Cyber Security Advantages of Optical Communications in SATCOM Networks

A Master's Project
Presented to
Department of Network and Computer Security

In Partial Fulfillment
of the Requirements for the
Master of Science Degree

State University of New York
Polytechnic Institute
By
Cameron Baker

Under the Supervision of
Dr. Hisham Kholidy, hisham.kholidy@sunypoly.edu

December 2020

Cyber Security Advantages of Optical Communications in SATCOM Networks

Declaration

I declare that this project is my own work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Cameron Baker

02/29/2020

Executive Summary

Space-based communications, whether it is ground-to-space or inter-satellite communications have so far been primarily within the RF spectrum. With the increase in space missions and the need for larger amounts of data being sent to and from satellites, the near infrared or optical spectrum has started to become more widely used instead of RF. Higher bandwidth is not the only advantage of using optics for communications over RF, there is also an inherent security advantage as well. Currently, there is far too little enforcement of security standards for space communications networks, and the use of RF only worsens the problem due to its very large beam spread when compared to optics. This paper will seek to prove that optics is a far more superior technology to be used for space communications networks from a security standpoint as well as providing an increase in available bandwidth. These points will be proven by first introducing the technology by examining current Free Space Optics (FSO) systems and space optics systems being provided by manufacturers. Secondly, this paper will discuss the current state of space communications security, and issues space communications networks are facing using RF with the recent advancement into low-cost SmallSat operations that threaten existing space vehicles, and the lack of standard security practices within these networks. Lastly, this paper will provide evidence into why optics communications can improve the security of spaced based communications due to its lower beam spread and the ability to incorporate quantum key distribution into the communications channel.

Keywords: Cybersecurity, Optical Communications, SATCOM Networks, 5G systems, Quantum Key Distribution

Contents

Table of Figures

Chapter 1: Introduction

1.1 Space Optical Communications

Utilizing space technology is no longer viewed as an activity that only nations and the vastly wealthy can be involved with. With the current era of commoditizing space smaller companies, universities, and independent organizations can afford to launch satellites into orbit to perform a variety of tasks. Many of these groups are not concerned with security measures that should be followed to protect these assets from ground-based or space-based security threats. This paper aims to provide information to IT professionals who are already familiar with cybersecurity practices and concepts that should be deployed on terrestrial networks. The information being provided will help to highlight the threats that unsecured space communications networks can pose, as well as solutions to these problems. Additionally, this paper will go into great depth discussing ground-to-space optical links and inter-satellite optical links. A prior understanding of optical communications, primarily fiber optics, is assumed since many of the concepts used in the previously stated technologies use the same concepts as fiber optics.

To understand space-based optical links a basic understanding of Free Space Optics (FSO) is required. FSO is a similar technology to fiber optics but the primary difference is that instead of the modulated light wave being transmitted through a fiber optic cable it is instead sent over laser pulses through open space. This distinction enables fiber optics speeds but over a wireless channel. The range of FSO is however greatly decreased when compared to fiber optics due to the added attenuation created by sending a laser beam through the atmosphere, additionally, adverse weather can make the link even less reliable. Some of the advantages of FSO over fiber optics and RF-based wireless networks are that it is

much cheaper to set up than fiber optics, it uses an unregulated EM spectrum, it does not interfere with other EM transmissions, and it is highly immune to interception and jamming [1].

Space-based optical links use the same technology present in FSO but instead of the transmitter and receiver being terrestrial-based one can be while the other is in space or both may be in space. This paper will focus on ground-to-space links as well as inter-satellite links. In a ground-to-space optical link, the disadvantage of having to send the beam through the atmosphere is still present which reduces the potential bandwidth of the link since error correction will need to take place to ensure the data is received properly. In inter-satellite links, however, since there is little to no atmosphere in orbit inter-satellite links can transmit data across thousands of kilometers at speeds in the Gbps range.

1.2 The Need for Optical Networks in Space

Most communications performed with space vehicles both within Earth's orbit and without has historically been primarily within the RF spectrum. Up until recently RF has been sufficient to provide enough bandwidth for most space communications, but with greater amounts of data being transferred and with new higher data requirement missions being launched the increase in bandwidth provided by optical links is causing many vendors and consumers to turn to this new technology instead of traditional RF links.

Fiber optics networks are used worldwide as the backbones of the global communications networks, these cables are costly to build, install, and maintain and are limited by constraints of geographical topology. Some companies have seen an advantage in moving high-speed data networks to Low Earth Orbit (LEO) satellite constellations using inter-satellite optical links as their backbones. This method of creating highspeed networks will save on costs concerned with running fiber optics cables and allows connections to be made anywhere in the world so long as a transceiver can be placed at both ends.

Higher bandwidth is not the only reason space communications networks should start to migrate away from RF and consider optics instead. There are certain inherent benefits to optical links that make them more secure than RF. For many satellites currently in operation, and for many vendors that currently

provide commercial satellites security is not a large concern. In the past, many space fairing organizations assumed that the cost of entry and the complexities in satellite communications (SATCOM) inhibited most cyber threats to very large corporations or governments. This assumption, however, is no longer valid, with improvements in computing technology, tracking systems for ground-based communications to satellites has become easier allowing attackers to transmit telemetry control information to insecure satellites, or allowing them to easily intercept transmissions being sent by satellites in orbit. Ground-based threats are not the only concern to SATCOM networks, with the introduction of small satellites (SmallSats) the costs for getting satellites into orbit have greatly decreased, allowing much smaller private organizations to pose a significant threat to insecure SATCOM networks if they can position their satellites in such a way to intercept transmissions.

1.3 Space Communications Security

The fundamental security issues with SATCOM is an issue that will be discussed in greater detail and should be addressed in many ways, this paper will show the advantages optics has over RF that can further improve the security posture of SATCOM networks. The primary advantage optics has over RF is that optical links have a much smaller beam spread than RF, this decrease in beam spread makes optics much harder to intercept and harder for ground-based threats to transmit to a satellite in orbit. Additionally, Quantum Key Distribution (QKD) is a relatively new way to securely transmit a shared key between two parties that theoretically makes it impossible for a man in the middle to intercept traffic without being detected. In traditional RF links, QKD requires an additional quantum channel to transmit the shared key, however, in optics this can be performed over the standard communications channel allowing satellites that use it to be made cheaper and lighter since they do not require two transceivers. RF signals are also very susceptible to jamming from other stronger RF signals, jamming of an optical link on the other hand is far more difficult since it would require precise targeting of the receiver to interfere with the legitimate communications traffic.

1.4 Overview

Currently, the security posture of SATCOM networks is far too lax, many organizations either incorrectly assume that attacking satellites in orbit is too costly and complex to be targeted, or commercial companies attempting to be competitive don't provide security to keep costs down. The goal of this paper is to bring to light the inadequacies of SATCOM security, the threats that currently exist to these networks, and possible solutions to improve SATCOM security. The idea that optics networks should start to replace RF for SATCOM networks will be made as well stating the security advantages provided by the technology. The points will be shown in the following sections by first describing the technology and how it compares to RF on a technical level. Next, this paper will discuss the current state of optics communications in SATCOM networks including current providers selling equipment and services, the near future networks currently being set up, and why providers are shifting to highspeed satellite constellations for global communications networks. This paper will then take a deeper look into the current state of security for SATCOM networks, why it is in such a state, and how changes may be made to improve the security posture. Lastly, this paper will go into detail describing the security benefits optics has over RF and why efforts should be made to transition away from RF networks to optical ones for SATCOM.

Chapter 2: Technical overview of RF and Optics

2.1 RF review

Current satellite networks using RF operate in the EM spectrum range from 1-40 GHz, using L-band, S-band, C-band, X-band, Ku-band, K-band, and Ka-band. The primary uses of these bands can be seen in Figure 1.

Band	Frequency Range	Use
L-Band	1-2 GHz	Global positioning system (GPS), satellite phones
S-Band	2-4 GHz	Weather radar, communications satellites used by NASA to communicate with the ISS, and the Deep Space Network (DSN)
C-Band	4-8 GHz	Satellite TV, communications with areas prone to rainfall
X-Band	8-12 GHz	Primarily used by the military as radar, and with the DSN
Ku-Band	12-18 GHz	Communications satellites in Europe for direct broadcast satellite services
K-Band	18-26 GHz	DSN
Ka-Band	26-40 GHz	Communications Satellites

Figure 1: RF bands and uses [2] [3]

To give rough estimates of the potential bandwidth these RF bands can provide the Shannon-Hartley theorem can be used which states $C = Blog_2\left(1 + \frac{S}{N}\right)$ where C is the channel capacity in bits per second, B is the bandwidth of the channel in hertz, S is the average received power in watts, and N is the average power of the noise in watts. Assuming a Ka-band link operating at 30 GHz with a power of 10 watts and

a noise level of 2 watts the potential bandwidth of that link will be roughly 208 bps. This equation shows how the increased frequency of a link correlates to the increased data rate of the channel, as well as how the power provided contributes to the data rate as well. These calculations will be performed again in the following section to show how FSO and optical frequencies contribute to much higher available bandwidth.

Another key factor to consider when comparing RF to optics is the differences in the beam spread of the two signals. Beam spread is the measure of the entire angle from edge to edge of the transmitted waveform. The term beam divergence is also used when discussing an EM wave which is the measure of one edge of the waveform to the center, making beam divergence essentially half of the beam spread. Figure 2 illustrates the difference between the beam spread and beam divergence. Beam divergence is proportional

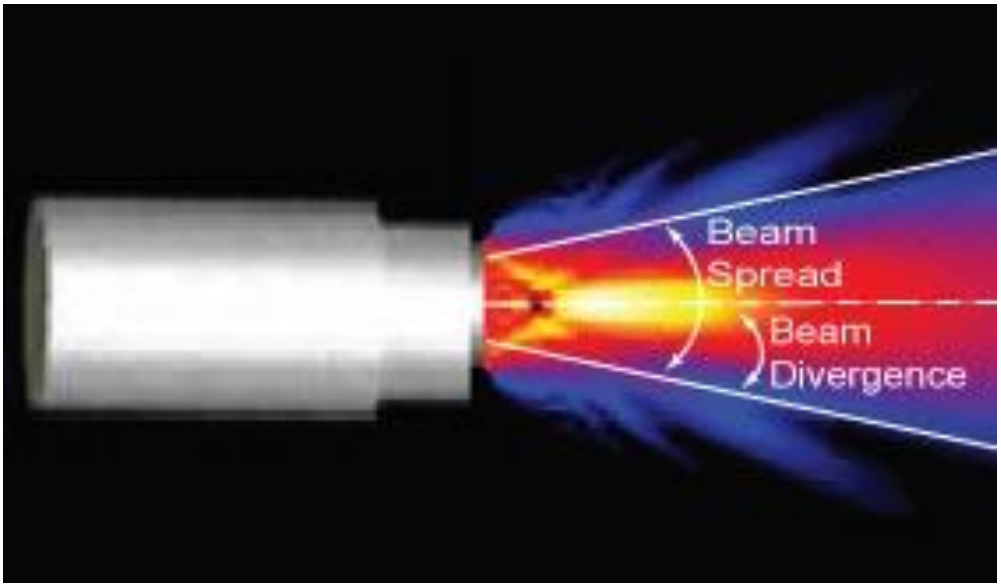

Figure 2: Beam spread vs divergence [7]

to the wavelength of the beam as can be seen with the following equation that can be used to calculate the beam divergence of a beam $\theta = \frac{\lambda}{\pi\omega}$ where θ is the beam divergence, λ is the wavelength, and ω is the beam

waist or the radius of the beam at its narrowest point[1]. Knowing frequency can be converted to wavelength with the formula $\lambda = \frac{c}{f}$ where c is the speed of light in a vacuum (299,792,458) and f is the frequency, the frequency of a Ka-band 30 GHz signal can be converted to a wavelength of roughly 10 mm. Using these numbers the beam spread of a 30 GHz signal can be calculated to show that given a 1 mm aperture the beam divergence of the wave would be roughly 3183 mrad which means at a range of 10 m from the aperture the diameter of the beam would be roughly 32 m wide[2]. These calculations will be performed again in the following section to show how the increased frequency of optics contributes to the reduced beam spread of a beam.

A key aspect that will be discussed further in this paper to argue the benefits of optics over RF has to do with how optics is more resilient to jamming. Jamming of an RF signal is when a malicious signal with higher power and the same frequency than the legitimate signal is directed at the receiver of a communications channel. This higher power malicious signal then denies the legitimate signal from getting interpreted by the receiver, effectively resulting in a denial of service in the communications link. Signal jamming has been used by governments, private organizations, and individuals for many years for nefarious acts and to gain battlefield advantages over their enemies. RF is especially susceptive to jamming due to the large beam spread of the signals. Beam spread contributes to the ease of jamming because it allows attackers to have much more freedom in the direction they point their jammer knowing that the signal will greatly spread out ensuring that the receiver will detect it and fail to detect legitimate traffic. The following section will go into greater detail regarding the spread of an optical signal and show how a smaller beam spread makes jamming of an optical signal significantly more challenging. Another vulnerability inherent with the large spread of an RF signal is that it makes interception of the signal very easy for an attacker. Since an RF signal, at a significant range can spread out to become many kms wide an attacker only needs

[1] For the purposes of all the calculations within this paper the beam waist will be at the aperture of the transmitter.

[2] Calculations within this paper to determine the area of the beam after a given distance are being performed at https://www.laserworld.com/en/laserworld-toolbox/divergence-calculator.html#divergence

to have a large enough receiver within that area to pick up the signal. It is for this reason encryption is used to keep data safe when transmitter over RF.

2.2 FSO

FSO is a communications technology used today that transmits data over laser pulses instead of fiber optics. FSO is conceptually the same technology used in optical SATCOM networks but is a much more mature technology. Therefore, a basic understanding of FSO can be applied to understand the newer technology of space-based optical networks more easily and how it compares to RF.

The first major difference FSO has over RF is the spectrum used by the technology, where RF resides within the range of 1 GHz to 40 GHz FSO uses frequencies within the visible light spectrum into ultraviolet

Laser	Wavelength [nm]	Laser/LED power	Beam divergence	Application
Matrics LEDs	450	6 W	180°	Underwater communication
Nd:YAG	532	250 mJ 12 ns	110 µrad	Deep space mission
LD	532/486	5 W	180°	Underwater communication
LD	785	25 mW	1 mrad	Ethernet
AlGaAs	830	60 mW	6 µrad	Inter-satellite communication
Argon-ion/GaAs	830	13 W	20 µrad	Ground-to-satellite link
VCSEL	850	9 mW	3.5 mrad	Last mile link
LED	800–900	bd	17 mrad	Communication between buildings
LD	1550	113 mW	50 mrad	UAV-to-UAV link, L = 2km
LD	1550	200 mW	19.5 µrad	Ground-to-UAV link
QCL	8400	740 mW (100ns, f = 1 MHz)	2 mrad	Laboratory FSO link (IOE MUT)

Figure 3: Applications of FSO [1]

which is in the 100s of THz range. Figure 3 shows a few applications of FSO with information such as wavelength and beam divergence. The wavelengths used by ground-to-satellite and inter-satellite applications equate to roughly 813 THz. Using this information, the potential bandwidth of an inter-satellite link can be calculated with the Shannon-Hartley theorem using the same received power and noise as the RF calculations made earlier (S= 10 watts, N=2 watts), this shows that the potential bandwidth of this link would roughly equal 297 bps. This is a 40% increase in data bit rate over a 30 GHz Ka-band signal which can provide 208 bps.

Due to the high frequency that FSO uses this directly relates to its divergence making it much smaller than that of an RF signal. Using the same calculation as previously used to calculate the beam divergence of an RF wave it shows that an FSO signal with an 830 nm wavelength and a 1 mm beam waist at the aperture has a beam divergence of .264 mrads meaning that in the distance of 10 m the 1 mm beam would spread to be 4 mm wide. This is far less of a spread than an RF signal resulting in a more concentrated signal at the receiver. This concentration at the receiver has the benefit of requiring less power from the transmitter to send the data since less of the signal is dissipating around and past the receiver. This very small beam divergence also makes FSO very difficult to jam or interfere with, since jamming relies upon overloading the receiver with noise so that the legitimate traffic gets dropped, the small divergence of an FSO link makes it very difficult for an attack to target the receiver accurately enough to jam it. Additionally, since FSO requires the precise targeting of the transmitter to receiver unless an attacker can intercept the line of sight (LOS) of the beam, he/she will be unable to intercept the traffic. It is for these reasons that FSO is used very heavily in military applications to protect transmitted data from attackers [1].

Fiber optics is another optical-based technology that benefits from the increased bandwidth of light to transmit far greater information than RF. FSO can attribute much of its success to the advancement of fiber optics since the two technologies share many attributes in common. For example, all of the previous research and work that has gone into advancing modulations techniques like OFDM and DWDM to transmit as large amounts of data over an optical link can be applied to FSO [4] [5]. The benefit of FSO over

traditional fiber optics cables is due to a couple of advantages the technology offers when compared to fiber optics. The first advantage is that the technology is of course wireless, this aspect allows a communications link to be created without first requiring a physical line being ran. The second advantage is related to the first in that since the technology is wireless setting up a communications link becomes much cheaper and easier than traditional fiber optics. Many companies and organizations around the world spend millions of dollars in establishing and maintaining their fiber optics networks, with FSO only the two endpoints need to be maintained without any fear of a physical line between them being damaged. However, FSO is not a technology that can effectively replace fiber optics since it does have disadvantages when compared to fiber optics. The primary disadvantage FSO has when compared to fiber optics is the reduced range of the link. The range of FSO is limited because it requires a LOS view between the sender and receiver and FSO sends a laser pulse through the atmosphere, within the atmosphere, there is a lot that can happen to a laser pulse that can damage or destroy it. One such action that can happen to a laser pulse traveling through the atmosphere is absorption. Absorption is when the molecules of the gases within the atmosphere absorb the light energy from a laser pulse. Such gases include water vapor, carbon dioxide, methane, and natural gas [6]. A second effect the atmosphere will perform on a laser pulse is scattering. Scattering is when a particle such as those found in dust, fog, or clouds roughly the same size as the light's wavelength deflects the light from its intended direction [6]. Due to these attenuating characteristics, a typical FSO link can stretch roughly 2 to 4 km whereas a fiber optics link can run up to 100 km[3]. It should also be noted that due to the adverse effects the atmosphere can cause to an FSO link adverse weather such as rain, fog, or snow will severely degrade the signal of an FSO link but not a fiber link.

[3] These numbers are without any use of amplifiers.

2.3 SATCOM Optical Links

At its fundamental level SATCOM, optical links use the same technology as FSO however there are a few other concerns that factor into dealing with this technology. The first of these issues is that in SATCOM both the sender and receiver are moving, sometimes in completely different directions and at great speeds. This fact causes two major issues, those issues being doppler shift and the need to point ahead of the target. Point ahead angle (PAA) is the requirement for a sender to target the laser beam ahead of where the receiver currently is because since light has a fixed speed limit when dealing with the distances and speeds of the targets used in SATCOM by the time the laser beam reaches its target it would be at a different location than where it was when the laser beam was sent out [7]. Doppler shift is an effect caused on all waves when the wave originator and receiver are moving in directions away from or towards each other. The

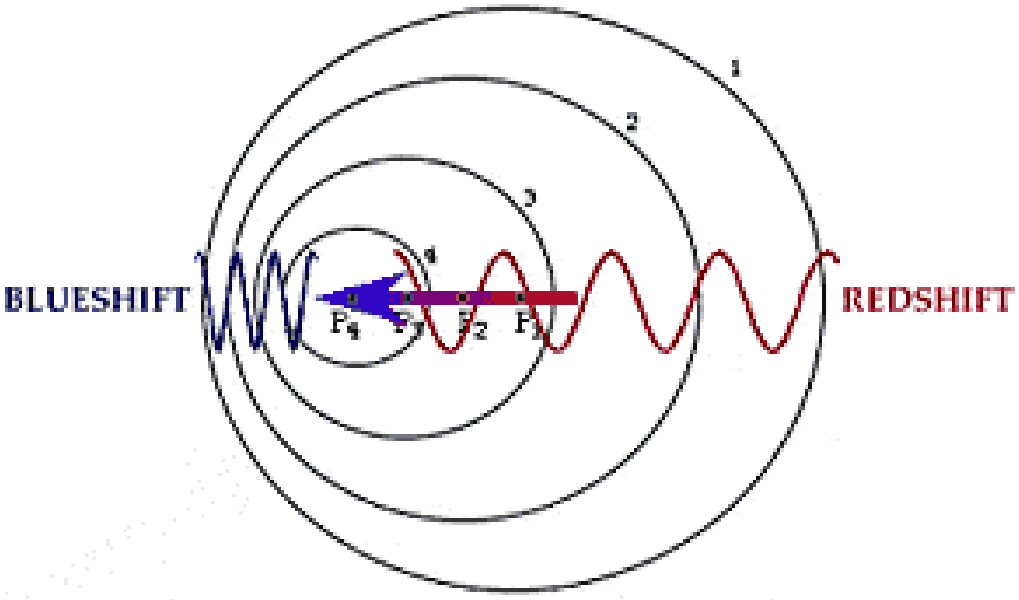

Figure 4: Doppler shift (http://scienceolympiadsbd.blogspot.com/2014/09/doppler-effect.html)

effect doppler shift has on a wave is that it can either compress a wave (increase in frequency) if the two ends are moving towards each other, or it can elongate a wave (decrease in frequency) if both ends are moving away from each other. This shift in an inter-satellite scenario can lead to a ±7.5 GHz shift between satellites in LEO to GEO orbits due to the drastic speed differences [7]. Figure 4 shows the effects of

doppler shift on a wave. To compensate for doppler shift the sender and receiver implement frequency tunning and a local oscillator is used at the receiver to adjust the signal as it enters the receiver.

To deal with the issues of optical links between two moving objects the sender and receiver need to implement an acquisition, tracking, and pointing (ATP) mechanism to ensure both ends of the link acquire each other and properly track each other as they move. During the acquisition phase, a large field of view (FOV) beacon signal is sent by the receiver with PAA considered. Once the receiver detects this signal it uses beam steering elements to point a steady beacon signal back towards the sender. Lastly once the large FOV beacon signal has been found by both the sender and receiver they both begin to narrow the signal down until both ends have locked onto each other [7].

As stated previously FSO is adversely affected by the weather changes and atmospheric turbulence, when dealing with ground-to-space or space-to-ground optical SATCOM links this continues to be a problem that needs to be dealt with. There are two primary methods to compensate for the effect of atmospheric turbulence in ground-to-space/space-to-ground optical links and these include physical layer methods, and TCP upper layer methods. The physical methods that can be used to compensate for atmospheric turbulence include aperture averaging, diversity, relay transmission, adaptive optics, and hybrid RF/FSO systems. Aperture averaging is a technique of increasing the size of the receiving aperture to average out the rapid fluctuations caused by eddies within the atmosphere that causes channel fading. Diversity is the use of multiple smaller apertures instead of a single large aperture to send multiple copies of the signal that are uncorrelated in either time, frequency, or space. This allows the receiver to combine the individual signals to recreate an accurate signal sent out helping to eliminate the effects caused by atmospheric turbulence. Relay transmission is a technique that uses spatial diversity to create a virtual antenna array. This is achieved not by using multiple apertures at the receiver or sender but by allowing multiple terminals to work cooperatively to create a huge diversity gain. Adaptive optics is a technique that attempts to pre-correct the effects of atmospheric turbulence on a beam by changing the optics of the sender/receiver to compensate for the effects of the turbulence. The use of a hybrid RF/FSO system is

essentially conceding to the idea that weather and atmospheric turbulence is unavoidable, but if the link must stay up regardless of whether it will operate at the full optical speeds or the lower RF speeds. In a hybrid RF/FSO system if the FSO link becomes too unstable or attenuated the system will fall back to the RF channel to maintain connectivity [7].

Atmospheric turbulence can be compensated for using methods within the TCP layer as well as the physical layer. These methods can include re-transmission, reconfiguration and re-routing, and quality of service (QoS). A widely used protocol for re-transmission is called automatic repeat request (ARQ) and there are several ways ARQ is implemented. One method of ARQ is for the receiver to send acknowledgments of received packets to the sender, if an acknowledgment is not received by the transmitter in a certain time frame the packet is deemed lost and re-transmitted. The drawback of this scheme is that it causes a large amount of delay, requires a large amount of energy and there are penalties to the bandwidth. Another method of ARQ that is more efficient than the previous one is ARQ selective repeat (SR-ARQ). In SR-ARQ packets are continuously sent to the receiver without waiting for an acknowledgment, the receiver will accept and acknowledge packets and if a packet is not acknowledged within a certain time frame it is re-transmitted. Reconfiguration and re-routing of the signal requires multiple paths from the sender to the receiver so that if one path is causing too much attenuation and data loss the signal can be re-routed to a different, possibly more reliable link. QoS is used in most terrestrial-based networks to prioritize certain traffic over others to get the most out of the available bandwidth of a given channel. The same is true for ground-to-space/space-to-ground optical links, one method of QoS demonstrated uses a buffer to store traffic before sending it in hopes of waiting for the link to clear up before sending the data [7].

Atmospheric turbulence is a problem for terrestrial-based FSO links as well as space-to-ground/ground-to-space optical links, however, inter-satellite links are becoming more popular and in many ways can outperform some terrestrial fiber optics links due to the fact there is little to no atmosphere in orbit which means there is nothing to interfere with the laser beams [8]. Terrestrial based FSO systems are limited to roughly 2 to 4 kms and can run over speeds of 2.5 Gbps, companies such as Tesat and Myarnic are proposing

systems that can operate at speeds of 10 Gbps and with ranges of up to 6,000 km between satellites [8]. These systems and others will be discussed further in chapter 3.

Previously within this paper, only small example ranges have been used to compare the advantages of optics to RF, to signify the advantage of beam spread when dealing with optical links more realistic numbers should be used. LEO altitude is stated to start at 2,000 km above sea level, continuing with the 30 GHz Ka-band signal and the 813 THz optical signal both with an aperture size of 1 mm after traveling from a LEO satellite to a ground station the Ka-band would reach a diameter of 6,366 km but the optical link will end up with a diameter of .528 km[4]. To put that into perspective this would mean that anybody from NY to California with a strong enough receiver would be able to pick up the signal being sent by the LEO satellite transmitting at 30 GHz.

[4] Note these numbers for RF beam spread are without the use of any beam forming techniques which is beyond the scope of this paper.

Chapter 3: SATCOM Networks

3.1 The Commoditization of Space

Historically space missions have only been capable by government organizations with an active space program or working with another government that has one. It has only been within the past 20 years that private companies and even some wealthy individuals have started deploying their satellites for various reasons. The rapid deployment of privately owned satellites typically put in place for economic gain has led to the commoditization of space.

According to David Livingstone, an associate fellow at Chatham House, and co-author of a Chatham House research paper on space and cybersecurity [9] we are entering what he refers to as the third era of space. Livingstone states that "the first era was really represented by programs such as Sputnik and the Apollo missions, which were about national prestige" and that "the second era, to [launch] heavily technological space missions such as very large communications satellites, and Earth Observation (EO) satellites, which provided data for scientific communities, and we also observed the advent of precise navigation and timing systems such as GPS" [10]. Livingstone explains that the first two eras of space have mostly been focused on scientific knowledge and advancement, but now that we are entering the third era space has become an outlet for companies to expand influence for financial gain, hence commoditizing it with payloads that are becoming smaller and more efficient to provide services to consumers at more competitive prices than their competitors.

This commoditization of space is harming security in space communications. Companies generally only care about "the bottom line" and as such are constantly competing with one another to make the most profit and beat their competition to the market. This attitude has led to many providers of SATCOM

equipment to become lax or simply not care at all about security standards in their product [11]. The challenges this aspect poses to space security is discussed further in chapter 4.

Some companies however are not blind to the issues of security in their products, and as such, some are starting to make the move into the optical spectrum to improve security. One such company that now provides optical SATCOM equipment is Tesat. Tesat offers a variety of SATCOM equipment ranging in capabilities from 100 Mbps over a distance of 1,500 km to 1.8 Gbps over a distance of 80,000 km [12]. Additionally, according to their product overview page, they offer this technology not just for the improvements in speed optics offers but also for the security and interference resiliency of the technology, figure 5 shows then laser SATCOM system Tesat offers [12].

Product	Data Rate	Range	Volume	Power Consumption	Mass
Cube LCT	100 Mbps	LEO to ground	9x9.5x3.5 cm^3	8 Watts	360 g
Tosiris	10 Gbps	LEO to ground	25x20x15 cm^3	40 Watts	8 kg
Con LCT	10 Gbps bidirectional	6,000 km	2 subunits	86 Watts	15 kg
Smart LCT	1.8 Gbps LEO to GEO	45,000 km	4 subunits	130 Watts	30 kg
LCT 135	1.8 Gbps	80,000 km	60x60x70 cm^3	150 Watts	53 kg

Figure 5: Tesat product information [12]

However, it is worth mentioning that after questioning a representative from Tesat whether or not they use encryption or any other security practices other than the inherent security advantages with optics I was told they use low probability of detection and low probability of interference (LPD/LPI), which equates to the advantage of the beam being narrower than RF. Tesat also uses coherent detection systems where they filter out the real communications signal from the light spectrum [13]. This shows that even a company that advertises security within their design still is not spending the extra time and effort to implement standard security practices such as encryption within their product.

3.2 Inter-satellite High-speed Constellations

There are other companies now that are deploying systems that will provide high-speed network services to consumers. These systems being deployed are large constellations of many satellites orbiting the earth that are using inter-satellite optical links to create an optical network capable of sending and receiving data at tremendous speeds from anywhere on the planet. As stated earlier these constellations can directly compete with fiber optics networks since they can be cheaper to install and require less maintenance but still provide comparable speeds since there is little to no atmosphere in space to degrade the optical link.

Possibly the largest company currently deploying such a high-speed constellation is SpaceX. SpaceX is a company founded in 2002 and its intent is to "revolutionize space technology, with the ultimate goal of enabling people to live on other planets" [14]. Starlink is the name given to the project by SpaceX and it is planned to be a constellation of satellites using optical inter-satellite channels and RF channels used for ground-to-space/space-to-ground links to provide high-speed communications services to residential, commercial, institutional, government, and professional users worldwide [8] [15]. Some other companies developing optical inter-satellite constellations include LeoSat, Mynaric, Telesat, and OneWeb. Starlink is a system that is meant for a large variety of customers, LeoSat's system is targeted more at large enterprises [8]. LeoSat's solution will use Ka-band antennas for ground-to-space/space-to-ground and optical inter-satellite links similar to the design of Starlink to provide up to 1.2 Gbps speed [16]. Mynaric offers a high-speed satellite network that not only uses optics for inter-satellite communications but also offers it for ground-to-space/space-to-ground or even air-to-space/space-to-air transmissions under certain circumstances. According to Mynaric's technology overview site, they too mention the security advantages of optics over RF stating the beam size being a large contributing factor as well as the ability to integrate QKD into the link [17]. Mynaric even provides information regarding beam sizes for laser, Ka-band, and

X-band signals at varying altitudes as shown in figure 6.

Typ. Scenario	Link distance	Laser beam size	Ka-band beam size	X-band beam size
Air-to-ground link from UAV	50 km	1 m	1,600 m	3,200 m
Air-to-air link of high-altitude constellation	200 km	5 m	6,500 m	13,000 m
Space-to-ground link of Earth observation mission	1,400 km	35 m	45,000 m	90,000 m
Inter-satellite link of LEO constellation	4,000 km	111 m	145,000 m	290,000 m

Laser aperture size: 80mm, Ka-band antenna size: 300mm, X-band antenna size: 600mm. Assuming physical limits for lowest possible beam size.

Figure 6: Beam Spread Comparisons [17]

3.3 Satcom in 5G Networks

As the use of mobile data has been steadily increasing in the last couple of decades the need for faster and higher bandwidth wireless networks has also increased. The newest generation of high-speed mobile networking is being referred to as 5G. The networking specifications that define a 5G network is a network capable of delivering 100 Mbps download speeds with 50 Mbps upload speeds, all while maintaining milliseconds of latency. These speeds are 5 times faster than the average household wireless network in both the US and Europe are fifteen times faster than the global average. To achieve these speeds 5G needs to operate at three times the spectral efficiency of 4G, tripling the volume of data being sent over the same amount of spectrum. Plans for how 5G will be used requires the network to be able to support a million devices within a single square km and be able to maintain a connection to devices that could potentially be moving up to 500 km/h [18]. The requirements for a fully realized 5G network are very large and for such a global network to become possible many different technologies and infrastructures will need to be able to operate together to provide this high-speed network where ever it is needed.

The use of satellites in the 5G network may very well be a requirement to provide the level of coverage and speed needed to create a truly next-generation network. Some satellite providers and equipment have

already reached the 100 Mbps speed needed for 5G such as ViaSat-2 [18]. However, speed is not the primary concern in a 5G satellite-based network, low latency in the communication link is also a requirement, this is the requirement that satellites, unfortunately, fall short. Currently, satellites positioned in a GEO orbit of 36,000 kms have a latency of approximately 500-700 milliseconds, satellites in a LEO orbit of 8,000 kms have a latency of fewer than 200 milliseconds [18]. Both orbits are far from the goal of just a few milliseconds required for 5G. SpaceX, OneWeb, and Telesat have all stated that they plan to have latency as low as 50 milliseconds or less but even that is still a bit too slow for true 5G latency [18]. This does not mean that satellites are not suited for 5G though, there is certain traffic that can be sent over 5G that is less latency sensitive than other data. Video for example can be buffered before playing which would make the latency issue less severe.

Even with the limitations of satellites and the issue they cause when dealing with latency concerns many experts still feel they will be indispensable in building a global 5G network. According to studies run by the 3rd Generation Partnership Project (3GPP) to determine the possible use for satellites in a 5G network, they determined that they would best be used as relay nodes or could act as a backbone for the 5G network infrastructure [19]. In a separate study, the use of satellites to act as active nodes in the 5G network was also investigated [19]. The lead of the European satellite business for the telecom, media, and technology practice at PwC's Strategy& division Theirry Lefort estimates that 5G will need five times as many base stations as the current 4G network [18]. The need for so many base stations could increase the installation and maintenance costs needed for deploying 5G in less populated rural areas. This is why Lefort feels that satellites will be needed since they can cover a much wider area than terrestrial base stations [18]. Additionally, using satellites to provide network access to hard to reach locations is much cheaper than running terrestrial infrastructure. According to a Geneva-based International Telecommunications Union's (ITU) Radiocommunications Bureau counselor Nelson Malaguti satellites can be used to trunk communications from central 5G ground stations to small rural stations to provide seamless global coverage to remote areas such as farms, mines, airplanes, cruise liners, and islands [18]. In this sense, a large satellite

constellation could act as the backhaul for the 5G infrastructure to transfer large amounts of data at high-speeds [20]. One final advantage satellites can provide in a 5G network is that they provide a reliable connection to the network infrastructure in case of natural disasters [20]. Many natural disasters such as earthquakes, hurricanes, and tsunamis can destroy terrestrial based infrastructure making it difficult for rescue workers to provide the best support possible. With the use of satellite network backbones, a rescue team could deploy mobile access points to connect to the satellite network and provide 5G coverage to the local area to aid in rescue operations.

One of the primary uses and need for a 5G network is the need to be able to provide a high-speed reliable network to the ever-growing Internet of Things (IoT). IoT is defined as "data exchange between a large number of devices and sensors connected wirelessly without human interference" [19]. It is no wonder that a need for a network capable of connecting to a million devices within a square km is needed when considering the ever-growing number of IoT devices around the world that require network connections. Satellites become an even greater necessity in the 5G network once IoT becomes a concern. This is because many IoT devices are in very remote locations where the use of a terrestrial connection is either infeasible or in some cases impossible. One such example is a system developed and deployed by Japan that is used to detect tsunamis and report to a monitoring station if one is detected to provide early warnings to locations along the coastline. These IoT devices are deployed on buoys positioned off the coast of Japan and require network access to send data to the base stations [19]. Any terrestrial-based networking solution would be impossible for such a system since running cable to the buoys would either be impractical or far too expensive. In this sense, satellites can provide a much more cost-effective alternative to provide network access to IoT devices [19].

It has already been stated that the use of LEO satellites will provide lower propagation delay and lower information loss than GEO satellites. However, in the case of IoT devices, this delay and information loss is sometimes not enough since many IoT devices lack the higher power transmitter/receivers to communicate with satellites in orbit. A solution to this is described in [19] which argues that the use of a

UAV satellite hybrid network could be used to provide a more reliable network to low-power IoT devices. The paper states that UAV devices could act as intermediaries between the IoT devices and the satellite network to provide a connection to the 5G network for the IoT devices [19]. Using this design principle it would allow the lower-powered IoT devices to communicate with a UAV within range which would have a higher-powered transmitter/receiver that can then relay the connection back up to the satellite network acting as the 5G backbone.

Lastly, one important use satellites can provide when used for 5G to support IoT devices is security. In many IoT system designs, the IoT device does not maintain a constant connection to the network, instead, it will store any data it needs to send waiting for a connection that could be provided by mobile access points that visit the vicinity at regular intervals. This design is used in locations where a constant network connection is unavailable, and the data being sent is not time-sensitive. The major drawback to this design is that the IoT device is unable to receive constant security updates and is therefore vulnerable to security risks. The number of insecure IoT devices in the world is staggering, allowing such things as botnets to be established using IoT devices that can cause insurmountable levels of damage to critical network infrastructure. Granted devices that only connect to a network on occasion are not as great a threat as insecure devices that are always connected, but that still does not mean that they cannot pose a risk. If a connection to the network can be maintained at all times to such IoT devices, it would allow updates to be sent to them as soon as available to secure them from being used maliciously [20].

3.4 The SmallSat Revolution

With the Commoditization of space comes the desire to make satellites smaller and cheaper without sacrificing functionality. This drive has led to the increased use of what are referred to as SmallSats or Small Satellites, also referred to as CubeSats. SmallSats have a range of sizes that the scientific community use to classify them which is as follows:

- A small-satellite has a mass below 500 kg

- A micro-satellite has a mass between 10 and 100 kg
- A nano-satellite has a mass between 1 and 10 kg
- A pico-satellite has a mass between .1 and 1 kg
- A femto-satellite has a mass below .1 kg [21].

A CubeSat is a relatively small and cheap satellite that can be put into orbit alongside other payloads since their weight is small it does not require dedicated launches to get several into orbit. The California Polytechnic State University and Stanford University have created a standard to define the size metrics of a CubeSat. This metric defines a unit or "U" as being a cube with 10 cm edges and a maximum mass of 1.33 kg. Multiple units or fractions of units can be combined to create n-U satellites where n typically ranges between 1.5 and 6 [21].

Due to the low-cost of these CubeSats, the original use for them was for educational purposes, however, their uses quickly expanded to include large communications constellations, startup companies, and earth observation missions. As electronics companies began to drive the price down even further while also improving the performance of their CubeSats this led to even more customers adopting these systems [21]. Figure 7 shows the increased use of CubeSats as well as a predicted further increase into the year 2023.

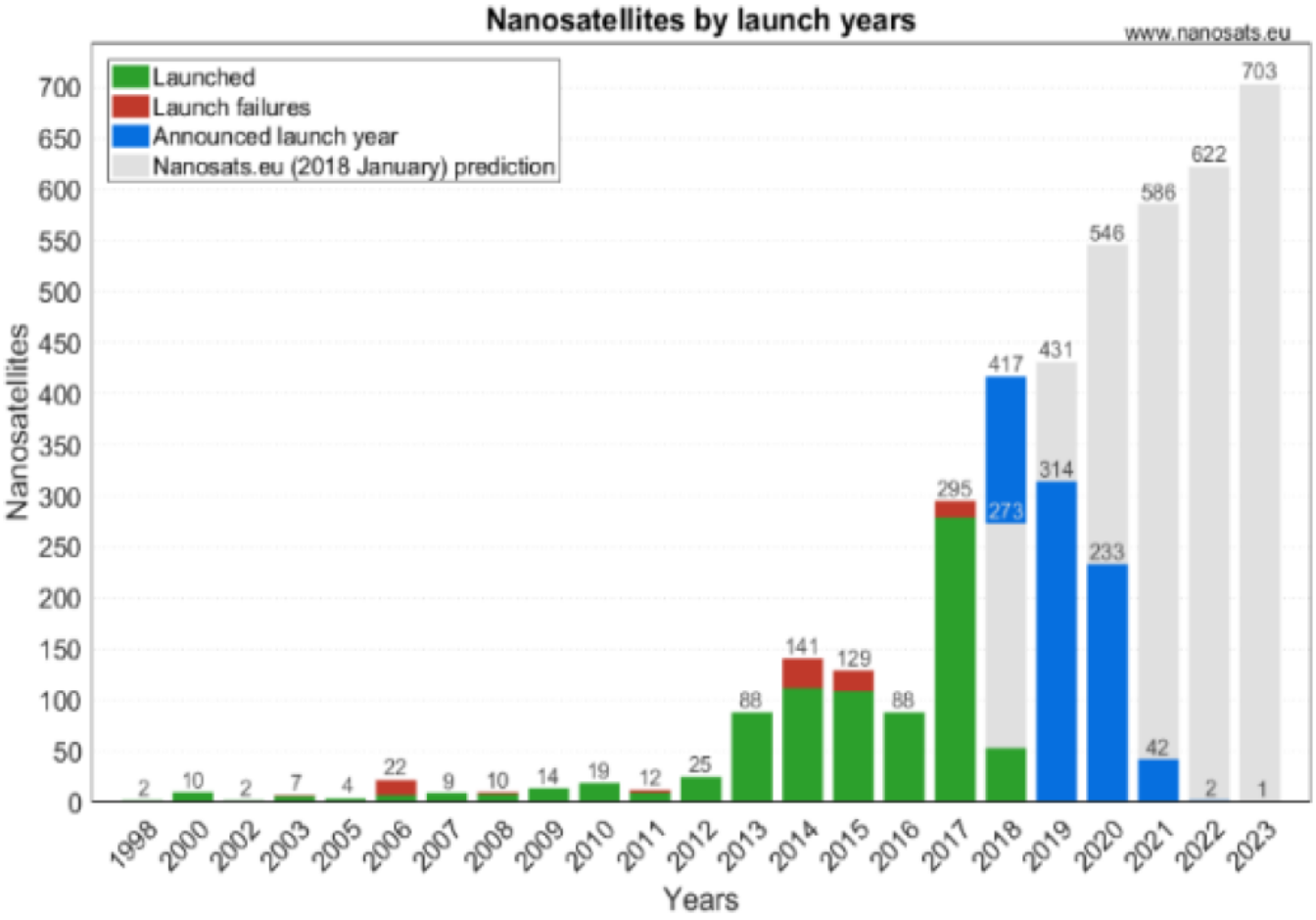

Figure 7: CubeSat Usage [18]

The problem with the increased use of these SmallSats leads to an increase in the lack of security standards that come with the use of them. To reduce cost many manufactures of SmallSats do not make use of any encryption standards with their telemetry control channels. The way the policy is written now all DoD-owned satellites must use encryption, however, there currently is no regulation stating that academic or commercial operators must encrypt up-links regardless of the capabilities of the satellite [21].

The lack of encryption is a serious problem when it comes to SATCOM as it is now and will be discussed further in chapter 4. One solution some organizations are taking to improve the security of SmallSat networks and to improve functionality is the use of optical communications instead of RF. NASA has demonstrated the advantages of using optical links aboard SmallSats in the Optical Communications and Sensor Demonstration (OCSD). OCSD was designed to show that a system designed using customer over the shelf (COTS) components could achieve a near error-free optical link at

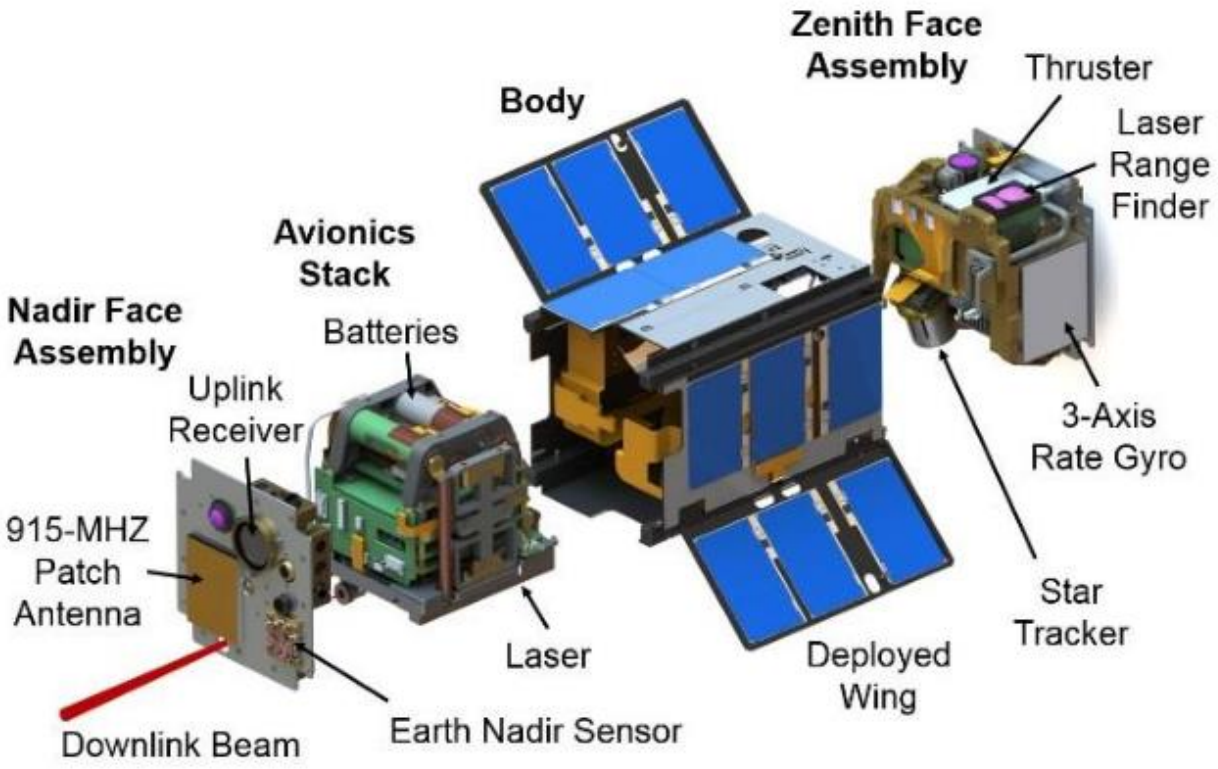

Figure 8: Breakout of OCSD spacecraft [19]

200 Mbps from LEO to ground elevation [22]. Figure 8 shows a breakout of the components used in the

OCSD spacecraft to show the overall simplicity in the design of the craft. OCSD was a demonstration set up by NASA in November or 2017 that used 3 1.5 U CubeSats to demonstrate the first-ever use of high-speed laser communications sent from CubeSats to a ground station as well as an optical uplink to a CubeSat [23]. The CubeSats used in the OCSD mission were equipped with a compact water-based propulsion system that was used to orient the CubeSats to send and receive optical signals since the transceivers were hard mounted to the satellites. Re-orientation of the satellites was performed by using miniature star trackers aboard the satellites to measure the position of stars for navigational purposes. This method of orienting the CubeSat saved on cost and weight of the craft and made it able for the craft to achieve an accuracy of better than .05 degrees, which is 20 times better than similar methods used by CubeSats at the time [23].

Chapter 4: SATCOM Security

4.1 Current State of SATCOM Security

When interconnected computing and the internet started gaining popularity security often was overlooked because most people had the notion that individuals would either not bother to attack it or not have the technical knowledge to do so. This led to several cyber threats in the forms of viruses, worms, and other malware that when compared to modern malware are very primitive since there were very little to no countermeasures to prevent such attacks. This notion of thinking that something is secure because there is a small chance anyone will attack is, unfortunately, the same way many organizations currently view SATCOM. Most individuals assume that the ability to hack a satellite in orbit is either so complex or offers no advantage to the attacker that they ignore security measures that should be in place to protect such assets.

Currently, cheaper and more powerful antennas are making it possible for individual hackers to be able to target satellites in orbit to cause potential damage, or jam communications causing DoS attacks. According to Bill Malik, VP of infrastructure strategies at Trend Micro, during an RSA conference he stated that attacks against NASA satellites are already happening and are known about. He further elaborates using the Hubble satellite as an example of the damage a hacker could do. The Hubble's telescope is very sensitive to light and Malik states that an attacker could point the lens at the sun and open the protective shield effectively destroying the sensitive optics. Additionally, an attacker could use the solar panels to destroy the batteries on the satellite as well [24].

5G technology has given rise to the greater need for more satellites in orbit to provide connectivity for IoT devices around the world. With the increase of satellites being sent into orbit the attack vector is

growing at an unprecedented rate. The increase of unsecured satellites provides a greater number of targets that an attacker can exploit to cause damages or potentially leverage the compromised system to gain further access. According to Todd Harrison, director of the Center for Strategic and Industrial Security's Aerospace Security Project, every satellite should send its data over encrypted channels regardless of the use for the satellite, because if security is not considered the satellite could become a target for hackers [25]. Many of these satellites being used for 5G are being launched with little security concerns in place. Due to the rapid increase in demand for 5G networks, the US military is unable to meet its demand quickly enough and may have to start relying upon commercial providers that are not practicing proper cybersecurity practices [26]. The lack of security practices for these satellites stems from the issue that there is an absence of standardized protocols when it comes to securing 5G networks [26]. These lacking protocols allow manufactures and providers to ignore cybersecurity. The use of satellites with weak cybersecurity practices can open the door for a variety of cyber-attacks including fraud and Satphone abuse. An example of using fraud to attack the satellite networks would be if an attacker were able to force a connection to be routed through satellite infrastructure instead of terrestrial infrastructure. This re-routing of data increases the value of the connection since the use of satellite infrastructure is far more expensive than terrestrial infrastructure, this increase in value can increase the revenue the attacker gains from the attack [27]. Satphones are special phones that connect directly to satellites to create a communications link to make voice calls around the world. This technology allows such devices to operate in remote areas where cell service is not available. Satphones become a problem since they do not need to travel through terrestrial links it makes them very hard to regulate the connection or to control communications access into and out from a geographic location. By abusing Satphones an attacker could bypass such mechanisms in place such as lawful wiretaps to conduct their nefarious operations undetected [27].

The importance of securing satellites becomes very important when the implications of the damage an attack could result in are considered. An example of damages that could be done by compromising a

satellite can be seen by an attack that a Russia-based cyber-espionage group named Turla was able to do by using a ground-based antenna to masquerade as the IP address of a legitimate user when connecting to an ISP's satellite. If an attacker uses such methods he/she could potentially inject data into a communication link between the satellite and an autonomous drone resulting in crashing the drone if desired [28]. Another important service that satellites provide that if attacked could cause large amounts of damage is GPS. GPS relies upon the use of orbital satellites to triangulate the location of objects on the ground to provide accurate location data to the user. By simply jamming the signals used in GPS this service could be blocked resulting in the lack of navigation for critical services such as logistics, transportation, and even GPS-guided missiles [28]. Apart from jamming an even worse case would be to deceive the GPS receiver since from the receiver's perspective nothing is wrong, but the attacker can covertly redirect the target to where he/she wants it to be. This method is referred to as GPS spoofing and one such method to perform such an attack targets the satellite by altering the output signal of the

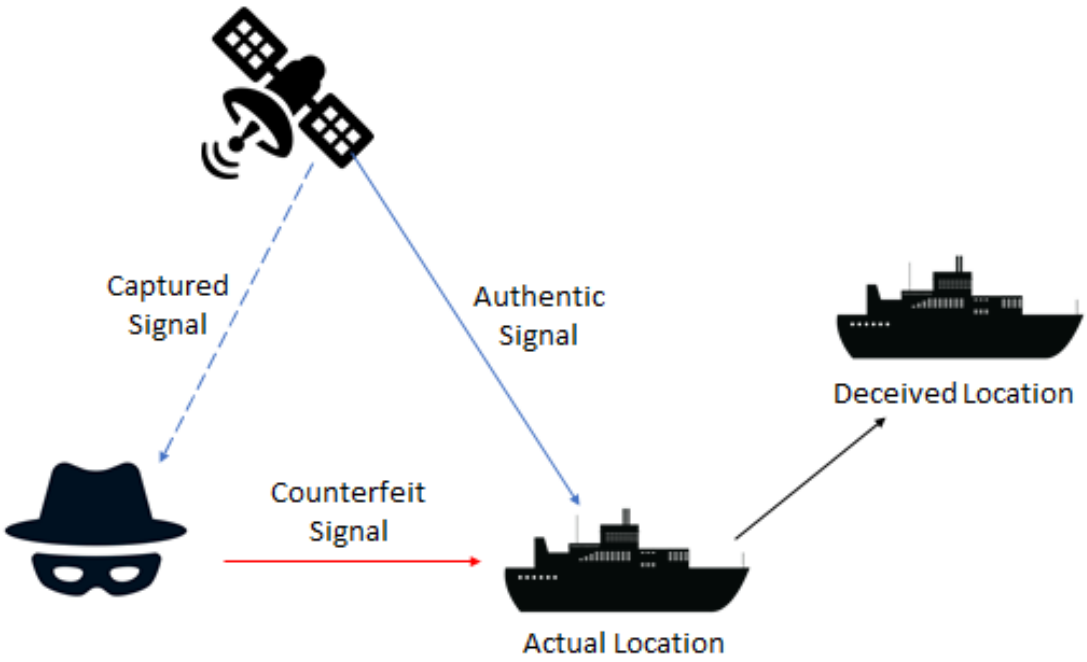

Figure 9: GPS Spoofing

satellite. Figure 9 shows how a malicious party could intercept a legitimate GPS signal and send a

counterfeit signal to the victim making it believe it is at a location that is not accurate. Another method uses software-defined spoofers that insert a weak fake signal behind the legitimate GPS signal. By gradually increasing the power of the fake signal it will eventually override the legitimate signal resulting in the receiver accepting the fake signal as legitimate. Such systems are relatively cheap to construct being shown that one can be assembled with about $1000-$2000 by Professor Todd Humphreys at the University of Texas, Austin [28]. In 2017 one such GPS spoofing attack was performed against 20 ships in the Black Sea resulting in the ships being re-routed 25 nautical miles off from the location the GPS reported the ships being at [28].

Attacks against the satellite systems themselves are not the only attack surface hackers have been able to exploit due to lack of security measures. Ground stations as well need to be protected from traditional cyber-attacks. To express the importance of securing ground stations it should not be overlooked that in April of 2018 a security incident was reported by NASA that compromised their mission control systems. The attack resulted in security officials at Johnson Space Center to temporarily disconnect from the DSN to prevent the attackers from corrupting data on the network. A federal review of the incident found that the attacker was able to target a Raspberry Pi device that was not authorized to be attached to the network and use that access to take advantage of the network's lack of segmentation to move through systems across the entire Jet Propulsion Laboratory (JPL) network [29]. A couple of mistakes were made which led to this attack being so successful by the attacker. First off, the lack of accounting of devices on the network allowed the attacker to target the raspberry Pi granting the initial access to the network. Secondly, segmentation of a network should be a standard security practice that should be implemented, and if was it would have prevented the attacker from gaining as much access as he/she was able to achieve.

Ground stations pose a much larger threat to security since they are more easily accessible by attackers. The use of satellite constellation networks like the ones described earlier from SpaceX and LeoSat greatly reduce the attack surface of these networks since they only utilize ground stations at the

distant ends of the communication instead of hopping back and forth from earth to space along the path of the communications link. Additionally, the use of optics makes it near impossible for an attacker to intercept data due to the complex maneuvering that would be required to place a malicious satellite in the path of the narrow laser beam link. Additionally, LeoSat will use encryption in their constellation network to further improve the communications link between satellites and ground stations [8].

Authors in [36-47] introduced recent researches in developing intrusion detection systems in different domains such as cloud computing and SCADA system security. These papers use different machine learning approaches, These papers will help us adjust their approaches in the 5G network and SATCOM security.

4.2 Challenges to Secure Space Communications

Securing space communications has many challenges to overcome if any real change will ever take place. Many of these challenges lay beyond manufactures and consumers tending to not have as high of concern or awareness of cybersecurity in their SATCOM systems. Three primary challenges that need to be overcome to make a positive difference in the security of space communications include changes within government policies in regards to space travel and launches, changes that commercial entities need to make to improve security, and a cultural change that encourages organizations to become more cybersecurity aware.

For drastic improvements to be seen in space cybersecurity governments will need to lead the charge. However, governments have repeatedly shown a lack of initiative and leadership in providing such policies and guidance. In a report by the U.S. General Accounting Office in 2002, it was stated that efforts towards providing infrastructure protection did not include the satellite industry [11] [30]. A recent paper published by Chatham House states that there is currently no global organization that addresses cybersecurity in space [9]. A solution to this issue is not as clear as one might think, since any

action a government might take to enforce security on space missions could just lead to customers performing launches with less restrictive governments to work around the rules set forth by a more strict government. It is for this reason that a global initiative must be formed that regulates policies for all launches worldwide [9]. The proposal Chatham House mentions that could result in the most successful regulatory regime to address this issue would be in an international organization of willing participants that rather than mandate policies instead will provide guidance and awareness to national regulatory and law enforcement authorities to standardize and improve overall security in space [9].

Governments should be first the organization to adopt cybersecurity practices for space communications since that will trickle down to other organizations and force them to follow suit. However, that should not stop commercial entities from making attempts to improve the cybersecurity of their space systems before law enforcement forcing them to. Many of the issues and challenges posed by government agencies to improve cybersecurity in space also affect the commercial sector. An improvement in collaboration between industries could greatly improve the cybersecurity posture of commercial entities [11]. One proposal that could have positive results would be to include some of the larger space transport industries in the international regime mentioned by Chatham House, this would allow these organizations to provide input into the actions of the regime and therefore provide some central voice that other organizations might follow to improve cybersecurity within their systems [9].

Lastly, the cultural issues in improving cybersecurity in space is a significant challenge to overcome. This issue is like the issue stated earlier when cybersecurity for internetworked computers was viewed as trivial back in the infancy stages of the internet. In an interview with one of the authors of the Chatham House paper David Livingstone, he mentioned that it will likely take a serious disaster such as an attacker de-orbiting an expensive satellite for organizations to realize the importance of cybersecurity in space [10]. Livingstone also mentions that to improve cybersecurity in space a cultural change needs to be seen in addressing security in the entire supply chain of satellite production, all the way down to the chip manufacturers. He states that currently this awareness is not seen and for the most part is disregarded.

Such a change that is needed to improve cybersecurity in space is not something that can happen overnight and hopefully does not require a significant incident like Livingstone mentions for awareness to arise. Hopefully, if governments and industries start to raise awareness of cybersecurity concerns then cultural awareness can raise as well.

4.3 Risks Posed by CubeSats

This Paper previously mentioned the increase in popularity of CubeSats in many consumer, academic, industry, and government space missions. New models of CubeSats have started to be equipped with their form of propulsion allowing them to extend their operational lifespan and perform more advanced missions. Since these are CubeSats and are manufactured in such a way to be cheap and efficient many of them are being designed without encryption on their telemetry, Tracking, and Control (TTC) channels in order save money and beat out competing manufactures. In a paper published by A. Kurzrok of Yale University, M. Diaz Ramos of University of Boulder Colorado, and F. S. Mechentel of Stanford University [21] these insecure CubeSats with propulsion could pose a serious threat to other more expensive satellites if they were to be used as projectiles by an attacker to damage such satellites.

CubeSat propulsion needs to be designed in such a way that the systems are cheap, light, and efficient. There is a host of aspects that need to be considered when discussing propulsion systems which include the total impulse of the system, the specific impulse (Isp), the theoretical velocity change or "Delta-v" (Δv), and the propulsion dry mass fraction. Total impulse is the thrust force the system provides over the run time of the system. Specific impulse is the total impulse per unit of propellant or thrust per unit mass. Delta-v is derived from the Tsiolkovsky rocket equation and is a function of mass loss during powered flight. The propulsion dry mass fraction is a ratio between the propellant mass expended and the remaining structural mass of the craft [21].

For spacecraft propulsion systems there are two primary types which include chemical propulsion and electrical propulsion. In chemical propulsion, thrust is generated when the propellant is combusted and

the kinetic energy from the combustion is harnessed through supersonic expansion through a nozzle [21]. Chemical propulsion is used in all matters of space flight due to the high thrust such systems provide, but the complicated systems are difficult to downsize for SmallSat operations. The types of chemical propulsion that currently exist include cold gas, warm gas, water electrolysis, monopropellant, liquid bi-propellant, solid, and hybrid. Electric propulsion generates thrust by using electrical power to heat or

Propulsion type	Thrust [mN]	Isp [s]	Dry mass ratio	TRL
Cold gas	$0.1 - 10^2$	40 – 80	0.5 – 0.95	9
Chemical reaction	$1 - 10^4$	150 – 300	0.4 – 0.8	6 – 8
Warm gas/ electrothermal	1 – 50	70 – 300	0.4 – 0.85	6 – 9
Electrostatic	0.01 – 10	800 – 5000	0.5 – 0.9	6 – 9
Electromagnetic	$10^{-5} - 1$	500 – 2000	0.8 – 0.99	6 – 9

Figure 10: Performance Metrics of SmallSat Propulsion Options [21]

directly accelerate a propellant. The external power is typically supplied by chemical, nuclear, or solar sources. Electrical propulsion is gaining popularity with SmallSats due to the simpler and more compact design of the systems. However, current systems require significant amounts of power to operate which in some cases is infeasible for a SmallSat to generate. Current research efforts focus on lowering these power requirements for electric propulsion so they could be more widely used on SmallSats [21]. The types of electric propulsion include electrothermal, electrostatic, and electromagnetic. Figure 10 shows the performance metrics of various SmallSat propulsion options. In figure 10 TRL stands for Technology Readiness Level and is a type of measurement NASA uses to assess the maturity level of a technology, the scale ranges from 9 which represents “Actual system flight-proven through successful mission operation” to 1 representing “Basic principles observed and reported” [3].

According to [21] a simulation was run to show the ranges capable of a SmallSat equipped with varying types of propulsion systems currently in use which could potentially be used on SmallSats soon. The propulsion systems include POPSAT/HIP1 by Microspace, 1N-HPGP by ECAPS, Micro Resistojet by Busek, BIT-3 by Busek, and EO-1 by NASA/Primex Aerospace [21]. The SmallSat used in the simulation is assumed to weigh 10 kg with 50% of the total mass allocated to the propulsion system. The craft is simulated to start its maneuver orbiting earth at 300 km in an equatorial circular orbit. The simulation is designed to show that if such a SmallSat was hijacked by an attacker, what would the range capabilities of the satellite be if the propulsion system were engaged to burn until all propellant is expended. Figure 11 shows the quantitative results of the simulation. The figure shows that chemical reaction engines can reach LEO orbit altitudes in less than 2 days and that electric propulsion systems can achieve GEO altitudes but take significantly longer to achieve such altitudes than a chemical propulsion system [21].

Propulsion Type	Maximum altitude [km]	Time of flight [h (days)]
Cold gas	360	480 (20)
Chemical reaction	2110	1.8
Warm gas/ electrothermal	480	27
Electrostatic	35600 (max limit at GEO)	9400 (392)
Electromagnetic	2420	3100 (129)

Figure 11: Range of Propulsion Systems on SmallSats [21]

The results of this simulation are important to note since this shows the potential danger that unencrypted TTC channels on SmallSats can pose. Military applications of Anti-Satellite (ASAT)

systems include the use of Kinetic Kill Vehicles (KKVs) which are crafts designed to crash themselves into other satellites to damage the target satellite. Most satellites in orbit follow very predictable orbits since many of them only have enough propulsion for minor course corrections if they have any at all. This allows KKVs to be very effective weapons since there is little the owner of the target satellite can do to protect their asset. With the increased use of SmallSats with propulsion, these crafts can be used by malicious actors to become KKVs to destroy potentially high-value targets for political, financial, or malicious intents. The vast majority of satellites currently in orbit reside within the LEO range the simulation performed above shows that chemical reaction thrust SmallSat could easily and quickly reach LEO orbit to pose a threat to missions operating at the altitude with little warning to the target operator that a collision is imminent. Furthermore, the simulation shows that electric propulsion systems could even threaten GPS systems[5]and satellites in GEO orbits. Of course with the massive time it would take for the collision to occur such a collision is less likely due to the discovery of the collision event allowing time for maneuvers by the target to avoid it, as well as potential orbital drifting of the target that the SmallSat will be incapable or correcting for after the initial burn. However, one silver lining [21] mentions is that purpose-built KKVs come equipped with systems designed for intercept and kill maneuvers that typical SmallSat systems will not have, but the threat is still there however unfeasible it may seem [21].

4.4 Recommendations to Improve Space Communications Security

With the increased threats that SmallSats with propulsion pose, as well as easier access to transmitters capable of sending signals to satellites in orbit, and the lack of concern for ground station security changes need to be made to secure space communications networks and missions. As stated earlier, changes made to policies and practices is a very difficult undertaking since there is no single authorizing

[5] GPS systems operate at 20,000 km altitudes.

agency for space launches. There are a few recommendations though that should be followed if improvements to SATCOM networks can be made.

The most prevalent security measure that is currently overlooked on SATCOM links is the lack of encryption, specifical encryption of the TTC link. Many products ensure encryption of the data being sent since that is a feature that can be advertised to consumers and therefore make their product more attractive, but many fail to mention that the TTC link is unencrypted which to many consumers would likely not be of concern since that does not threaten their data directly. However, failure to encrypt this link can lead to the hijacking of the satellite system to re-orient or propel to a different orbit. Companies that manufacture TTC modules should start to consider encryption as a standard practice and cooperate to make a self-regulated agreement to provide encryption of TTC links [21]. Currently, space launches have not become cheap enough that any small organization has the means to launch their satellite. Many organizations, including NASA, rely upon third party commercial entities to launch their satellites into orbit. These third-party organizations act as the "gatekeepers" of space missions, it should fall to them to ensure that a certain level of security controls have been implemented to the payload before agreeing to launch. This approach is advantageous over government jurisdiction since commercial organizations tend to be more flexible and can apply such policies quicker than a government entity can [21]. Lastly, the government has to step in to ensure that encryption is a standard requirement for satellites, as mentioned earlier such an act should not be in the form of policies and regulations since that could lead to a backlash and just drive the industry to a less restrictive government. Instead, there needs to be cooperation between governments to ensure that all measures be attempted to ensure encryption is in place.

Ground station security is just as important as security in orbit. Organizations that maintain control stations for satellites in orbit should revisit the basic concepts of securing a network. Segmentation of the network can help keep an attacker from gaining access to critical systems if they can undermine an insecure system on a less critical section of the network. Proper monitoring of assets on the network can prevent an attacker from inserting a surveillance device or backdoor device on the network. Proper

training of staff to recognize phishing attempts or social engineering attempts can prevent an attacker from gaining knowledge about the security posture of the network or organization. These concepts of security practices should be employed in all networks, but especially in a system that could have the potential to cause the level of damage that can be achieved by hijacking an orbital system.

The ability for attackers to acquire communications systems capable of transmitting to a satellite in orbit is becoming cheaper, allowing many more attackers the window of opportunity to attempt such attacks. Simply put the best solution to prevent such attacks is to lower that window of opportunity. The use of optical links greatly reduces that window of opportunity since with the narrow beamwidth an attacker has a much smaller section of the sky he/she would need to send the signal for the satellite to pick it up. This level of precision is not needed in traditional RF since the beam spread is so large the attacker needs to only aim in the general direction of the victim satellite, and it will likely pick up the signal. Figure 12 shows a visual representation of the challenge an attacker would have to intercept the narrower beam of an optical inter-satellite link compared to an RF link (the figure is not to scale).

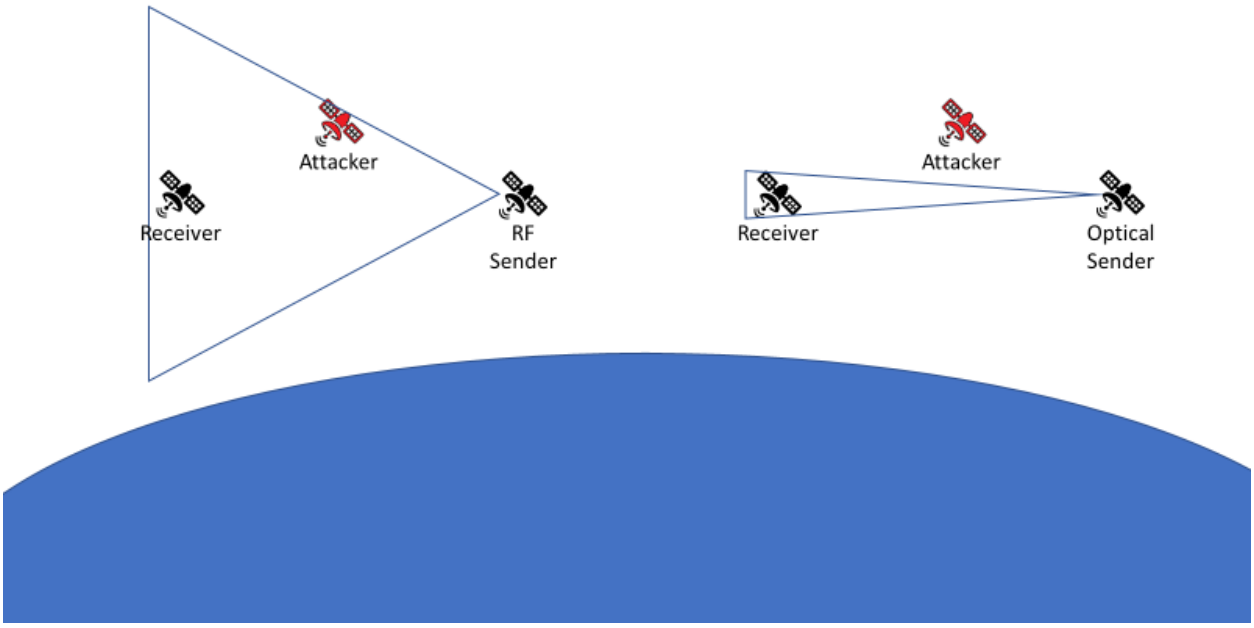

Figure 12: Interception of inter-satellite links

Secondly, with optical links orientation of the transceivers is critical, a misaligned transceiver could make it impossible for an attacker to transmit to a satellite if they are not at the right location on earth or in orbit and at the right time.

Chapter 5: Security Advantages of Optics

5.1 Quantum Key Distribution

Security concerns about the current state of SATCOM networks need to improve before a major security incident occurs. In the previous chapter, many of the improvements that could be made can be implemented in both the RF and optical spectrum. However simply moving to optics has an advantage over RF even if other security practices are not observed or are lacking.

The first major advantage optics has over RF is the ability to integrate Quantum Key Distribution (QKD) into the communications channel of the satellite as opposed to dedicating a side channel to the purpose. QKD is a relatively new method of sharing keys with two communicating parties that in theory make it impossible for a MitM to intercept the traffic without discovery. To understand how QKD works some fundamental knowledge in quantum mechanics is needed. In quantum mechanics there is an expression known as the Copenhagen interpretation, in the expression, it states that measurement of a quantum particle will result in the collapse or reduction of the wave function [31]. This collapse of the wave function is known as wave function collapse. The Copenhagen interpretation can be best portrayed by the famous Schrödinger's cat thought experiment. In the Schrödinger's cat experiment, it portrays a box and inside the box is a cat, a flask of poison, and a radioactive isotope. If an internal sensor detects radioactivity the flask is shattered, and the cat is killed. Due to the unknown nature of the radioactive decay of the isotope, it is impossible to determine if the cat is alive or dead, so therefore until it is observed the cat is both alive and dead. Once an observer opens the box to reveal the state of the cat the quantum fate of the cat being alive and dead collapses and the observer is left with the ultimate reality of the cat's state.

This characteristic is true for quantum particles and in QKD the quantum particles are photons that have been polarized into 1 of 4 possible polarizations, if a MitM observes the polarization of the particles this affects the outcome of the particles when they are received by the recipient. The four polarization states include horizontal, vertical, 45-degree, and 135-degree. Each polarization corresponds to a bit value where a horizontal or 45-degree photon represents a zero, and a vertical or 135-degree photon represents a one. In a hypothetical scenario, Alice would send a stream of photons representing ones and zeros to Bob using this method of distinguishing photon polarization states to bit values. Bob would then pass these photons through a random polarization filter to filter out horizontal and vertical photons and 45-degree and 135-degree photons which remove any photons that Bob did not guess the state of correctly. Bob is only able to determine these two states since the polarization of a photon can only be determined if they are parallel or perpendicular. Once Bob has the results he sends to Alice the photons he was able to receive and the polarization state of those photons, if the transmission was not altered Alice should be able to agree to the results Bob received from her. Due to the random mix of diagonal and perpendicular photons in the transmission, any interception of these will alter the transmission in a

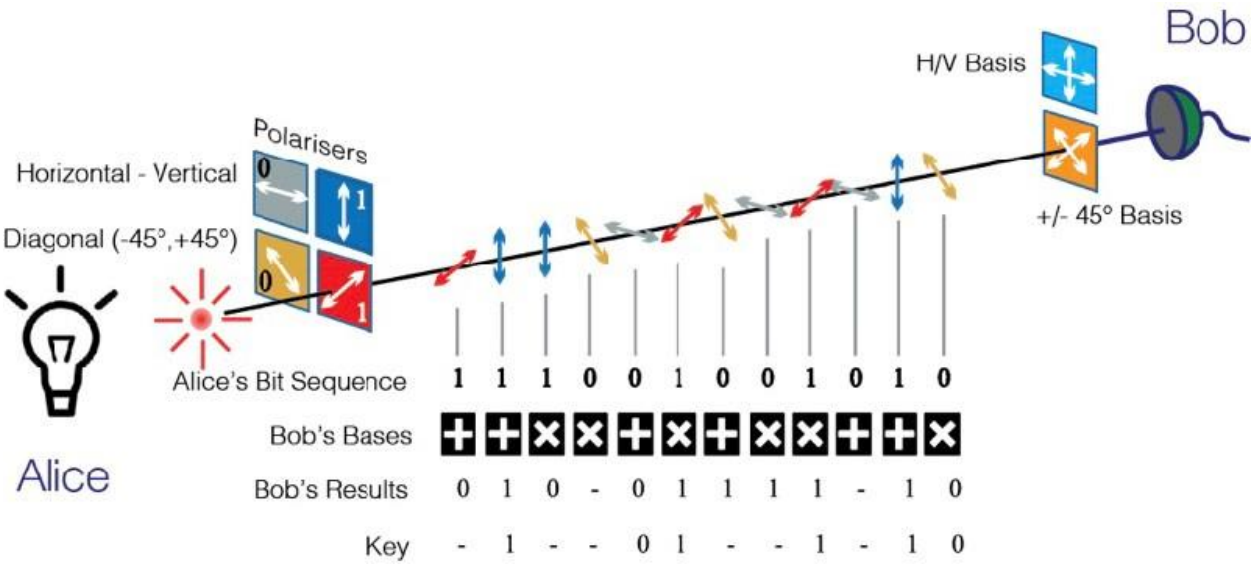

Figure 13: QKD (https://qt.eu/understand/underlying-principles/quantum-key-distribution-qkd)

way that would create too great of a disagreement between Alice and Bob that they would know that the transmission was intercepted [2]. Figure 13 shows a visual representation of how QKD is performed. Due to the nature of QKD, it is theoretically impossible to intercept and retransmit the exchange of the key in a way that would not reveal that it had been tampered with. Thus far any vulnerabilities to QKD are only achievable by exploiting loopholes within the protocols used to transfer the key, not in the mechanism itself [32].

QKD requires what is called a quantum channel to distribute the shared key, a quantum channel is simply a link capable of sending the polarized photons across to set up the shared key. In an optical communications system, the same link that is used to transfer data can be used as the quantum channel to share the keys before any data is transmitted. On an RF satellite wishing to use QKD, it would require an RF transceiver as well as an optical one, this adds weight to the satellite and increases cost to launch and build. If an optical communications satellite is used instead this security feature is available without any added weight or cost, ultimately making optics more secure by design than RF.

5.2 Narrow Beam

The second advantage has been discussed already and that is the narrow beam diameter provided by optical links. However, the full implications of why a narrow beam lends itself to a much greater degree of security in SATCOM situations has not yet been fully explained. To fully understand why a narrow beam greatly increases security in a SATCOM system some understanding of orbital mechanics is needed. The basic principles of an object orbiting another object can be defined by Kepler's Laws of planetary motion. The first law is "all planets move about the Sun in elliptical orbits, having the sun as one of the foci". The second law states "a radius vector joining any planet to the Sun sweeps out equal areas in equal lengths of time". The third and final law states "the squares of the sidereal periods of the planets are directly proportional to the cubes of their mean distance from the Sun". Kepler's Laws were used to describe the orbits of planets around the Sun but the principles hold for any orbiting object so we

will replace any instance of planet with satellite and the Sun with Earth. The First Law is very clear stating that a satellite will orbit Earth in an elliptical pattern. The second law results in satellites moving faster when they are closest to their periapsis (the point at which the satellite is closest to Earth) and

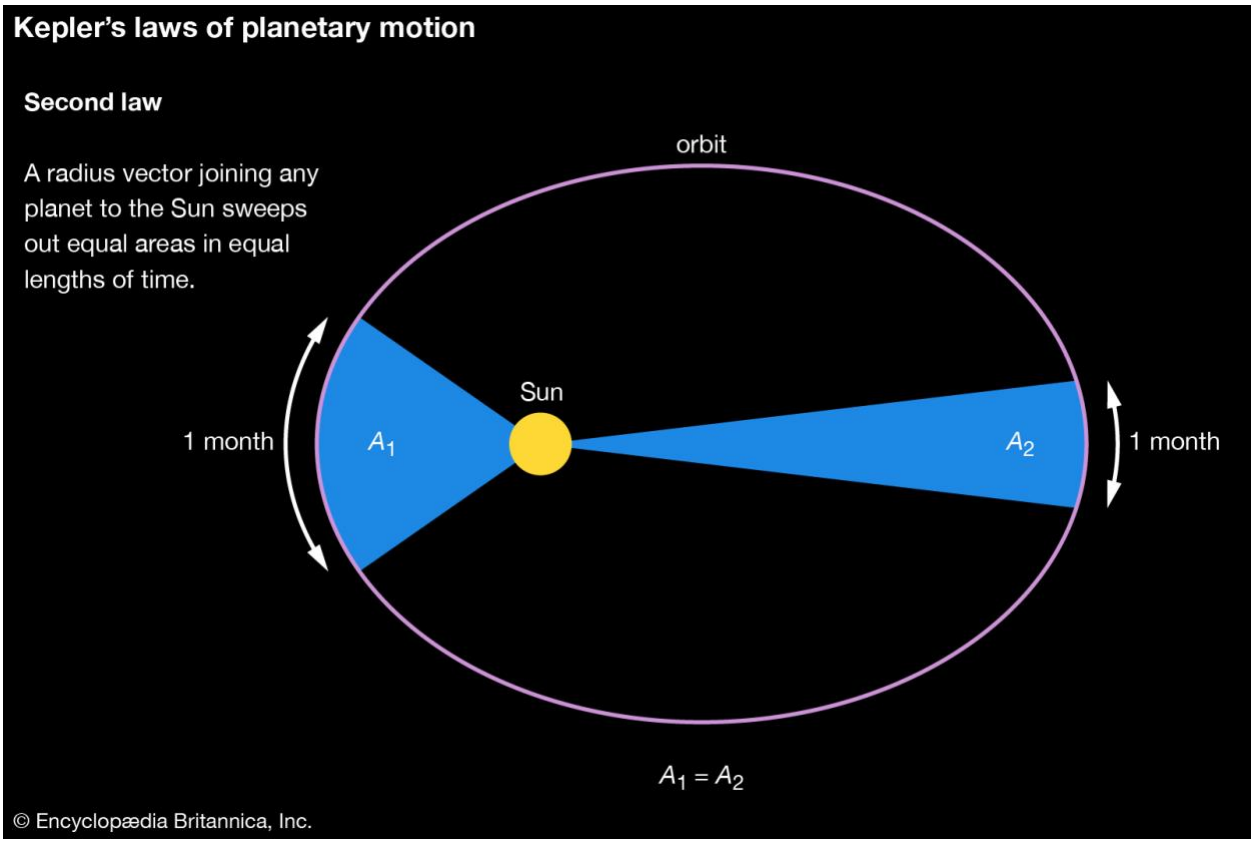

Figure 14: Kepler's Second Law of Planetary Motion(https://www.britannica.com/science/Keplers-laws-of-planetary-motion)

moving slower when they are closest to their apoapsis (the point at which the satellite is furthest from Earth). Figure 14 gives a visual representation of Kepler's second Law of planetary motion. Kepler's third law results in the fact that the further a satellite is from Earth the slower it will orbit Earth. Kepler's third law is the reason why GEO satellites need to be at 35,786 km above Earth so that their orbital period

matches that of the speed the Earth rotates. LEO satellites are much lower and therefore travel much faster and will orbit Earth up to 11 times a day.

Orbital mechanics as defined by Kepler's Laws of planetary motion show that very precise maneuvering is required for a satellite to be able to intercept an optical beam sent between two satellites. To achieve such an orbit a satellite has two options. Option one would be to position the malicious satellite between to communicating satellites and then match its orbit to those satellites so that it does not move out of alignment to intercept. This option relies on the perception that the two satellites share a common orbital trajectory and are not simply communicating over a brief moment while proper alignment has been achieved, and it puts the attacker satellite at risk of discovery since it essentially "parked" in that orbit intercepting traffic. The second option would be for a malicious satellite to maneuver into an orbital trajectory that would briefly put it in the path of transmission to intercept it. This option would make discovery less likely however now that the satellite has a vastly different orbit than the two communicating satellites the likelihood of it ever being in a position to intercept traffic from those two satellites again would be near impossible without a further course correction. A satellite capable of constantly altering course to intercept traffic would need large amounts of fuel and would be infeasible for anyone but the most well-funded cybercriminals. Additionally, this option would rely on the knowledge that the attacker will know when the two communicating satellites will be sending a transmission and plan well in advance on a course that can ensure it is in the right place at the right time to intercept the transmission, and the more extreme the course correction is, the more fuel the satellite will consume.

The complications of orbital mechanics are not the only aspect that makes the narrow beams of optical links vastly more secure than RF. RF receivers are far more forgiving when receiving a single from an RF transmitter, whereas optical receivers must contend with ATP operations before a link is established. Most optical communications systems use a protocol to acquire tracking locks between two optical transceivers. Some methods include using a wide FOV tracking beam to get the initial lock and

then gradually narrowing that beam until a full lock is achieved. If this protocol is not understood by an attacker or it is a nonstandard protocol that only the manufacture knows a malicious satellite will be unable to properly track an optical link to intercept it, and it will be unable to retransmit since it will not know how to acquire a lock with the receiver. Additionally, further security could be added to an ATP system that could for example use a method of frequency hopping in the use of the wide FOV tracking beam. This difficulty for an attacker to properly track and acquire a lock on a communications satellite also lends itself to securing the satellite from jamming attempts made by the attacker as well.

Conclusion

Space launches and the ability for small organizations to be able to place satellites into orbit is becoming increasingly cheaper and easier. With this new era of commoditizing space for economic and scientific purposes, the attack surface for cybercriminals is growing. With this growing attack surface, proper practices and policies are not growing in parallel with that attack surface. This disproportionate growth of these two factors can quickly lead to catastrophic cybersecurity incidents that could lead to massive costs in damages that can happen to valuable space infrastructure. Moving forward security needs to be addressed more seriously when designing and developing satellites and SATCOM networks as well as terrestrial-based systems that communicate with orbiting satellites. Many approaches should be practiced to improve the current state of SATCOM security and one of the best solutions put forth in this paper is the migration to optical network as opposed to traditional RF network. Not only does optics provide more bandwidth but it offers better security due to the narrow beam diameter in comparison to RF, as well as the ability to integrate QKD within the same channel used for communications.

Further research into this field that was not covered in this paper includes the use of ATP systems to improve the security of a SATCOM network and current vulnerabilities in the application of QKD that has led to vulnerabilities in its implementation. ATP has the potential to further improve the security of optical communications since it relies upon an agreed-upon mechanism between the sender and receiver to achieve a lock before data is transmitted. Knowing that a manufacturer could create proprietary ATP protocols that will only work with their systems would prevent any unauthorized or malicious attacker to achieve a lock with a legitimate satellite. As previously mentioned QKD is theoretically impossible to intercept without discovery due to the quantum nature of the polarized photons. However, research has

shown that there are still vulnerabilities in a QKD system, these vulnerabilities arise from the implementation of the protocol not the mechanic of it. These implementation flaws should be investigated further, and attempts should be made to remove them to make QKD as secure as possible.

References

[1] J. Mikolajczyk, Z. Bielecki, M. Bugajski, J. Piotrowski, J. Wojtas, W. Gawron, D. Szabra and A. Prokopiuk, "Analysis of Free-Space Optics Development," Metrology and Measurement Systems, vol. 24, no. 4, pp. 653-674, 2017.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science, vol. 560, no. 1, pp. 7-11, 2014.

[3] B. Dunbar, "Technology Rediness Level," 7 August 2017. [Online]. Available: https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html. [Accessed 16 May 2020].

[4] R. Gupta, T. S. Kamal and P. Singh, "Performance of OFDM: FSO Communication System with Hybrid Channel Codes during Weak Turbulence," Journal of Computer Networks and Communications, vol. 2019, no. 1306491, p. 6, 2019.

[5] S. Parkash, A. Sharma, H. Singh and H. P. Singh, "Performance Investigation of 40 GB/s DWDM over Free Space Optical Communications System Using RZ Modulation Format," Advances in Optical Technologies, vol. 2016, no. 4217302, p. 8, 2016.

[6] T. Garlington, J. Babbitt and G. Long, "Analysis of Free Space Optics as a Transmission Technology," Vols. WP No. AMSEL-IE-TS-05001, p. 12, March 2005.

[7] H. Kaushal and G. Kaddoum, "Optical Communications in Space: Challenges and Mitigation Techniques," Communications Surveys & Tutorials, no. DOI 10.1109/COMST.2016.2603518, IEEE , p. 41, 28 May 2017.

[8] L. Press, "Inter-Satellite Laser Link Update," 6 September 2019. [Online]. Available: http://www.circleid.com/posts/20190906_inter_satellite_laser_link_update/.

[9] D. Livingstone and P. Lewis, "Space, the Final Frontier for Cybersecurity?," Chatham House, September 2016. [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf. [Accessed 10 February 2020].

[10] D. Livingstone, Interviewee, Expert Paints Bleak Picture of Cyber Threat to Space Industry. [Interview]. 21 February 2017.

[11] D. Fidler, "Cyber Security and the New Era of Space Activities," 3 April 2018. [Online]. Available: https://cfr.org/report/cybersecurity-and-new-era-space-activities. [Accessed 7 February 2020].

[12] Tesat, "Laser Portfolio," Tesat, 21 February 2018. [Online]. Available: http://tesat.de/en/laser. [Accessed 17 February 2020].

[13] M. Motzigemba, "AW: Communications Systems Security," personal e-mail, 2020.

[14] SpaceX, "spaceX: About," [Online]. Available: https://www.spacex.com/about. [Accessed 11 April 2020].

[15] M. Albulet, "SpaceX Non-Geostationay Satellite System," Space Exploration Technologies Corp, 2016.

[16] Leosat, "leosat.com," [Online]. Available: https://ftl.to/leosat/to/media/1114/leosat-technical-overview.pdf. [Accessed 11 February 2020].

[17] Mynaric, "mynaric:technology," [Online]. Available: https://mynaric.com/technology. [Accessed 11 April 2020].

[18] C. Henry, "What the satellite industry needs to know about where 5G stands," 1 October 2018. [Online]. Available: https://spacenews.com/what-the-satellite-industry-needs-to-know-about-where-5g-stands/. [Accessed 24 October 2020].

[19] M. Marchese, A. Moheddine and F. Patrone, "IoT and UAV Integration in 5G Hybrid Terrestrial-Satellite Networks," Sensors, Vols. Sensors 2019, 19, no. 3704, 26 August 2019.

[20] A. Baryer, "5G from space: The role of satellites in 5G," 10 March 2020. [Online]. Available: https://www.futurithmic.com/2020/03/10/5g-from-space-role-of-satellites/. [Accessed 24 October 2020].

[21] A. Kurzrok, M. Diaz Ramos and F. S. Mechentel, "Evaluating the Risk Posed by Propulsive Small-satellites with Unencrypted Communications Channels to High-Value Orbital Regimes," in 32 Annual AIAA/USA Conference on Small Satellites, Utah, 2018.

[22] T. S. Rose, D. W. Rowen, S. D. LaLumondiere, N. I. Werner, R. Linares, A. C. Faler, J. M. Wicker, C. M. Coffman, G. A. Maul, D. H. Chien, A. C. Utter, R. P. Welle and S. W. Janson, "Optical communications downlink from a low-earh orbiting 1.5U CubeSat," Optics Express, vol. 27, no. 17, 2019.

[23] NASA, "NASA.gov," 18 September 2019. [Online]. Available: https://www.nasa.gov/directorates/spacetech/small_spacecraft/ocsd_project.html. [Accessed 17 February 2020].

[24] R. Whitwam, "Hacking Satellites Is Surprisingly Simple," 8 March 2019. [Online]. Available: https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think.

[25] D. Werner, "Small satellite sector grapples with cybersecurity requirements, cost," 8 August 2018. [Online]. Available: https://spacenews.com/small-satellite-sector-grapples-with-cybersecurity-requirements-cost/. [Accessed 12 September 2020].

[26] T. Hitchens, "Experts Decry Lax Rules for 5G Sat Networks," 12 June 2020. [Online]. Available: https://breakingdefense.com/2020/06/experts-decry-lax-rules-for-5g-sat-networks/. [Accessed 12 September 2020].

[27] C. Gibson, "IoT and Satellite Security in the Age of 5G," 11 June 2018. [Online]. Available: https://www.trendmicro.com/en_us/research/18/f/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot.html. [Accessed 12 September 2020].

[28] G. Falco, "Job One for Space Force: Space Asset Cybersecurity," Harvard Kennedy School Belfer Center for Science and International Affairs, Cambridge, 2018.

[29] T. Seals, "Feds: Cyberattack on NASA's JPL Threatened Mission-Control Data," 19 June 2019. [Online]. Available: https://threatpost.com/feds-hackers-mission-control-data-nasa-jpl/145842. [Accessed 7 February 2020].

[30] United State General Accounting Office, "Critical Infrastructure Protection Commercial Satellite Security Should Be More Fully Addresed," 2002.

[31] H. Wimmel, "Quantum Physics & Observed Reality: A Critical Interpretation of Quantum Mechanics," World Scientific, 1992, p. 3.

[32] A. Huang, S. Barz, E. Andersson and V. Makarov, "Implementation Vulnerabilites in General Quantum Cryptography," New Journal of Physics, vol. 20, 2018.

[33] ESA, "Satellite Frequency Bands," [Online]. Available: https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellite_frequency_bands. [Accessed 16 March 2020].

[34] A. Kwok, Frequency and Channel Assignments, 2009, p. 10.

[35] NDT, "Transducer Beam Spread," NDT Resource Center, [Online]. Available: https://www.nde-ed.org/EducationResources/CommunityCollege/Ultrasonics/EquipmentTrans/beamspread.htm. [Accessed 21 March 2020].

[36] Kholidy, H.A., Fabrizio Baiardi, Salim Hariri: 'DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks'. The IEEE Transaction on Dependable and Secure Computing, 10.1109/TDSC.2014.2327966, pp:164–178, June 2015.

[37] Kholidy, H.A., Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset For Cloud Computing and Masquerade Attacks ", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cidd/

[38] Kholidy, H.A., Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cids/

[39] Kholidy, H.A., Baiardi, F., Hariri, S., et al.: 'A hierarchical cloud intrusion detection system: design and evaluation', Int. J. Cloud Comput., Serv. Archit. (IJCCSA), 2012, 2, pp. 1–24.

[40] Kholidy, H.A., "PH.D. Thesis: Cloud Computing Security, An Intrusion Detection System for Cloud Computing Systems".

https://pdfs.semanticscholar.org/cf8a/14dc638480dbc5304824dd99a631d917d3fe.pdf

[41] Kholidy, H.A., "Autonomous mitigation of cyber risks in the Cyber–Physical Systems", Future Generation Computer Systems, Volume 115, 2021, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.09.002.

http://www.sciencedirect.com/science/article/pii/S0167739X19320680

[42] Kholidy, H.A., Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", in Journal of Computing, Springer, DOI: 10.1007/s00607-016-0495-8, June 2016.

[43] Kholidy, H.A., Abdelkarim Erradi, "A Cost-Aware Model for Risk Mitigation in Cloud Computing SystemsSuccessful accepted in 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.

[44] Kholidy, H.A., Ali Tekeoglu, Stefano Lannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, "Attacks Detection in SCADA Systems Using an Improved Non-Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), December 19-20, 2017.

[45] Qian Chen, Kholidy, H.A., Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and

Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017. Conference publisher: Springer.

“Industrial control system (ics) cyberattack datasets, http://www.ece.uah.edu/~thm0009/icsdatasets/PowerSystem_Dataset_README.pdf

[46] Kholidy, H.A.,, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, “A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.

[47] Kholidy, H.A., “Detecting impersonation attacks in cloud computing environments using a centric user profiling approach”, Future Generation Computer Systems, Volume 115, issue 17, Decmenr 13, 2020, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12 , https://www.sciencedirect.com/science/article/abs/pii/S0167739X20330715