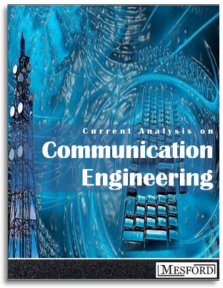

Cybersecurity Considerations for Internet of Things Small Satellite Systems

David Bird*

British Computer Society, London, UK.

Abstract:

Background: Today's Internet of Things capabilities provide low data-rate technologies that disseminate data from the front-end sensors to back-end processors. Increasingly satellites are becoming a credible alternative bearer to augment terrestrial networks utilized by the Internet of Things. However, cyber-attacks against Ground and Space Segments could arise as a follow-on from many years of encountering terrestrial critical national infrastructure threats. Vulnerabilities have been exposed by researchers within some satellite terminal equipment utilized by the User Segment and some previous cases of larger satellite malfunctions in the past may have been attributed to cyber threats targeting the Space Segment. Ground Segment weaknesses may be able to be exploited by hacker groups determined to embark on nefarious objectives against either the command and control element or effect attacks against upstream and downstream data links serviced by the Space Segment.

Objective: Therefore, cybersecurity is becoming more relevant for the Internet of Things small satellite systems agenda. There are assertions that satellites are secure and resilient but in this age of heightened cyber threats traditional perspectives of satellite security can now be overturned. All Segments are explored in relation to Internet of Things small satellite communications and connectivity perspectives. This article challenges misinterpretations from the legacy status quo relating to traditional commercial satellite communication methods. Communications paths that potentially offer exploitable vulnerabilities or weaknesses to hackers.

Conclusion: The aspiration for using Internet of Things satellite communication paths are particularly pertinent as these will form part of machine-to-machine technologies that are starting to underpin future services, industries and critical national infrastructure. Previous cyber events provide a context about weaknesses associated with larger space assets and these lessons should be learned by the small satellite industry. The spectre of cyber-attacks is becoming more profound and a paradigm shift is required by the space industry to move away from legacy security measures and embrace cybersecurity principles. If attackers compromise ground station networks, they could in effect either take control of small satellites (high skill level) or cause an outage (low skill level) that would in varying degrees ultimately affect the satellites under ground station control. Cybersecurity aspects need to be considered to protect not only command and control and user data uplinks and downlinks, but also inter-satellite cross-links; in order to protect data confidentially and preserve data integrity. Without a reassessment of space protective measures in this day and age the damage to the reputation of the evolving space assets supporting the Fourth Industrial Revolution could be dire. A rethink now can address the imbalance of inherent weaknesses drawn from the past and benefit the security state of tomorrow's Internet of Things small satellite swarm constellations.

Publication History: Received: 11 December 2018 | Revised: 03 March 2019 |Accepted: 03 March 2019

Keywords:
Cybersecurity, Internet of Things, Small Satellites, Satellite Networks.

1. INTRODUCTION

A third-wave of technology innovation [1] has now established itself as the Internet of Things (IoT) driving the Fourth Industrial Revolution [2]. Advances in communications has produced Low Power Wide Area Networks (LPWAN) that fill the gap between IoT short range communications such as the IEEE802.15.4 Zigbee standard and 3rd Generation (3G) to 4th Generation (4G) cellular networks. Data can be carried from front-end devices to the back-end processing systems using the following: (a) Narrowband-IoT, (b) Global System for Mobile communications for IoT that repurposes 2nd Generation Edge technology (2.5G) for slower data-flows, and (c) Long-Term Evolution (LTE) for Machines as an alternative bearer for low bitrates [2].

This is at a time when the Northern Sky Research report estimates that 5.8 million Machine-to-Machine (M2M) and IoT

*Address correspondence to this author at the British Computer Society, London, UK.; E-mail: david.bird@bcs.org

Mesford Publisher Inc
Office Address: Suite 2205, 350 Webb Drive, Mississauga, ON L5B3W4, Canada; T: +1 (647) 7109849 |E: cace@mesford.ca, contact@mesford.ca, https://mesford.ca/journals/cace/

connections will be available in 2023 [3]. There is also a link between IoT assets and 5th Generation (5G) hybrid networks. Consequently, a number of consumer industry verticals have been identified that include: (a) automotive mobile solutions, (b) energy and building technology, (c) media and entertainment, and (d) factories of the future [4]. High-level M2M architecture has been proposed by Minoli consisting of a Device and Gateway Domain and a Network Domain and Applications Domain [5]. The resultant framework in principle enables IoT front-end sensors to communicate with the back-end domain within terrestrial network models. Furthermore, IoT continues to mature resulting in governance being introduced; examples include an IoT security compliance framework, a new IoT security maturity model [6] and the publishing of a Commonwealth and United States (US) voluntary code of practice [7]. However, IoT capabilities are not just constrained to assets on terra firma, it now includes the space dominion.

Mobile Satellite Service providers and Fixed-Satellite Service providers (FSS) provide popular narrowband radio frequency (RF) services aimed at the current generation of IoT. Meanwhile, 5G will provide low data-rate connectivity for IoT [5] between not only terrestrial assets but also satellites [8]. It has been stated that small satellites are also crucial for IoT's success deriving a requirement for IoT devices to communicate with space assets [9]. Originally small satellites were conceived in the 1980's [10] and miniaturization has invigorated the expansion of this capability for the purposes of Earth Observation (EO) and now Satellite Communications (SatCom) [11]. At that time small space vehicles were seen to be economical, cost effective and simplistic even though inter-satellite cross-links or multiple ground stations were also considered as a necessity in the future [12]. A renaissance of narrowband for IoT has opened up the market, encouraged by a diversity of small satellite launch options [13, 14, 15]. This has enabled companies such as Eutelsat [16, 17] and new companies like Hiber [18] and Australian Fleet Space Technologies [13] to expand into the Low Earth Orbit (LEO) arena. Their vision – to set up a space-borne communications capability for IoT.

Today small satellites have moved away from the limitations experienced by the first Cube Satellites (CubeSat) through improved technology enabling better manoeuvrability. This has facilitated better usability through the development of various electric propulsion systems to compensate for volume, mass and power constraints [19, 20]. The European Space Agency has stated that satellites offer important attributes, which include security, resilience, capacity and coverage [21]. Certainly, measures have been taken by the Consultative Committee for Space Data Systems (CCSDS) to provide security advice, guidance and reference architecture for the Ground, User and Space Segments. Furthermore, the cybersecurity of small satellite systems is becoming a more pertinent topic since satellites themselves have been deemed to be an extension of Critical National Infrastructure (CNI).

This paper deliberates over the cybersecurity perspective drawing upon lessons learned from real-world events to help inform security aspects of future IoT small satellite system designs. This perspective relates to communications paths and transceiver technologies which facilitate end-to-end connectivity in the small satellite realm. Therefore, the following areas have been analysed:

- The Space Segment, which incorporates the satellite vehicle with functional Command and Control (C2) equipment and transponder payloads and includes inter-satellite radio connectivity options for space-borne infrastructure.
- The User Segment that comprises the user terminal equipment and antennae for electromagnetic signal relay of channelized data uplinks and downlinks.
- The Ground Segment, which contains the ground stations, satellite dishes and ground network infrastructure for Telemetry, Tracking and Control (TT&C) used to manage satellite C2.

2. ONBOARD DESIGN AND COMMUNICATIONS CONTEXT

Larger commercial satellites typically employ bespoke control and payload architectures conjoined by the network bus. This is a means of segregating the TT&C, altitude and orbit control, electrical power and thermal control subsystems from the functional subsystems. Functional subsystems include payload data handling, transponders and antennas or EO sensors. Contrastingly, small satellites are using commercial-off-the-shelf (COTS) products for the subsystems such as a combined Command and Data Handling Unit (C&DU) type architecture attached to the Payload Data Transmission (PDT) component [22]. The density of this architecture effectively diminishes the component segregation effect making it appear difficult to add in any security enforcing functions *per se.*

A large proportion of small satellites of the past have used bespoke simple control loop or interrupt-based control systems in firmware [23]. However, in recent years there has been an adoption of Real-Time Operating Systems (RTOS) from the aerospace industry. RTOS COTS products provide additional benefits contributing to modular system design of component-based development in embedded systems; thus, enabling core C&DH elements to be deployed into updatable micro controllers like Field Programmable Gate Array (FPGA) type systems on a chip. Furthermore, RTOS delivers an array of multi-threaded processes for the timely data collection and data transfer to subsystems onboard the spacecraft [23, 24, 25]. Moreover, modern RTOS builds for space applications have an advantage of being conformant with DO-178B Software Considerations in Airborne Systems and Equipment certification and more recently the European Cooperation for Space Standardization certification. Ultimately, for intensive and perennial space applications the use of RTOS assures that critical onboard software is segregated from less critical software in a fault-tolerant manner [26, 27].

Earth-to-Satellite communication paths provide slightly different characteristics to the physical and data link layers of terrestrial ethernet baseband network conduits. This is due to the use of the electromagnetic spectrum for communications and connectivity. In radio-based systems Open Systems Interconnection (OSI) Layer 2 upwards is transposed and modulated for carriage by radio waves. From base principles satellite RF emanations require radio transponders; these comprise filters, amplifiers, modulators and demodulators and associated antennae. Data signals can be diplexed and de-diplexed respectively on small satellites using shared TT&C and SatCom payload communications emitters [28]. C-band has been trialled for medium data-rate IoT communications relay in Geostationary Earth Orbit (GEO); however, the data-rate lag in GEO necessitates Internet Protocol (IP) Acceleration [29, 30]. The Ultra High Frequency (UHF) range [31, 32], especially L and S-band satellite systems are currently being pursued for slow bitrate relays [33] in LEO; this enables low gain satellite antennas to be used in LEO compared to directional high gain antennas on larger higher throughput satellites stationed in Medium Earth Orbit (MEO) and GEO.

However, there are aspirations for the development of broadband data-rates over Super High Frequency (SHF) and Extremely High Frequency (EHF) small satellite links [11]. For example, the Iridium constellation already uses K above-band (Ka) broadband technology for inter-satellite links in LEO [5]. The viability of using higher microwave frequencies in the Ka-band for cross-links has been proven using space hardened FPGAs. This has been tested by Nano Satellite (NanoSat) category spacecraft of three-unit size upwards [34]; advances in technology has enabled RF power output to be doubled but requires gimbal functionality to direct the RF. This opens the door to millimetre wave technologies for hybrid data relay links, which has become synonymous with 5G.

Multiple Input and Multiple Output (MIMO) beamforming technologies adopted for 5G Radio Access Network (RAN) connectivity has also been used in satellite communications. MIMO provides multiple paths where the communications function of a handset provides spatial channelization between the antenna and user terminal [35] for multi-frequency sensing and dynamic data-rate alteration [36]. Hybrid applications for dual polarization MIMO communications have already been devised for narrowband mobile satellite systems using both L and S-band waveforms [37] between terrestrial and satellite elements. These can also be used to extend inter-satellite communications. The transformative effect of 5G technologies also provides a cognitive frequency sharing opportunity for the small satellite community facilitated by spectrum reuse [21, 38].

Cross-link communications between CubeSats has already been demonstrated. This opens up a potential opportunity for global IoT communications. This approach provides the prospect of creating satellite mesh networks or satellite swarms rather than continue with traditional constellation formations [39]. Research has been conducted by the Massachusetts Institute of Technology (MIT) into free space optical technologies dubbed Lasercom; lasers are being considered as an option not only for LEO stationed satellite downlinks, but also inter-satellite cross-links in four-unit sized NanoSats. Lasercom involves the use of space-grade FPGA technology to generate the seed laser in C and L-band, modulators and amplifiers in order to transmit the signal; a miniaturized optical communications transceiver is then used to focus the laser beam reaching up to 200 Gigabits per second [40, 41].

3. CYBERSECURITY PERSPECTIVE

There are many well documented and differing threats to space vehicles [42, 43, 44] in LEO on elliptical polar orbits that includes single event upsets [45]. Additionally, small satellites use either the Global Positioning System (GPS) or stargazing sensors for navigation; unfortunately, the former can be subject to jamming [46] and spectrum denial using electronic warfare (EW) means. However, cyber means could be used to create a similar disorientation effect to EW; thereby creating the circumstances where a satellite could be instructed by an attacker to enter into a 'spin of death' [47] or cause it to deorbit and decay back towards the Earth.

In 2016, Chatham House released a research report highlighting the potential consequences of cyber-attacks against the Ground and Space Segments by learning lessons from Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) hacks. Their hypothesis presented a case that it may not be insurmountable for the focus of cyber-attacks to gravitate towards aerospace and exposed vulnerabilities in spaceborne assets [48]. This is a similar dilemma to the one presently being encountered by the maritime community, which faces cyber threats against the shipborne systems by white and black hat hackers [49].

The subsequent race for dominance in the small satellite market has also been criticized for implementing 'security as an afterthought' [50]. Indeed, weaknesses in satellite implementations were declared by the US Senate Committee as far back as 2001 [51]. This is a similar theme to the one being reincarnated in IoT front-end technologies themselves; IoT products have been plagued with fundamental security flaws [52], misconfigurations [53] or a lack of security rigor blamed on the limitations of front-end compute and/or restrictions on power consumption.

3.1. The Lessons from Real-World Events

This section draws out real-world lessons that can be learned from a variety of suspected near-misses or abuses of existing satellite systems or their communications paths.

In 1998, the PANAMSAT's Galaxy IV satellite failure was attributed to an on-board processor anomaly, which had the effect of disabling between 36 to 40 million pagers across the US for up to four days [51]. Again, in the same year, cyber-intrusion means were suspected after a software error initiated from the Goddard Space Flight Center caused a German-US X-ray satellite to rotate towards the sun; damaging its high-resolution imager [54].

Between 2007 and 2008, various US satellites experienced a form of interference. It has been alleged that Chinese hackers used the C2 link from the ground station to disrupt the operation of the National Aeronautics and Space Administration (NASA) Landsat 7 satellite; this occurred at least twice in October 2007 and July 2008. Similarly, the Terra

EOS AM-1 NASA satellite was interfered with in June and October 2008 [55].

Also, in 2008 hackers infiltrated the Johnson Space Center's mission control network and used this as a foothold to upload a Trojan Horse to the International Space Station's computers disrupting communications [56]. Consequently, it has been identified that the use of multiple ground stations, with a dependency on the Internet for data access and file transfers, is contingent to providing an attack vector for nefarious interference operations [57].

Fanning justified a case that satellite signals can be 'messed with' or corrupted, which includes GPS [58]. This has been proven in the the Iranian downing of a US Unmanned Aerial Vehicle (UAV) in 2011. They employed jamming of the UAV's C2 and the encrypted GPS military P(Y) code on L1 and L2 frequency bands. This potentially caused the aircraft as a tertiary measure to resort to the unencrypted GPS C/A code. Subsequently, GPS spoofing of the C/A code on L1 was used to coerce the UAV into landing in Iran [59]. This example is particularly relevant for small satellites that use the GPS C/A code rather than stargazing sensors for navigation purposes.

In 2014, the U.S. National Oceanic and Atmospheric Administration (NOAA) ground satellite data network was taken down for an unscheduled outage due to an Internet-sourced cyber-attack [60]; the originator of the attack was suspected to be an entity in China [61]. Data had been exfiltrated from the NOAA network in the previous year and the organization had been subsequently criticized for allowing contractor computers to connect to their network; a malware infection case from the latter was suspected to be the foothold that was used to conduct a data exfiltration attack [62].

According to Kaspersky Labs in 2014 a Russian cyber-espionage group Turla obfuscated their hacking activities by detecting and stealing IP addresses from users of a satellite Internet provider [63]. This was possible because the downstream link from the satellite is unencrypted. The group used the stolen IPs to conduct C2 and instructed subverted target hosts to send traffic to these IPs across the Internet. It was relayed to the satellite downstream link and while the machines of the real IP owners dropped any spurious traffic, this Advanced and Persistent Threat group were able to receive the data within the satellite footprint [64, 65].

In 2015, claims were made that unencrypted uplinks to the Globalstar satellite could be eavesdropped using COTS equipment [66]. In the same year car tracking systems that used the Globalstar satellite data links were also declared to be prone to attack [67]. This is an example of a trait of re-using open telecommunications protocols that are inherently insecure [68, 69]. In the same year a hacker demonstrated the feasibility of intercepting insecure signals employed by the 80's generation Iridium satellites using a software-defined radio [70].

Between 2015 and 2016 it was declared that NASA had decided to upgrade its security measures to include the inter-ground station connectivity of long-haul terrestrial elements for their Deep Space Network [71]; oversights made NASA non-compliant with US federal requirements and weaknesses demonstrated that NASA was unnecessarily vulnerable to cyber-attack and cyber-espionage [72]. For example, the CCSDS endorsed Space Link Extension service provides no more inbuilt security capabilities beyond authentication; therefore, the CCSDS recommends mission data carried by packets should be encrypted end-to-end as well as the physical link itself between the space and ground elements [73]. Interestingly, in 2016 China launched a satellite into orbit to test quantum encrypted communications over large distances arguably illuminating the point that the protection of satellite communications is a national priority [74].

Between 2014 and 2017, the security company IOBit found issues with various brands of User Segment terminal equipment; the company provided an exposé of hardcoded credentials, backdoors, weak encryption algorithms, insecure protocols and susceptibility to remote injection attacks from specially crafted Short Message Service messages [75, 76, 77]. In 2018, an IOBit researcher declared that passenger infotainment networks on planes could be hacked from the ground due to onboard vulnerabilities in the satellite communications equipment [78].

A report from the Secure World Foundation last year indicated that non-state actors are actively identifying hardware and software vulnerabilities in commercial satellite systems [79]. By 2018, an espionage group based in China, known as Thrip, used malware to infect ground station computer systems linked to the C2 capability of satellites. It is alleged this was an attempt to spy on satellite communications or even take over control of the satellites in order to reposition or disrupt them [80, 81].

In 2018 Thomas from MIT presented a case that the current trend in unexpected fault conditions of control systems over the past 10 years, or attacks against control systems, is due to unforeseen system implementations. These could lead to deliberate hacker actions against authorized processes or services resulting in undesirable consequences; examples cited included the miscalculations of an inter-planetary lander that caused it to crash on a celestial body and terrestrial autonomous vehicle hacks that abused legitimate communications to force unsafe events [82].

3.2. Complexities of IoT Networking

Cross-link communications and relay capabilities in the Space Segment have been proposed by NASA [83] to increase IoT long-haul coverage; this might inevitably mean that both C2 and PDT traffic will be carried between satellites using the inter-satellite links. In support of IoT satellite networks an evolution of specialized Medium Access Control (MAC) protocols have been proposed for the datalink layer of satellite Mesh Radio Access Networks (MRAN) [84].

MACs combined with logical link control enables OSI layer 2 frames to be transmitted over shared multiple-access radio channels within an assigned spectrum [85]. Consequently, there is a concern that it might be possible to change MAC addresses remotely via the TT&C; or potentially interfere with unprotected cross-link communications through MAC spoofing by rogue satellites within emanation range. In addition, it may be possible to affect a condition within RTOS-based C&DU type architectures where a subsystem component could be abused due to manipulated or malformed communications messages. Even with layer 2 collision detection and error correction mechanisms it might be possible to overload the internal satellite network fabric; and thereby deny other subsystems access to component interfaces starving them of critical data that may induce an error state or failure [86].

The concept of IP version 6 (IPv6) encapsulation into IP version 4 addressed packets has previously been used for PDT data transition over satellites [87] due to bandwidth constraints; however, concepts are now being proposed for using IPv6 over meshed cross-links in disruptive or delay tolerant networks [84]. Thus, enabling the emergence of IoT swarm satellite concepts that will enable group-based M2M connectivity [88].

To this end OSI layer 2 Routing Protocol for Low-power and Lossy networks (RPL) is an IoT distance-vector routing protocol compatible with OSI layer 3 IPv6; this protocol has a diversity of uses that may include not only terrestrial use-cases over LPWAN but also potentially cross-linked MRANs in the Space Segment. RPL supports three fundamental traffic topologies: Multipoint-to-Point, Point-to-Multipoint and Point-to-Point. RPL messages provide three levels of security: 'Unsecured', 'Pre-installed' with a preconfigured symmetric key, and 'Authenticated' via a key authority acting as a router. RPL operates on a ranking basis – from root to subservient child nodes. However, a number of attacks have been identified that consist of direct and indirect flooding and resource exhaustion attacks [89]; this would only occur where the Unsecured level is used or when a compromised node advertises a false rank to manipulate and change the routing path in the network [90]. In a more secure-mode RPL provides authenticity by using payload encryption through 128-bit Advanced Encryption Standard with Counter Cipher Block Chaining Message Authentication Code and digital signatures [91]. Without it there is a possibility that unprotected cross-link communications could be abused; whereby satellites could be spoofed by rogue assets posing as a legitimate spaceborne node [92]. Certainly, blockchain has been proposed as a method for not only protecting IoT but it is being investigated by the US Defense Advanced Research Projects Agency for securing satellite connectivity [93]. A diversification of zero-knowledge proof protocols brings with it an opportunity to protect the privacy of the prover and verifier in blockchain transactions [94].

3.3. User Data Considerations

Presently, a favoured long-haul IoT protocol is the Message Queuing Telemetry Transport (MQTT) originally developed for SCADA OSI layer 7 applications; this is a M2M lightweight protocol that is quite flexible and can transported by Hypertext Transfer Protocol (HTTP) to publish and subscribe [95, 96] using broker services. MQTT has spawned various options for back-end processing whether it be traditional data centres or cloud services; most notably, Amazon Web Services and Microsoft Azure offer MQTT compatible IoT-based services [95]. MQTT can be secured if it is implemented properly [97]; this involves the use of robust credentials for M2M authentication and Transport Layer Security (TLS) operating at OSI layer 4 and 6 to encrypt data-in-transit. However, recent research has found that improper IoT server configuration is able to be detected by the Shodan IoT search engine; this provides an opportunity for hackers to attack MQTT-based applications [96]. It has also been asserted by the antivirus company Avast that cyber-criminals are now focusing on taking over IoT end-points [96]; their intent is to use them as bots for malicious purposes such as Distributed Denial-of-Service (DDoS) attacks [97, 98].

The diversity of IoT User Segment communications paths is shown in Fig. (**1**). From a downstream perspective it is the users' responsibility in the User Segment to ensure their data is protected end-to-end via satellite PDT; satellite users should not place reliance upon the ground terminal function and the satellite link itself to protect their IoT services. As demonstrated in the Globalstar case, secure uplinks and downlinks of the User Segment may not be a consideration of satellite service providers; if encryption is not applied then potentially anyone with the right equipment in the satellite footprint could intercept the radio signal and potentially reconstitute the data carried by that bearer.The round trip time of Transmission Control Protocol exchanges via satellites in LEO provide a comparable latency to terrestrial networks thus making TLS connections possible; however,wider user adop--tion of User Datagram Protocol-based for IoT communications security methods is likely to be more performant for long network paths using satellites.

3.4. C2 weaknesses

From a Ground Segment perspective, the concept of an architectural framework for advanced operational autonomy of small spacecraft was justified back in 1995 [99]. Today the common Extensible Mark-up Language (XML) Telemetry and Command Exchange format is used to pass satellite telemetry and commanding data following CCSDS recommendations [100]. Therefore, C2 applications employed by the ground stations use web interfaces to perform telemetry monitoring and analysis, C2 procedure creation and automatic data ingestion to databases [100]. This approach therefore presents a richer IP-based cyber-attack landscape within which there are a multitude of attack surfaces; such as enterprise networks that may be indirectly connected to the Ground Segment. Unless the data objects within the XML are encrypted or the HTTP session is encrypted using TLS then the data could be intercepted.

Dacey [51] highlighted that the TT&C uplink of 1990s generation satellites should be encrypted but identified that the telemetry downlink may not; in fact, back in 2002 the report stated that encrypting the TT&C and data links was viewed as not really providing much more security than existing techniques. A statement like this indicates that there has perhaps been an over reliance on techniques like spread-spectrum [51]; subsequently spread-spectrum frequency hopping in some cases has been found to be fallible [101]. A diagram representing TT&C links is shown in Fig. (**2**).

Zero-knowledge proof challenge and response techniques are a known quantity for the purposes of authentication and secure link establishment between ground stations and satellites; thereby avoiding the risk of replay attacks posed through the

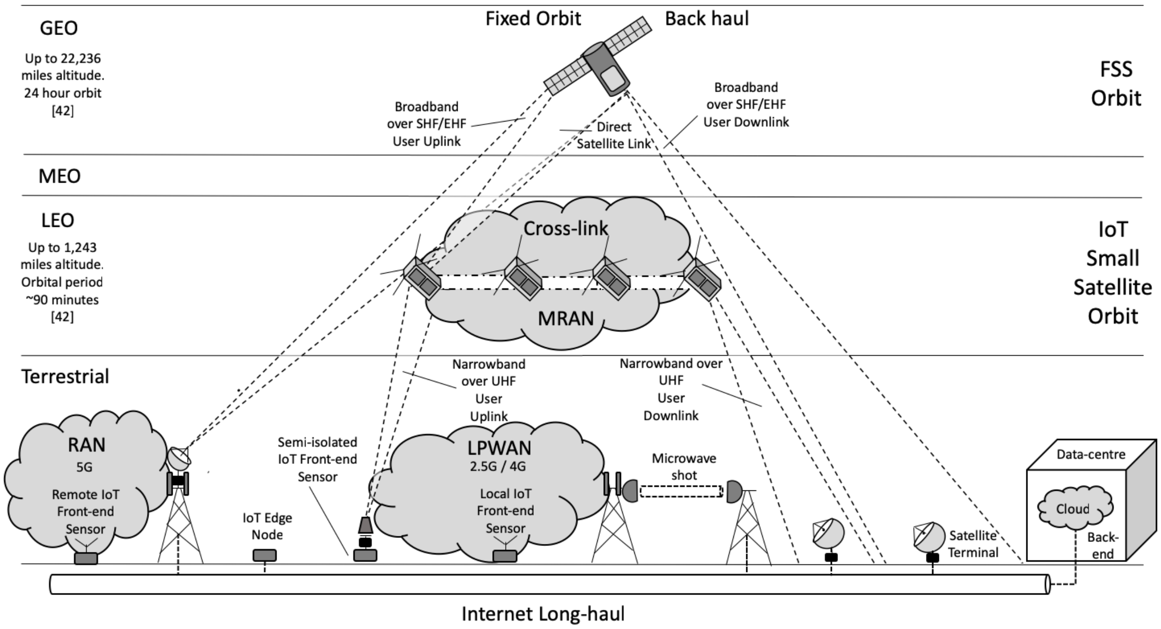
GEO
Up to 22,236 miles altitude. 24 hour orbit [42]
Fixed Orbit
Back haul
Broadband over SHF/EHF User Uplink
Direct Satellite Link
Broadband over SHF/EHF User Downlink
FSS Orbit
MEO
LEO
Up to 1,243 miles altitude. Orbital period ~90 minutes [42]
Cross-link
MRAN
IoT Small Satellite Orbit
Terrestrial
Narrowband over UHF User Uplink
Narrowband over UHF User Downlink
RAN
5G
Remote IoT Front-end Sensor
Semi-isolated IoT Front-end Sensor
IoT Edge Node
LPWAN
2.5G / 4G
Local IoT Front-end Sensor
Microwave shot
Satellite Terminal
Data-centre
Cloud
Back-end
Internet Long-haul

Fig. (1). PDT across Terrestrial, User and Space Segments.

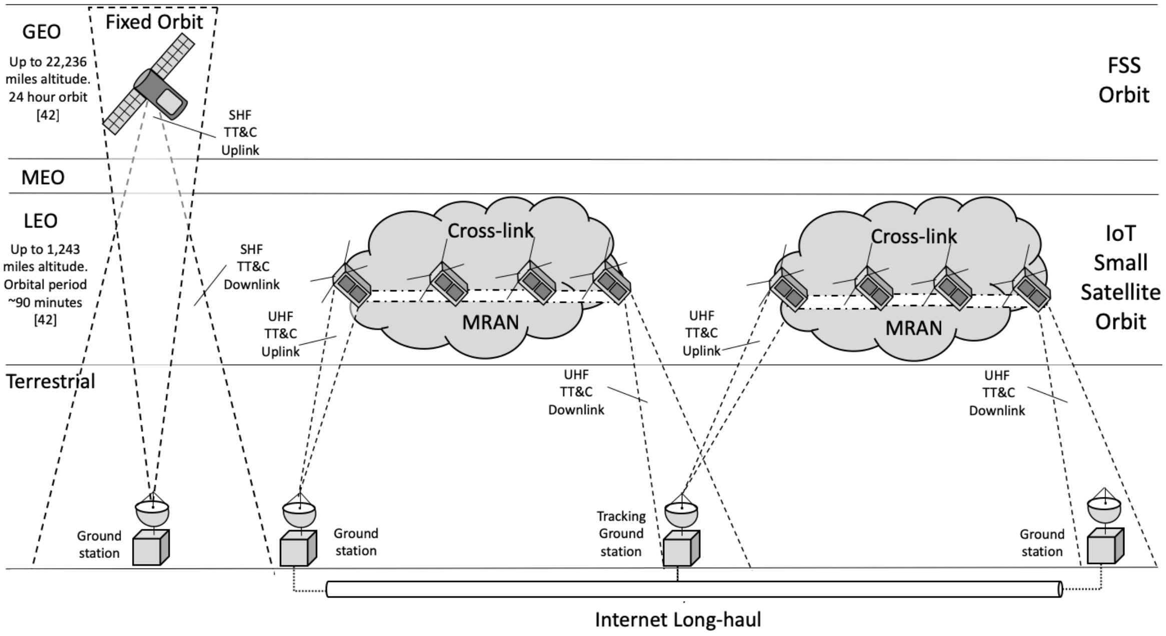

Fig. (2). TT&C and Ground Segment interaction.

use of passwords [102]. However, a recent study by London Cyber Security Ltd alleges that TT&C links of some more modern satellites are still not necessarily encrypted – either for simplicity or as a cost saving measure [54]. Effectively, without both authentication and encryption mechanisms in place valid command codes could be exposed over the link. In addition, the use of protected waveforms for the provision of radio link transmission security has not been widely adopted due to historical considerations or conflicts with legacy operating procedures [103]. Therefore, it is asserted that with the right COTS radio equipment satellite C2 uplink and downlink signals could be intercepted. Malign hackers could potentially: (a) reconstitute data or commands being passed, or (b) if protected using zero-knowledge proofs, attempt to affect a small satellite RTOS resource starvation attack by constantly issuing bogus challenges that consume satellite processes.

It has been speculated in the past that if the Ground Segment is breached, then the Space Segment would be virtually unprotected [50]. The CCSDS does consider ground station security by including network components and protocol filtering firewalls, device hardware encryption as well as physical boundaries such as shielded rooms or air gaps [104]. Notwithstanding this, a remote attack could still be conducted against a ground station network especially where there is poor cyber hygiene and flawed processes that can be abused through indirect methods; this was the case in the NOAA case-study. Also, as previously demonstrated in the aforementioned case-studies the ground station could act as an ingress point and be used to springboard an attempted hijack of a satellite via the TT&C. This could be achieved by separately intercepting the TT&C as previously discussed to acquire knowledge of C2 message sequences, learn their structure and meaning and then attempt to take control by hacking a targeted ground station. Once a foothold is established further stages of a cyber-attack could then be attempted against the satellite.

3.5. End-to-end security-by-design

The CCSDS also provides advice relating to the standardization of: (a) data system architecture, (b) systems engineering and security, (c) modulation methods and space datalink security, (d) network protocols and data exchange formats, (e) authentication between entities and so forth. Within this it is also specified that security measures to de-risk the use of the electromagnetic spectrum should include but not be limited to the following: terrestrial and space datalink encryption, spread-spectrum or related jamming avoidance approaches [104]. Historically, protracted lead times for satellite projects have made it difficult for security to be embedded within traditional satellite fabrication [54]. With the benefit of hindsight and with a shorter manufacturing cycle for small satellite production, there is now a stronger argument to build in cybersecurity requirements from the outset.

In effect supply chain security should be considered from the start of the contracting process and built upon through the continuous improvement of trust between suppliers and their customer. Another relevant consideration across all Segments is the security of code, especially where high-level languages are used. Software security should also consider the lock down and hardening of unnecessary services [105, 106] avoiding the use of hard-coded or default credentials, backdoors as well as insecure and undocumented protocols [82]. Hacker manipulation is not limited to vulnerabilities such as zero-days, but also the abuse of legitimate services and inter-process communications to cause unexpected real-world impacts.

IoT is a prime example that has exposed some vendors who have rushed insecure or flawed terrestrial products to market [107]. Human complacency could open up further satellite orientated cyber vulnerabilities [108] so small satellite manufacturers must learn lessons from the wider space industry. This means implementing security measures in a similar vein to the conscious decision taken by the European Galileo programme [109]. Exploitation of IoT satellite negotiated network paths could cause disruption or some form of service denial across the wider IoT global infrastructure. In 2014, Japan held a view that threats to space-based assets may be preventable but only when the system is robust enough [110]. To this end, a series of cybersecurity principles have been proposed in Table **1** to strengthen IoT small satellite design considerations:

Table 1. Cybersecurity Considerations.

Cybersecurity Principles	Considerations and Context
Small satellite businesses	Paradigm shift away from a reliance upon outmoded protection mechanisms and adopt cybersecurity measures.
Security of supply chain	Equipment and software procurement to include integrity checks of hardware components and code/software.
Secure-by-design	Cyber-secured architectures for both downstream and upstream assets.
Secure radio techniques	Protected waveform utilization between ground station and satellite to secure at least C2 links.
Defence-in-depth	Boundaries and zoning, separation and segregation, and adoption of encryption techniques to secure data-in-transit and/or objects/files across all Segments using encrypted links.
Interoperability	Interoperability including error/correction mechanisms and authentication between Ground Segment and Space Segment and also between cross-linked upstream assets.
Security of application	Measures for checking data integrity should not only consider invalid or incorrect parameters as part of the data validation process, but also verify data exchange legitimacy.
Monitoring and backup or recovery	Processes for safe update and reboot cycles in the Space Segment.

4. SUMMARY

Small satellite deployments are now challenging the traditional stereotypes that satellite technology is costly and has propagation delays [111]. In 2015 it was argued that NanoSats could help with Satcom resilience and expand coverage areas [112]. The importance of IoT small satellites is now being realized as an integral part of hybrid networks [113] and coexistence with other capabilities such as 5G satellite bearers [114]. The satellite industry has thus far escaped a high-profile cyber event avoiding reputational damage witnessed by other sectors of industry [115]. But in recent years there has been an upward trend in more prolific and diverse cyber-attacks across other industries [116, 117]. Based on the evidence it is entirely plausible that there could be a shift to more prolific ground station and small satellite vehicle hacking scenarios. Cyber-attacks are therefore more credible now there is a wider adoption of satellite technology fuelled by the popularity of small satellite use-cases [98, 118].

There is a fear that the use of COTS equipment and more common operating systems such as RTOS in small satellites presents risks [119] that needs action by both governments and industry [120]. It has been alleged that attitudes such as 'security as an afterthought' [50] contributes to an increase in the potential attack surface of space capabilities. In this third era of space, frameworks need to be agreed for low-cost satellite deployments [121] following in the footsteps of the terrestrial IoT frameworks and codes of practice [6, 7]. This is relevant at a time when conglomerates and the European Union are pushing for the future diversification of IoT connectivity via satellite MRANs [122].

There is a greater risk of original equipment manufacturers, their suppliers and users succumbing to a cyber-attack scenario which may leach out data pertaining to product capabilities, limitations and weaknesses [123]. Historically the probability of mechanical satellite failure has been far greater than electrical faults [124]; however, this paper has articulated a number of cyber-attack perspectives related to satellite-borne networks across all Segments. This necessitates another look at security controls and security enforcing functions within the satellite domain. Without it there is a risk of active cyber-attacks that could continue to induce computer interference and potential malfunctions against either the Ground Segment or the Space Segment. This therefore demands more robust C2 [42] and cyber compatible upstream, downstream and inter-satellite link security measures [125].

CONFLICT OF INTEREST

The author declares that there are no conflicts of interest.

ABBREVIATIONS

2.5G	–	2nd Generation (Edge)
3G	–	3rd Generation
4G	–	4th Generation
5G	–	5th Generation
C2	–	Command and Control
CCSDS	–	Consultative Committee for Space Data Systems
C&DU	–	Command and Data Handling Unit
CNI	–	Critical National Infrastructure
COTS	–	Commercial-Off-The-Shelf
CubeSat	–	Cube Satellite
EHF	–	Extremely High Frequency
EO	–	Earth Observation
EW	–	Electronic Warfare
FPGA	–	Field Programmable Gate Arrays
FSS	–	Fixed-Satellite Service
GEO	–	Geostationary Earth Orbit
GSM	–	Global System for Mobile communications
HTTP	–	Hypertext Transfer Protocol
ICS	–	Industrial Control Systems
IoT	–	Internet of Things
IP	–	Internet Protocol
IPv6	–	IP version 6
Ka	–	K above-band
Lasercom	–	Laser communications
LEO	–	Low Earth Orbit
LPWAN	–	Low Power Wide Area Networks
LTE	–	Long-Term Evolution
M2M	–	Machine-to-machine
MAC	–	Medium Access Control
MEO	–	Medium Earth Orbit
MRAN	–	Mesh Radio Access Networks
MIMO	–	Multiple Input and Multiple Output
MIT	–	Massachusetts Institute of Technology
MQTT	–	Message Queuing Telemetry Transport
NASA	–	National Aeronautics and Space Administration
NOAA	–	National Oceanic and Atmospheric Administration
OSI	–	Open Systems Interconnection model
PDT	–	Payload Data Transmission
RAN	–	Radio Access Network
RF	–	Radio Frequency
RPL	–	Routing Protocol for Low-power and Lossy networks
RTOS	–	Real-Time Operating Systems
SatCom	–	Satellite Communications
SCADA	–	Supervisory Control and Data Acquisition
SHF	–	Super High Frequency
TLS	–	Transport Layer Security
TT&C	–	Tracking and Control
UAV	–	Unmanned Aerial Vehicle
UHF	–	Ultra High Frequency
US	–	United States
XML	–	Extensible Mark-up Language

REFERENCES

[1]. Bird, D. 5G The need for speed. Available from: https://www.bcs.org/content/conWebDoc/55211

[2]. Bird, D. Industry 4.0 – the aggregated risks. Available from: https://flipflashpages.uniflip.com/3//84078/1099130/pub/html5.html#page/1

[3]. Marashi, M. Satellites are critical for IoT sector to reach its full potential. Available from: https://techcrunch.com/2017/06/08/satellites-are-critical-for-iot-sector-to-reach-its-full-potential/

[4]. Dow, R. Satellites and 5G for Business Opportunities Event; 2018 Nov 6; London, UK; Space Applications Catapult and European Space Agency.

[5]. Minoli, D. Innovations in Satellite Communications and Satellite Technology: The Industry Implications of DVB-S2X, High Throughput Satellites, Ultra HD, M2M. New Jersey, US: John Wiley and Sons 2015. ch. 3, 6, 8.

[6]. Carielli, S., Rudina, E., Soroush, H., and Zahavi, R. IoT Security Maturity Model: Description and Intended Use. Industrial Internet Consortium, US: Object Management Group Inc 2018.

[7]. Ashford, W. IoT firms sign up to UK security code of practice. Available from: https://www.computerweekly.com/news/252450588/IoT-firms-sign-up-to-UK-security-code-of-practice

[8]. Luciano, M. Satellites Will Play Instrumental Role In 5G Network. Available from: https://www.ecnmag.com/blog/2018/01/satellites-will-play-instrumental-role-5g-network

[9]. Reichert, C. Satellite IoT startup Myriota raises $15m. Available from: https://www.zdnet.com/article/satellite-iot-startup-myriota-raises-15-million/

[10]. Cochetti, R. Mobile Satellite Communications Handbook, Second Edition. New Jersey, US: John Wiley and Sons 1998: ch. 7.

[11]. Press, L. Might CubeSats Provide Broadband Internet Connectivity One Day? Available from: http://www.circleid.com/posts/20180904_might_cubesats_provide_broadband_internet_connectivity_one_day/

[12]. National Research Council. The Role of Small Satellites in NASA and NOAA Earth Observation Programs. Washington, DC: The National Academies Press 2000; pp. 1-104.

[13]. Nott, G. IoT firm Fleet reveals launch plan for first two nanosats. Available from: https://www.cio.com.au/article/642625/iot-firm-fleet-reveals-launch-plan-first-two-nanosats/

[14]. Henry, C. Sigfox's CTO on where satellite fits in an IoT-only network. Available from: https://spacenews.com/sigfoxs-cto-on-where-satellite-fits-in-an-iot-only-network/

[15]. Osborne, J. KEPLER and CATAPULT TO SPEED UP LAUNCH OF IOT CAPABLE SATELLITES. Available from: http://www.keplercommunications.com/blog/item/kepler-catapult-to-speed-up-launch-of-iot-capable-satellites

[16]. Eutelsat. Eutelsat Developing Low Earth Orbit Satellite for IoT Services. Available from: https://www.multichannel.com/news/eutelsat-developing-low-earth-orbit-satellite-iot-services-418569

[17]. Eutelsat. EUTELSAT COMMISSIONS ELO, ITS FIRST LOW EARTH ORBIT SATELLITE DESIGNED FOR THE INTERNET OF THINGS. Available from: http://news.eutelsat.com/pressreleases/eutelsat-commissions-elo-its-first-low-earth-orbit-satellite-designed-for-the-internet-of-things-2440770

[18]. Hiber. Hiber got €1.8M to launch 2 IoT satellites in 2018: 5 things to know about Amsterdam space startup. Available from: https://siliconcanals.nl/news/startups/hiber-e1-8m-launch-2-iot-satellites-2018/

[19]. Foust, J. More startups are pursuing cubesats with electric thrusters. Available from: https://spacenews.com/more-startups-are-pursuing-cubesats-with-electric-thrusters/

[20]. Leomanni, M. Garulli, A., and Giannitrapani, A. Propulsion Options for Very Low Earth Orbit Microsatellites; 2016 Nov 7; Acta Astronautica: Italy.

[21]. Franchi, A. and Arnold, K. Satellites and 5G for Business Opportunities Event; 2018 Nov 6; London, UK: Space Applications Catapult and European Space Agency.

[22]. Murtaza, H. Designing a Small Satellite in LEO for Remote Sensing Application. Islamabad, PK. Journal of Space Technology 2011; 1 (1): 11-16.

[23]. Cooke, C. Implementation of a Real-Time Operating System on a Small Satellite Platform. Proceedings of the Space Grant Undergraduate Research Symposium 2012: 1-2.

[24]. Tyler, T. Modern software development for aerospace. Available from https://www.aerospacemanufacturinganddesign.com/article/modern-software-development--for-aerospace/

[25]. Zeldman, B. How to choose an RTOS for your FPGA and ASIC designs. Available from: https://www.eetimes.com/document.asp?doc_id=1274573

[26]. Beus-Dukie, L. COTS Real-Time Operating Systems in Space. School of Computing and Mathematics, University of Northumbria 2001: 1-2.

[27]. Slačka, J and Halás, M. Safety Critical RTOS for Space Satellites. Proceedings of the 20th International Conference on Process Control 2015 Jun 9-12. Strbske Pleso, Slovakia. IEEE 2015.

[28]. Roeper, G., Goldsmith, R., Hatziathanasiou, I., McLaren, C., and Maguire, P. MINIATURE TT&C MODULE FOR SMALL SATELLITES IN LOW EARTH ORBITS. Proceedings of the 5th Workshop on Tracking, Telemetry and Command Systems for Ground and Space Applications: 2010; Noordwijk, NL: European Space Agency.

[29]. Ghani, N and Dixit, S. TCP/IP Enhancements for Satellite Networks. IEEE Communications Magazine 1999; 37(7): 64-72.

[30]. Fraunhofer IIS. Fraunhofer IIS demonstrates direct IoT connectivity via GEO satellite. Available from: https://www.iis.fraunhofer.de/en/pr/2018/20180607_KS_Geo.html

[31]. Tiainen, A. Inter-Satellite Link Antennas: Review and The Near Future. Masters Dissertation. Luleå, SE: Department of Computer Science, Electrical and Space Engineering, University of Technology 2017; pp. 99-100.

[32]. NASA. State of the Art of Small Spacecraft Technology: Chapter 09 Communications. Available from: https://sst-soa.arc.nasa.gov/09-communications

[33]. Amyx, S. HOW SATELLITE COMMUNICATION IS ENABLING GLOBAL COVERAGE FOR IOT. Available from: https://www.iottechexpo.com/2017/06/iot/how-satellite-communication-is-enabling-global-coverage-for-iot/

[34]. King, J., Aghahassan, H., Bertino, M., Cooper, B., Kim, J., Leveque, K. Ka-band for CubSats. Proceedings of the 29th Annual AIAA/USU Conference on Small Satellites; SSC15 2015.

[35]. Masterton, C. Defining Massive MIMO in a 5G World. Available from: https://www.mwrf.com/systems/defining-massive-mimo-5g-world

[36]. Baldini, G., Sturman, T., Biswas, A., Leschhorn, R., Godor, G., and Street, M. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead, IEEE Communications Surveys and Tutorials 2012; 14(2): 355-379.

[37]. Chatzinotas, S., Ottersten, B., and Gaudenzi, R. Cooperative and Cognitive Satellite Systems. Elsevier Science and Technology Books Inc., Elsevier Ltd 2015; ch. 7-11.

[38]. Ofcom. Update on 5G spectrum in the UK. Ofcom Statement 2017; pp. 6, 11.

[39]. Lemonbeat. Nanosatellites for the Internet of Things. Available from: https://www.wespeakiot.com/nanosatellites-for-the-internet-of-things/

[40]. Kingsbury, R. and Cahoy, K. Prof. Optical Communications for Small Satellites. PhD Dissertation. MIT, US: Department of Aeronautics and Astronautics 2015.

[41]. Clements, E. and Cahoy, K. Prof. Laser Communications Downlink and Crosslink Designs for CubeSats. MIT, US: Space, Telecommunications, Astronomy and Radiation Lab 2016.

[42]. Bird, D. Trouble in space? Available from: https://www.bcs.org/content/conWebDoc/56519?changeNav=10130

[43]. Garino, B. Chapter 21 Space System Threats, SPACE SYSTEM THREATS. AU-18 2009; pp. 273-281.

[44]. Thomson, A. Satellite Vulnerability: a post-Cold War issue? Available from: https://fas.org/spp/eprint/at_sp.htm

[45]. Wang, F and Agrawal, V. Single Event Upset: An Embedded Tutorial. Proceeding of the 21st International Conference on VLSI Design; 2008 Jan 4-8; Hyderabad, India. IEEE 2008

[46]. National Space-Based Positioning, Navigation, and Timing Advisory Board. Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures. Available from: https://www.gps.gov/governance/advisory/recommendations/2010-11-jammingwhitepaper.pdf

[47]. Hatfield, M. Dellingr: The Little CubeSat That Could. Available from: https://www.nasa.gov/feature/goddard/2018/dellingr-the-little-cubesat-that-could

[48]. Livingstone, D and Lewis, P Dr. Space, the Final Frontier for Cybersecurity? Available from: https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity

[49]. Jiang,J. Hacked Off. Available from: https://splash247.com/hacked-off/

[50]. Hutchins, R. Cyber Defense of Space Assets. Massachusetts, US: Tufts School of Engineering 2016; pp. 1-18.

[51]. Dacey, R. Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed, GAO, Diane Publishing 2002; pp. 20-33.

[52]. Wall, M. 'A cyber-attack could stop the country'. Available from: https://www.bbc.co.uk/news/business-45952693

[53]. Allen, T. There is a massive hole in IoT security, says Avast researcher. Available from: https://www.computing.co.uk/ctg/news/3061282/there-is-a-massive-hole-in-iot-security-says-avast-researcher

[54]. Horowitz, M., Randles, M., and Levi, R. Space Cybersecurity's Final Frontier. London Cyber Security 2015; pp. 3-31.

[55]. Arthur, C. Chinese hackers suspected of interfering with US satellites. Available from: https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected.

[56]. Bichler, S. MITIGATING CYBER SECURITY RISK IN SATELLITE GROUND SYSTEMS. Air University (U.S.). Air Command and Staff College 2015; pp. 15-16.

[57]. Infosec Island. Malicious Cyber Activities Directed Against U.S. Satellites. Available from: http://infosecisland.com/blogview/18279-Malicious-Cyber-Activities-Directed-Against-US-Satellites.html

[58]. Bartels, M. Why Satellites Need Cybersecurity Just Like You. Available from: https://www.space.com/42658-cybersecurity-for-satellites.html

[59]. Rawnsley, A. IRAN'S ALLEGED DRONE HACK: TOUGH, BUT POSSIBLE. Available from: https://www.wired.com/2011/12/iran-drone-hack-gps/

[60]. Gruss, M. NOAA Admits to Cyberattack on Satellite Data Networks. Available from: https://spacenews.com/42561noaa-admits-to-cyberattack-on-satellite-data-networks/

[61]. Peters, S. NOAA Blames China In Hack, Breaks Disclosure Rules. Available from: https://www.darkreading.com/noaa-blames-china-in-hack-breaks-disclosure-rules/d/d-id/1317460

[62]. Sternstein, A. Hacker Breached NOAA Satellite Data from Contractor's PC. Available from: https://www.nextgov.com/cybersecurity/2014/07/hacker-breached-noaa-satellite-data-contractors-pc/89771/

[63]. Gregory, F. Job One for Space Force: Space Asset Cybersecurity. Cyber Security Project, Belfer Center 2018; p. 7.

[64]. Drozhzhin, A. Russian-speaking cyber spies exploit satellites. Available from: https://www.kaspersky.com/blog/turla-apt-exploiting-satellites/9771/

[65]. Tanase, S. Satellite Turla: APT Command and Control in the Sky. Available from: https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/

[66]. Tucker, P. Hacker Cracks Satellite Communications Network. Available from: https://www.defenseone.com/technology/2015/08/hacker-cracks-satellite-communications-network/118915/

[67]. BBC. Globalstar tracking system 'open to attack'. Available from: https://www.bbc.co.uk/news/technology-33731185

[68]. Knott, F. Cyber Concerns For The Satellite Sector. Available from: https://attilasec.com/blog/satellite-cybersecurity/

[69]. Threatmodeller. Why Satellite Security is Important. Available from: https://threatmodeler.com/2018/05/22/why-satellite-security/

[70]. Porup, J. It's Surprisingly Simple to Hack a Satellite. Available from: https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite

[71]. Gaudin, S. NASA installs VPN to protect Deep Space Network. Available from: https://www.computerworld.com/article/3150973/space-technology/nasa-installs-vpn-to-protect-deep-space-network.html

[72]. Carreau, M. NASA Agrees To Address Deep Space Network Upgrade, Security Needs. Available from: http://aviationweek.com/space/nasa-agrees-address-deep-space-network-upgrade-security-needs

[73]. CCSDS. SPACE LINK EXTENSION—INTERNET PROTOCOL FOR TRANSFER SERVICES CCSDS 913.1-B-2. Blue Book. CCSDS 2015; pp. 23-25.

[74]. Burgess, M. Hackers targeting satellites could cause 'catastrophic' damage. Available from: https://www.wired.co.uk/article/satellites-vulnerable-hacking-chatham-house

[75]. Jackson, K. Satellite Communications Wide Open To Hackers. Available from: https://www.darkreading.com/vulnerabilities---threats/satellite-communications-wide-open-to-hackers/d/d-id/1204539

[76]. Gonsalves, A. Major security flaws threaten satellite communications. Available from: https://www.csoonline.com/article/2146021/cyber-attacks-espionage/major-security-flaws-threaten-satellite-communications.html

[77]. Paganini, P. IOActive disclosed 2 critical flaws in global satellite telecommunications Inmarsat's SATCOM systems. Available from: https://securityaffairs.co/wordpress/64902/breaking-news/satcom-amosconnect-8-flaws.html

[78]. Brewster, T. This Guy Hacked Hundreds Of Planes From The Ground. Available from: https://www.forbes.com/sites/thomasbrewster/2018/08/09/this-guy-hacked-hundreds-of-planes-from-the-ground/#7aad172e46f2

[79]. Guss, M. A new target for hackers? Satellites. Available from: https://www.fifthdomain.com/dod/2018/04/11/a-new-target-for-hackers-satellites/

[80]. Beavers, O. Rising concerns over hackers using satellites to target US. Available from: https://thehill.com/policy/cybersecurity/394037-satellites-become-latest-tool-for-hackers-targeting-businesses-consumers.

[81]. Kirk, J. Hackers Hit Satellite Operators and Telecoms, Symantec Says. Available from: https://www.bankinfosecurity.com/symantec-says-hackers-struck-satellite-operators-telecoms-a-11111

[82]. Thomas, J Dr. LESSONS FROM SAFETY ENGINEERING – APPLYING SYSTEMS THINKING TO CYBER SECURITY; 2018 Apr 10-12; Manchester, UK. NCSC 2018.

[83]. NASA. NASA Small Satellite Duo Deploys from Space Station into Earth Orbit. Available from: https://www.nasa.gov/centers/ames/engineering/projects/nodes

[84]. Sanctis, M., Cianca, E., Araniti, G., Bisio, I., and Prasad, R. Satellite Communications Supporting Internet of Remote Things. IEEE Internet of Things Journal 2016; 3(1): 113 – 123.

[85]. Radhakrishnan, R. Edmonson, W., Afghah, F., Rodriguez-Osorio, R., Pinto, F., and Burleigh, S. Survey of Inter-Satellite Communication for Small Satellite Systems: Physical Layer to Network Layer View. IEEE Communications Surveys and Tutorials 2016: 18(4): 2442 – 2473.

[86]. Ødegaard, K. and Skavhaug, A. Simple Methods for Error Detection and Correction for Low-Cost Nano Satellites. Matthieu ROY. SAFECOMP 2013 - Workshop DECS 2016; Toulouse, FR: 32nd International Conference on Computer Safety, Reliability and Security.

[87]. Sun. Z. Satellite Networking: Principles and Protocols, Second Edition. New Jersey, US: John Wiley and Sons 2014; ch. 4, 6, 7.

[88]. Mayzaud, A., Badonnel, R. and Chrisment, I. A Taxonomy of Attacks in RPL-based Internet of Things. International Journal of Network Security, IJNS 2016; 18 (3): 459 - 473.

[89]. Semedo, F., Moradpoor. N., and Rafiq, M. Vulnerability Assessment of Objective Function of RPL Protocol for Internet of Things. Proceedings of the 11th International Conference for the Security of Information and Networks; 2018 Sep 11-12; Cardiff, UK: Cardiff University. ACM 2018.

[90]. Granjal, J., Monteiro, E., and Sá SilvaSecurity, J. Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues. IEEE COMMUNICATION SURVEYS and TUTORIALS 2015.

[91]. Gibson, C. Attack Vectors in Orbit: The Need for IoT and Satellite Security in the Age of 5G. Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/

[92]. Wong, J. Even the US military is looking at blockchain technology—to secure nuclear weapons. Available from: https://qz.com/801640/darpa-blockchain-a-blockchain-from-guardtime-is-being-verified-by-galois-under-a-government-contract/

[93]. Banafa, A. A Secure Model of IoT with Blockchain. Available from: https://www.technologyreview.com/s/603298/a-secure-model-of-iot-with-blockchain/

[94]. Shor, L. On Zero-Knowledge Proofs in Blockchains. Available from: https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1

[95]. Bird, D. Information Security risk considerations for the processing of IoT sourced data in the Public Cloud. Proceedings of the PETRAS Living with the Internet of Things conference; 2018 Mar 28-29; London, UK: Institution of Engineering Technology. IEEE 2018.

[96]. Hron, M. Are smart homes vulnerable to hacking?. Available from: https://blog.avast.com/mqtt-vulnerabilities-hacking-smart-homes

[97]. Salat, M. The dark side of IoT devices. Available from: https://blog.avast.com/the-dark-side-of-iot-devices

[98]. Henry, C. Cyber experts say threats to satellites are legion. Available from: https://spacenews.com/cyber-experts-say-threats-to-satellites-are-legion/

[99]. Siewert, S. and McClure, L. A System Architecture to Advance Small Satellite Mission Operations. Proceedings of the 9th Annual AIAA/Utah State University Conference on Small Satellites:1995 Sep 18-21; Utah, US.

[100]. Object Management Group. INFORMATION MODEL FOR SPACECRAFT TELEMETRY AND COMMANDING DATA. Available from: https://www.omg.org/xtce/index.htm

[101]. Moore. C. Spread Spectrum Satcom Hacking. Black Hat USA; 2015 Aug 1-6; Las Vegas: USA.

[102]. Gardner, V. An Appliance Based Approach to Small Satellite Command and Control. Kratos Defense and Security Solutions. The Aerospace Corporation 2014; pp.1-5

[103]. Butler, R. PROTECTED SATELLITE COMMAND AND CONTROL (C2) WAVEFORMS AND ENHANCED SATELLITE RESILIENCY. Proceedings of the 34th Space Symposium; 2018 Apr 16; Colorado, US.

[104]. CCSDS. REFERENCE ARCHITECTURE FOR SPACE DATA SYSTEMS CCSDS 311.0-M-1. Magenta Book. CCSDS 2008; pp. 4-7, 6-13, 7-8.

[105]. Tarel, G., Jubineau, F., Sainct, H. Dumas, R., MartinezDeAragon, A. Small Satellites Constellations and Network: Architectures and Technologies. Proceedings of the 13th Annual AIAA/USU Conference on Small Satellites; SSC99-IV-4 1999.

[106]. Sadek, R. Cyber-Hardening: why it is critical to satellite communications. Available from: https://www.thuraya.com/content/cyber-hardening-why-it-critical-satellite-communications

[107]. Tarpley, B. The Disadvantages of Satellites. Available from: https://sciencing.com/disadvantages-satellites-8607699.html

[108]. Bird, D. Buckle Up. Available from: https://www.bcs.org/content/conWebDoc/55749

[109]. Griffin, A. CYBER ATTACKS ON SATELLITES COULD SPARK GLOBAL CATASTROPHE, EXPERTS WARN. Available from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/cyber-attacks-on-satellites-could-spark-global-catastrophe-experts-warn-a7321361.html

[110]. Baylon, C. Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives. Research Paper 2014; pp. 29-30.

[111]. Holmes, M. Expert Paints Bleak Picture of Cyber Threat to Space Industry. Available from: https://www.satellitetoday.com/telecom/2017/02/21/expert-paints-bleak-picture-cyber-threat-space-industry/

[112]. Gunduzhan, E., and Dewayne Brown, K. Narrowband Satellite Communications: Challenges and Emerging Solutions. John Hopkins APL Technical Digest. 33(1): 1-56.

[113]. Werner, D. Small satellites are at the center of a space industry transformation. Available from https://spacenews.com/small-satellites-are-at-the-center-of-a-space-industry-transformation/

[114]. SatCom WG. NetWorld2020's – SatCom WG The role of satellites in 5G. Available from: https://www.networld2020.eu/wp-content/uploads/2014/02/SatCom-in-5G_v5.pdf

[115]. Henry, C. Satellite industry doing surprisingly well against cyber threats, experts say. Available from: https://spacenews.com/satellite-industry-doing-surprisingly-well-against-cyber-threats-experts-say/

[116]. Ambrose, G. Half of UK manufacturers fall victim to cyber-attacks. Available from: https://www.telegraph.co.uk/business/2018/04/22/half-uk-manufacturers-fall-victim-cyber-attacks/

[117]. Malhik, E. GCHQ warns public 'absolute protection not possible' as it briefs power and transport firms on cyber attacks. Available from: https://www.telegraph.co.uk/news/2018/04/21/gchq-warns-public-absolute-protection-not-possible-arranges/

[118]. Sweating, M. Modern Small Satellites-Changing the Economics of Space. IEEE Proceedings 2018; 106(3): 343-361.

[119]. Holmes, M. Cyber Experts: The Truth About The Threats to Satellite. Available from: http://interactive.satellitetoday.com/via/may-june-2017/cyber-experts-the-truth-about-the-threats-to-satellite/

[120]. Fidler, D. Cybersecurity and the New Era of Space Activities. Available from: https://www.cfr.org/report/cybersecurity-and-new-era-space-activities

[121]. Paul, F. Is the IoT in space about to take off? Available from: https://www.networkworld.com/article/3315736/internet-of-things/is-the-iot-in-space-about-to-take-off.html

[122]. Winnefield, J. Cybersecurity's Human Factor: Lessons from the Pentagon. Available from: https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

[123]. Ernest and Young. Top 10 risks in aerospace and defense 2017. Ernest and Young Report.

[124]. Yates, J. Satellite Communication Presentation. Institution of Engineering Technology Event: Coventry University UK 2014.

[125]. Werner, D. Small satellite sector grapples with cybersecurity requirements, cost. Available from: https://spacenews.com/small-satellite-sector-grapples-with-cybersecurity-requirements-cost/