(7), 1536–1539 (2019)
101. Argyris, A., Syvridis, D.: Chaos Applications in Optical Communications, pp. 479–510. Springer, Berlin (2010). https://doi.org/10.1007/978-3-642-04117-4_25
102. Arroyo, D., Alvarez, G., Fernandez, V.: On the inadequacy of the logistic map for cryptographic applications. arXiv:0805.4355 (2008)
103. EO Portal Directory: Flock 1. https://directory.eoportal.org/web/eoportal/satellite-missions/f/flock-1. Accessed 17 May 2019
104. The Consultative Committee for Space Data Systems: Space Data Link Security Protocol. Technical Report. CCSDS 355.0-B-1 (Sep 2015)
105. Iso 7498-2:1989 (2000). https://www.iso.org/standard/14256.html
106. Wang, R., Taleb, T., Jamalipour, A., Sun, B.: Protocols for reliable data transport in space internet. IEEE Commun. Surv. Tutor. **11**(2), 21–32 (2009)
107. Kopparty, S., Krishnamurthy, S., Faloutsos, M., Tripathi, S.: Split TCP for mobile ad hoc networks. pp. 138–142 vol. 1 (12 2002)
108. Gregory Totsline: Issues when using ipsec over geosynchronous satellite links (2002). https://www.sans.org/reading-room/whitepapers/vpns/issues-ipsec-geosynchronous-satellite-links-770. Accessed 26 Feb 2020
109. Demirel, D., Alagoz, F., Çağlayan, M.: Ipsec over satellite links: A new flow identification method. vol. 2006, pp. 140–145 (01 2006)
110. Djeddai, L., Liu, R.K.: Ipsecopep: Ipsec over peps architecture, for secure and optimized communications over satellite links. In: 2016 7th IEEE international conference on software engineering and service science (ICSESS). pp. 264–268. IEEE (2016)
111. Bhutta, M.N.M., Cruickshank, H.: A new dynamic multilayer IPSec protocol. In: Pillai, P., Shorey, R., Ferro, E. (eds.) Personal Satellite Services, pp. 119–129. Springer, Berlin (2013)
112. Needham, R.M., Wheeler, D.J.: Tea Extensions. Report Cambridge University, Cambridge (1997)
113. Krawczyk, H., Bellare, M., Canetti, R.: RFC2104: HMAC: Keyed-hashing for message authentication (1997)
114. Ko, Y., Hong, S., Lee, W., Lee, S., Kang, J.S.: Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST. In: FSE, pp. 299–316. Springer (2004)
115. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full sha-1. In: Shoup, V. (ed.) CRYPTO, pp. 17–36. Springer, Berlin (2005)
116. Lu, J.: Related-key rectangle attack on 36 rounds of the XTEA block cipher. IJIS **8**(1), 1–11 (2009). https://doi.org/10.1007/s10207-008-0059-9
117. The Consultative Committee for Space Data Systems: The Application of Security to CCSDS Protocols. Technical Report CCSDS 350.0-G-3 (2019)
118. The Consultative Committee for Space Data Systems: CCSDS File Delivery Protocol. techreport 727.0-B-4, The Consultative Committee for Space Data Systems (Jan 2007)
119. Wood, L.: Saratoga: scalable, speedy data delivery for sensor networks. CoRR arXiv:1204.3263 (2012)
120. Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S.: Rfc3647: Internet x.509 public key infrastructure certificate policy and certification practices framework (2003)
121. Jiang, C., Wang, X., Wang, J., Chen, H., Ren, Y.: Security in space information networks. IEEE Commun. Mag. **53**(8), 82–88 (2015)
122. International Satellite Cloud Climatology Project: ISCCP Data Access. https://www.ncdc.noaa.gov/isccp/isccp-data-access. Accessed 03 April 2019
123. Anderson, J.M., Carroll, K.L., DeVilbiss, N.P., Gillis, J.T., Hinks, J.C., O'Hanlon, B.W., Rushanan, J.J., Scott, L., Yazdi, R.A.: 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). Institute of Navigation (2017). https://doi.org/10.33012/2017.15206
124. Perrig, A., Canetti, R., D. Tygar, J., Song, D.: The TESLA broadcast authentication protocol. RSA CryptoBytes 5 (11 2002)
125. Fernandez-Hernandez, I., Rijmen, V., Seco-Granados, G., Simón, J., Rodríguez, I., Calle, J.D.: A navigation message authentication proposal for the Galileo open service. Navigation. J. Instit. Navig. 63 (03 2016)
126. Caparra, G., Sturaro, S., Laurenti, N., Wullems, C.: 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). IEEE (2016). https://doi.org/10.1109/icl-gnss.2016.7533685
127. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: Spins: security protocols for sensor networks. Wirel. Netw. **8**(5), 521–534 (2002)
128. Câmara, S., Anand, D., Pillitteri, V., Carmo, L.: Multicast delayed authentication for streaming synchrophasor data in the smart grid. In: ICT systems security and privacy protection, pp. 32–46. Springer (2016). https://doi.org/10.1007/978-3-319-33630-5_3
129. Liu, D., Ning, P.: Multilevel μTESLA: broadcast authentication for distributed sensor networks. ACM Trans. Embed. Comput. Syst. **3**(4), 800–836 (2004). https://doi.org/10.1145/1027794.1027800
130. Scheidl, T., Handsteiner, J., Rauch, D., Ursin, R.: Space-to-ground quantum key distribution. In: Karafolas, N., Sodnik, Z., Cugny, B. (eds.) International Conference on Space Optics—ICSO 2018. SPIE (Jul 2019). https://doi.org/10.1117/12.2535987
131. Sheridan, L., Scarani, V.: Security proof for quantum key distribution using qudit systems. Phys. Rev. A **82**(3), 030301 (2010)
132. Lee, O., Vergoossen, T., Ling, A.: An updated analysis of satellite quantum-key distribution missions. arXiv:1909.13061 (2019)
133. Kerstel, E., Gardelein, A., Barthelemy, M., Fink, M., Joshi, S.K., Ursin, R., Team, C., et al.: Nanobob: a cubesat mission concept for quantum communication experiments in an uplink configuration. EPJ Quantum Technol. **5**(1), 6 (2018)
134. Podmore, H., Souza, I., Hudson, D., Jennewin, T., Cain, J., Higgins, B., Midwinter, C., Scott, A., Mccolgan, A., Caldwell, D., Zheng, S.H.: Optical terminal for Canada's quantum encryption and science satellite (QEYSSat) (10 2019)
135. Jennewein, T., Grant, C., Choi, E., Pugh, C., Holloway, C., Bourgoin, J., Hakima, H., Higgins, B., Zee, R.: The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite. In: Gruneisen, M.T., Dusek, M., Rarity, J.G., Lewis, K.L., Hollins, R.C., Merlet, T.J., Toet, A. (eds.) Emerging Technologies in Security and Defence II: and Quantum-Physics-based Information Security III. SPIE (Oct 2014). https://doi.org/10.1117/12.2067548
136. Bloch, M., Barros, J., Rodrigues, M.R.D., McLaughlin, S.W.: Wireless information-theoretic security. IEEE Trans. Inf. Theory **54**(6), 2515–2534 (2008). https://doi.org/10.1109/tit.2008.921908

137. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. IEEE Trans Wirel. Commun. **7**(6), 2180–2189 (2008)
138. Ma, S., Hempel, M., Yang, Y.L., Sharif, H.: An approach to secure wireless communications using randomized eigenvector-based jamming signals. In: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference. pp. 1172–1176. IWCMC '10, Association for Computing Machinery, New York, NY, USA (2010). https://doi.org/10.1145/1815396.1815665
139. Mukherjee, A., Swindlehurst, A.L.: Robust beamforming for security in mimo wiretap channels with imperfect CSI. IEEE Trans. Signal Process. **59**(1), 351–361 (2011). https://doi.org/10.1109/TSP.2010.2078810
140. Vazquez-Castro, A., Hayashi, M.: Physical layer security for RF satellite channels in the finite-length regime. IEEE Trans. Inf. Forensics Secur. **14**(4), 981–993 (2019). https://doi.org/10.1109/tifs.2018.2868538
141. del Portillo, I., Cameron, B.G., Crawley, E.F.: A Technical Comparison of Three Low Earth Orbit Satellite Constellation Systems to Provide Global Broadband. In: 2018 International Aeronautical Conference. IAF (2018)
142. Plaga, R., Koob, F.: A formal definition and a new security mechanism of physical unclonable functions. Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance p. 288–301 (2012). https://doi.org/10.1007/978-3-642-28540-0_24
143. Group, T.C.: Trusted platform module (tpm) 2.0 (2015). https://www.trustedcomputinggroup.org/wp-content/uploads/TPM-2.0-A-Brief-Introduction.pdf. Accessed 16 June 2019
144. England, P., Aigner, R., Kane, K., Marochko, A., Mattoon, D., Spiger, R., Thom, S., Zaverucha, G.: Device identity with dice and riot: keys and certificates. Technical report. MSR-TR-2017-41 (September 2017). https://www.microsoft.com/en-us/research/publication/device-identity-dice-riot-keys-certificates/. Accessed 21 June 2019
145. Dr. Edwin V. Bell, I.: Phobos project information. https://nssdc.gsfc.nasa.gov/planetary/phobos.html. Accessed 04 Mar 2019
146. Montenegro, S., Dannemann, F.: Rodos—real time kernel design for dependability pp. 66– (05 2009)
147. Capkun, S., Hubaux, J.: Secure positioning in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 221–232 (2006)
148. Franck, L., Maral, G.: Routing in networks of intersatellite links. IEEE Trans. Aerosp. Electron. Syst. **38**(3), 902–917 (2002)
149. Qi, X., Ma, J., Wu, D., Liu, L., Hu, S.: A survey of routing techniques for satellite networks. J. Commun. Inf. Netw. **1**(4), 66–85 (2016)
150. Banu, R., Vladimirova, T.: On-board encryption in earth observation small satellites. In: 40th international carnahan conference on security technology, pp. 203–208. IEEE (2006)
151. Epstein, K., Elgin, B.: Network Security Breaches Plague NASA (Nov 2008). https://www.kepstein.com/2008/11/20/network-security-breaches-plague-nasa/. Accessed 29 May 2019
152. Paganini, P.: Fancy Bear Hackers use a new Mac Trojan against aerospace industry (Sep 2016). https://www.cyberdefensemagazine.com/fancy-bear-hackers-use-a-new-mac-trojan-against-aerospace-industry/. Accessed 29 May 2019
153. Butt, Y.: Effects of chinese laser ranging on imaging satellites. Sci. Glob. Secur. **17**, 20–35 (2009). 06
154. Wong, T.F.: Introduction to Spread Spectrum Communications. http://wireless.ece.ufl.edu/twong/Notes/CDMA/ch2.pdf. Accessed 30 May 2019