Earth to Space Communication – A Security Overview

Ryan Morganti

Abstract

This project is a survey over space communications and the security associated with these communications. This project will explore the various technologies that are in use to achieve communication with satellites and any vulnerabilities that have been present in the software/hardware of those devices. Further, this project will investigate remediations to these vulnerabilities and any challenges associated with implementing them.

Introduction

Wireless communication use continues to become more prolific every day. It is estimated that by the end of the year 2021, mobile telecommunication subscriptions increased to 8.65 billion subscriptions (Taylor, 2023). As the world continues to become more dependent on this technology, it is important to review the security associated with communications. Since this technology carries sensitive information, it must be secure and protected from tampering.

Within the area of wireless communication is a branch focusing on space communication. Instead of low power wireless LANs and cellular networks, these transmitters have powerful antennae on Earth and satellites in orbit that can cover vast swatches of land. Since the first satellite launched in 1957, communication between Earth and space has become an important part of daily life (UNOOSA, n.d.). Today, GPS accurately locates devices, companies like Starlink connect devices to the internet, television can be viewed via satellites, and much more. According to the UN Office for Outer Space Affairs there are around 12,000 active objects orbiting the Earth (UNOOSA, n.d.). These objects produce terabytes of data daily and serve so many purposes that security is a necessity (Stevens Institute of Technology, 2023).

Cyber security in space is an emerging threat landscape where security has mostly been covered by obscurity and lack of transparency. Most satellites are years outdated, and it is no simple task to update software/firmware of a satellite that is orbiting in space. This paper will explore the various concerns associated with this emerging field and provide insight into space communication.

History of Satellites

On October 4th, 1957, Sputnik 1 was launched by the Soviet Union and marked the first time that a man-made satellite orbited the earth (Britannica, n.d.). This event, historically, is linked to the start of the space race which would span decades in the 1900s. Sputnik 1 was a sphere with 4 antennae attached and was only capable of transmitting low-frequency radio signals back to earth. It lasted for 22 days before the battery died and the satellite failed (Britannica, n.d.). Just a few months later, the US launched their first satellite, the Explorer 1, on January 31st, 1958 (NASA, n.d.). Equipped with more scientific measuring tools, this satellite was much more advanced than Sputnik 1 and made the first discoveries in space, mainly that the earth is ringed with radiation belts which later were named the Van Allen belts.

Just later that year, on December 19th, 1958, the US launched the first satellite in space that relayed voice communication. This satellite had a prerecorded message from President Dwight Eisenhower and broadcasted via shortwave radio the message “…wish for peace on Earth and goodwill toward men everywhere” (Britannica, n.d.). Dubbed SCORE, this satellite was the first to play human voice in space and broadcast to Earth. Although the transmitter was weak, and only specifically tuned radios on Earth were able to pick it up, this still marked the beginning of space communication (Smithsonian, n.d.). Earth to space and space to Earth communication was now possible. Within the next 5 years, satellite technology drastically improved, and satellites were broadcasting television images, being passive reflectors of communication, being recharged with solar panels, and using amateur radio to communicate. With the launch of Telstar 1 on July 10th, 1962, and Relay 1 on December 13th, 1963, high-speed data, television, and telephone data was spanning the Pacific. The Relay 1 satellite was the first to transmit data across the Atlantic and was used to broadcast the 1964 Olympic Games in Tokyo to the US in tandem with the satellite Syncom 3 (Smithsonian, n.d.). Since then, satellites have grown more complex and technologically capable, being able to carry terabytes of data daily and processing high-speed connections.

Breakthroughs in technology and space communications continue to occur to this day with systems being able to support much higher bandwidth and features. The future of satellites and the frontier of space will continue to grow and become more important as the years go on. Especially as humanity looks towards the stars and navigating to other planets, communications between the Earth and other planets will be essential, and those systems will need to be properly secured and protected. To understand the risks to satellites, an understanding of how they work is essential.

How Satellites Work

There are three types of orbital satellites that are placed into Earth’s atmosphere. These operate in the Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Earth Orbit (GEO). LEO exists between 100 and 1,000 miles above the surface, MEO exists between 6,300 and 12,500 miles and GEO exists at 22,236 miles (Britannica, n.d.). The Van Allen radiation belts make it impossible for satellites to operate between each of these orbits as the electronic components are fried due to the radiation. The LEO and MEO bands are often used for satellites that need quick transmission like voice service and mobile communications as the latency is fairly low. To provide coverage to the entire Earth, there needs to be between 20 and 40 satellites in these bands and tracking is needed to coordinate with the positions of the satellites at any given time. Conversely, in the GEO band, a total of 3 satellites can cover the entire Earth and the satellite’s position will remain fixed above a point on the Earth allowing for easy communication. The satellites’ positions in GEO are often used for broadcasting as the delay can take up to 0.22 seconds from satellite to the ground (Britannica n.d.).

In a communication satellite, signals are relayed from one spot on Earth to another. There are three steps to this: uplink, internal processing, and downlink. In most cases, a single source will uplink the data to the satellite. The satellite will then broadcast that same signal down to one or more other sources (Woodford, 2023). An example of this is commercial satellite television. The network station creates the channel lineup and tv guide and will send that data to the satellite. The satellite processes the data, does some manipulations to enhance frequency and signal, and then downlinks to its covered area, providing customers access to television. Likewise other satellites that are used for research, photography, or military follow the same principles. Military grade satellites are built with more security in mind and access to them for research purposes is off limits, so little is known about their entire capabilities. Other purpose satellites like GPS skip the uplink step and only provide downlink data to receivers. Since it takes a powerful antenna and source to uplink, GPS satellites just provide customers with downlink data and the end device trilaterates its own location from gathered data streams from multiple satellites. (Woodford, 2023).

The actual physics of launching a rocket and getting it into the proper orbit is quite intricate and complicated. Even maintaining the proper orbit is challenging once there. But besides the logistical challenges of setting up the satellite, there are many cyber and physical challenges that satellites face once active.

Challenges of Satellites

Satellites come with a variety of challenges that range from physical to cyber. Each satellite launched has to contend with intense temperatures, the vacuum of space, radiation, lack of maintenance, and a limited physical body (Britannica, n.d.). Since launching things into space is costly, the weight of the satellite must be limited. That means that all parts of the satellite must be self-contained and built to last for years with little to no assistance. The Falcon 9 rocket from the US has launched satellites with an average cost of $51-65 million per launch. This is equivalent to $2,600 per kilogram of weight (Roberts, 2022). This means that satellites are made to last as replacing them and putting new satellites in orbit is costly and time consuming. Finding older satellites with outdated technology and parts is not uncommon. Many of these older satellites, and even many newer ones were not built with security in mind, leaving space a very vulnerable frontier.

Another issues that satellites face is a limited fuel supply. Although satellites are recharged with solar panels, the internal fuel that corrects the satellite’s position is finite. Once this fuel supply runs out, the satellite will slowly lose its position relative to the earth due to gravitational pull and slowly fall into the atmosphere and burn up. This limits their lifetime to however long their fuel supply can last.

Dangers to Satellites

Satellites are rife with inherent dangers and vulnerabilities. There are many attack vectors that can affect them as well. The dangers associated on the satellite end include jamming attacks, directed energy attacks, missile attacks, and other space debris (DIA, 2022). Jamming attacks are possible on any sort of wave communication and satellites are no exception. Depending on distance of the satellite, these jamming attacks may need sophisticated, high powered equipment to block the signals to the satellite. This can be accomplished in two ways, either uplink jamming or downlink jamming. In uplink jamming a device will transmit a high powered frequency at the satellite to prevent it from receiving any other ground signals. In downlink jamming, a localized ground source sends out specific frequencies that interfere with the signal in that area (DIA, 2022). In either case the goal is to deny service of the satellite.

In directed energy attacks, high powered microwaves or lasers are used and pinpointed directly to a satellite. These are designed to either temporarily blind cameras, break sensors, or otherwise incapacitate the satellite. Since these sensors and hardware are not designed to withstand these directed attacks, the satellite may just be temporarily impacted or taken offline altogether, and a replacement becomes necessary (DIA, 2022). Another attack is kinetic anti-satellite missiles. These missiles are similar to ICBMs and are launched with a satellite target. The missile will find its target and detonate, destroying the satellite completely. The last risk is other space based weaponry. Other orbital satellites can be equipped to cause harm to other satellites through lasers, jammers, chemicals, microwaves, collisions, or other physical methods. Since physical security in space is almost nonexistent, other satellites have direct access to the physical medium and can destroy fellow satellites (DIA, 2022).

Most commercially launched satellites have little to no security in mind and are often protected with security by obscurity. (Burgess, Willbold, 2023). Since many companies use proprietary firmware and software, the source code is not out there to be analyzed and reverse engineered. Most of these systems also “…are not built by software developers. They are built by aerospace engineers, for the most part.” (Burgess, Falco, 2023, para. 13). Since most satellites are designed to orbit well and are produced by engineers, not a whole lot of security design goes on in the software. The idea that an extensive cyber attack could be performed against satellites is not something that is often considered. For the most part attacking a satellite is difficult work, the proper connection needs to be established, the firmware and software needs to be exploited, or payloads crafted. Also, satellites can be protected with encryption or access codes and determining the correct sequence is difficult, making a cyber-attack even more difficult to perform.

The idea that satellites could be attacked and need to be properly secured really came to mind with Russia’s attack on Ukraine in 2022 (Laursen, 2023). Russia was able to launch a denial of service attack by jamming satellites and taking Viasat satellites offline across Europe (Laursen, 2023). These attacks helped prove just how defenseless satellite communication is and increased the preparations against future attacks. Russia proved that knocking GPS offline in areas was not far fetched and had steep consequences to systems that relied on GPS. The easiest attack vector against satellite communication is against the base stations on Earth that act as command and control (Gent, 2021). Gaining access to these systems could open many avenues of attacks and release sensitive information that is traveling through the satellite. Though satellites face many different challenges and attack vectors, there are many things that companies are doing to better protect these communication channels.

Protections and Remediations

As companies and governments begin to see the growing use of space communication and warfare, future satellites will have better protection. Currently, techniques like spread spectrum modulation, temporal and transform-domain adaptive filters, improved antennae, and cryptographic improvements are being implemented (Laursen, 2023). Most of these techniques mentioned improve on the physical wave medium that is being sent and are useful to avoid jamming attacks. By utilizing spread spectrum, jamming against a specific frequency will be ineffectual since many frequencies are being alternated between to communicate. Also using adaptive filters can help improve echo cancellation, channel equalization, and noise control. (Spanias, n.d.). All of these will improve current signals and reduce the ability to perform jamming attacks. By increasing the cryptological layer, satellites will be better protected as only authorized entities will be able to access them. By securing and checking for proper validation and access, the chances of access by a rogue user is decreased.

The US government branch NIST has released draft guidelines to help companies develop and cultivate best security practices on satellites. (Laursen, para. 15). Other considerations are taking place by building large constellations of satellites so that if one were to be taken offline then plenty of others could take over and knocking a single node offline will not impact the overall network (Gent, 2021). The biggest change will be having built in security design to the entire process and writing of software to be used in satellites. But since space-cyber warfare is such a new concept, governments are still trying to determine what to do about it. Laura Grego, a Nuclear Security Fellow at MIT, says about cyber-attacks on satellites: “I would call those activities concerning, because there isn't a shared understanding of where the thresholds are for retaliation” (Gent, 2021, para. 5). What this means for the future is unclear as space will become another frontier for cyber related incidents.

For now, like all other wireless communication, Earth-space communication is improving and becoming more secure. With an increase in relevance and as attacks become more common, the security in satellites must respond and adapt. Although there are many challenges associated with protecting satellites, there are solutions out there and security is being improved by using better cryptography and utilizing spread spectrum in transmission. Satellites communication will continue to grow in importance and the security of such systems is a top priority especially if these devices stay in the atmosphere for decades of operation.

Works Cited

Burgess, M. (2023, July 20). *Satellites are rife with basic security flaws*. Wired. <https://www.wired.com/story/satellites-basic-security-flaws/>

DIA (2022). *2022 challenges to security in space - Defense Intelligence Agency*, [www.dia.mil/Portals/110/Documents/News/Military\_Power\_Publications/Challenges\_Security\_Space\_2022.pdf](http://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf)

DIA (2019). *Challenges to security in space - U.S. Department of Defense*, [media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF](https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF)

Encyclopædia Britannica, inc. (n.d.). *Development of satellite communication*. Encyclopædia Britannica. <https://www.britannica.com/technology/satellite-communication/Development-of-satellite-communication>

Gent, E. (2021, December 17). *What might war in space even look like?*. IEEE Spectrum. <https://spectrum.ieee.org/space-cyberwar>

Laursen, L. (2023, July 25). *Satellite signal jamming reaches New Lows*. IEEE Spectrum. <https://spectrum.ieee.org/satellite-jamming>

NASA. (n.d.). *10 things to know about explorer 1, America’s first satellite - NASA science*. NASA. <https://science.nasa.gov/missions/explorer/10-things-to-know-about-explorer-1-americas-first-satellite/>

Roberts, T. G., & Kaplan, S. (2022, September 1). *Cost for space launch to low Earth Orbit- Aerospace Security Project*. Aerospace Security. <https://aerospace.csis.org/data/space-launch-to-low-earth-orbit-how-much-does-it-cost/>

Schauer, K. (2023, August 9). *Space communications: 7 things you need to know*. NASA. <https://www.nasa.gov/missions/tech-demonstration/space-communications-7-things-you-need-to-know/>

Smithsonian. (n.d.). *Communications Satellite, relay 1*. Homepage. <https://airandspace.si.edu/collection-objects/relay-1-communications-satellite/nasm_A19670216000>

Smithsonian. (n.d.). *Communications Satellite, score*. Homepage. <https://airandspace.si.edu/collection-objects/communications-satellite-score/nasm_A20030091000>

Spanias, A. (n.d.). *Brief survey of time- and frequency-domain adaptive filters*. Arizona State University. <https://sensip.engineering.asu.edu/wp-content/uploads/2020/04/IEEE-IISA-2016-Adaptive-Survey-Explore-compliant-192-spanias-PID4373685.pdf>

Starling, Clementine G. (2021, October 28). *The future of security in space: A Thirty-year US strategy*. Atlantic Council. <http://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/the-future-of-security-in-space/>

Stevens Institute of Technology. (2023, May 11). *When it comes to satellite data, sometimes more is more*. Phys.org. <https://phys.org/news/2023-05-satellite.html>

Systems, C. (2023, September 27). *What are the key factors driving wireless communication system growth?*. Wireless Communication System Growth: Factors, Challenges, and Opportunities. <https://www.linkedin.com/advice/0/what-key-factors-driving-wireless-communication>

Taylor, P. (2023, March 31). *Topic: Mobile communications*. Statista. <http://www.statista.com/topics/1147/mobile-communications/#topicOverview>

UNOOSA (n.d.). *United NationsOffice for Outer Space Affairs*. OSOidx. <http://www.unoosa.org/oosa/osoindex/index.jspx?lf_id=>

Wikimedia Foundation. (2023, March 1). *List of communications satellite firsts*. Wikipedia. <https://en.wikipedia.org/wiki/List_of_communications_satellite_firsts>

Woodford, Chris. (2023, April 11). *How does GPS Satellite Navigation Work?*. Satellite navigation. <https://www.explainthatstuff.com/howgpsworks.html>

Woodford, Chris. (2022, June 6). *How do satellites work?*. Satellites. <https://www.explainthatstuff.com/satellites.html>