Ensuring the Security of Space Systems from Eavesdropping Attacks

Caleb Richardson, Mark Reith and Wayne Henry
Air Force Institute of Technology (AFIT), Wright-Patterson AFB, USA
caleb.richardson@afit.edu
mark.reith@afit.edu
wayne.henry@afit.edu

Abstract: In a day and age where satellite communications are more important than ever to ensure global communication, establish international military power, and support our everyday way of life, satellite security must be at the forefront of innovation. However, eavesdropping attacks pose a serious threat to satellite communication systems that have not been adequately addressed. An eavesdropping attack threatens to put sensitive data in the wrong hands or even jeopardize critical missions. Research is needed to explore why defense against eavesdropping attacks is crucial, particularly for satellite systems. Three potential solutions to the problem are presented, addressing different challenges. Realistic solutions to the eavesdropping threat are needed urgently to defend the space domain from malicious threats.

Keywords: Satellite security, space systems, cyber security, eavesdropping attacks

1. Introduction

With space and cyber emerging as warfighting domains, anticipating the intersection of the two is vital. The most important issue to address in modern warfighting is ensuring the digital security of our nation’s space systems. When it comes to satellites, we are concerned with three core security levels. First is the physical level. Physical security deals with securing the satellite’s hardware and any related components on the ground. Next is the information level. This layer is concerned with ensuring that data sent to or from a satellite is confidential, maintains its integrity, and is available. Finally, there is the transmission layer, which focuses on ensuring the security of transmitting information to and from the satellite [10]. At the physical level, increased security may include more guards, stronger walls or classification levels.

This paper focuses on the information and transmission layers of security for satellites. One of the bigger problems that must be solved in regard to satellites is the eavesdropper attack [1]. This attack allows an unauthorized third party to intercept or potentially modify information being sent to or from a satellite. This type of attack has perpetuated itself in many forms across any device that sends information across a wire, the internet, or similar mediums. While this is not new to the technology world, it is one that is especially important with any satellite that transmits sensitive information. That is why finding a solution to this type of attack should take precedence over others. For the United States and its allies to stay at the forefront of technological capability, it is imperative to find a better solution to its satellites’ most pressing security threat: the eavesdropper attack.

2. Background

Satellite communication operates similarly to communication across any network. The key layers of the Open Systems Interconnection (OSI) model (Physical, Data Link, Network, Transport, and Application) are still present [5]. However, the most significant difference is the distance that the radio signal has to travel.

While there are many types of satellites, this paper will primarily look at those in geostationary earth orbit (GEO). These satellites are the most used for communication because they are in a fixed position and can be reliably reached. Communications satellites are the most likely target of an eavesdropping attack because of the data that can potentially be acquired from them.

First, we briefly define an eavesdropping attack, and how it can be executed on a satellite. An eavesdropping attack, also known as a man-in-the-middle attack, is when an unauthorized agent listens in on communication they are not meant to receive. Due to the nature of how a satellite broadcasts a signal back down to earth, with the right equipment it is possible to intercept this communication without even being in close proximity to the satellite’s ground receiver.

Satellites are not less prone to eavesdropping attacks because of new technologies. A potential eavesdropping attack has been modelled on the Thuraya network which implements the Geo Mobile Radio (GMR-1) standard
This attack was successfully theorized as a potential way to disrupt downlink communications. It could even be modified to modify the bit stream of the communication, manipulating the transmitted information [2]. Tests have even been conducted with equipment that an average person could purchase in which maritime communication was intercepted, including military and government communication [7, 8]. If this is possible to execute in an experimental environment, it is also a threat that could originate from someone with more malicious intentions.

3. Research

This research evaluates three potential solutions to the eavesdropper problem. Each of them presents a novel perspective on existing technologies that would make satellite transmission more secure against an eavesdropper attack. Each approach’s fundamental structure is outlined followed by its strengths and weaknesses. After an overview of each solution, a composite solution is proposed using the most realistic and viable parts of each potential solution.

3.1 Quantum Key Distribution

One potential solution to the eavesdropping model could be implementing continuous variable quantum key distribution. This method uses quantum keys for encryption which greatly lowers the chance of an eavesdropping attack occurring [6]. The utilization of this encryption method allows for a constant secure key rate (SKR) under a lower aperture. This means that the downlink of the satellite will not have to transmit data at such a high frequency to the receiver. Having a lower transmission frequency decreases the area around the receiver where a potential eavesdropping attack could occur. Throughout the transmission process the SKR remains constant to ensure a reliable transmission [6].

In Figure 6 is an example of a transmitter $A_a$ and a receiver $A_b$. $A_{ex}$ represents the exclusion zone. In this exclusion zone, photons cannot be captured without the satellites knowing. Utilizing SKRs that are possible through quantum key distribution, the transmission frequency is low enough such that any potential eavesdropper will fall into one of two categories. They will either be too far away to intercept the transmission, or they will fall into the exclusion zone and the satellites will be notified of malicious activity and can act accordingly. Even if the eavesdropper attempts for optimal positioning, it will still fall into the exclusion zone [6].

![Figure 1: Satellite transmission between transmitter $A_a$ and $A_b$ [6]](image)

The pros of this approach are that if it were implemented it would almost guarantee secure transmission against even the most sophisticated eavesdropper attacks. This technology is also faster than any current communication method so it would have massive implications in situations where information needs to be transmitted as close to real time as possible, such as when a decision needs to be made during a military conflict. The biggest downside to this solution is that the long-distance transmission of quantum keys is not yet at the point of reaching space as the furthest recorded transmission of a quantum key is currently 511 km [13]. Yet, as quantum key distribution technology grows in strength this will become an increasingly more attractive solution.

3.2 Cross Layer Architectures

Another option for increased satellite security is adopting a cross layer architecture (CLA). CLA is a design approach allowing non-adjacent layers of an OSI reference model to cooperate to optimize system performance. One solution would add additional protections in the TCP/IP stack as shown in Figure 2. While this approach was designed with streaming in mind it could also have applications in the cyber defense realm. The base approach...
is as follows. In the transport layer, UDP-Lite would be used instead of UDP. This makes a distinction between sensitive and insensitive parts of a packet and any errors that occur within sensitive parts result in a packet drop. Because this is incompatible with the current IP security at the protocol level, a cross layer IP security (CL-IPsec) would be implemented. CL-IPsec is cross layer because it has access to the checksums of the UDP-Lite packet at the transport layer.

Figure 2: The CL-IPsec protocol stack [9]

The CL-IPsec network model is one that results in fewer packet drops of important data while gaining increased performance as it can forward packets to their destination as long as all the sensitive parts are untouched [9]. This could also have applications in security as a similar checksum could be used to ensure data is not tampered with via an outside attack. The CL-IPsec approach has both the benefit and detriment of modifying existing network protocol structures. Because the base protocols already exist, modifying them in this way would not be too difficult from the perspective of merely redefining what it expects from packets. This would make it a lot more difficult as we would have to figure out how to make a new protocol system accept both new and old types of packets.

3.3 Channel Estimation Error

Utilizing channel estimation error involves calculating what the estimated error of communication across a channel should be with and without third party eavesdropping and utilizing those values to determine whether the communication is being tapped [3]. The channel estimation error method is unique because it takes into account the possibility of there being multiple eavesdroppers in a given scenario and specifically tests the secrecy performance of the method with multiple eavesdroppers.

Figure 3: Model of a satellite transmission with both authorized ($B_1$ and $B_N$) and unauthorized ($E_1$ and $E_M$) listeners [3]

As mentioned previously, on satellite downlink it is possible for the eavesdropper to be in a separate geographical location and still intercept the communication. Because of this, it is possible for multiple
eavesdroppers to be in multiple locations and attempt to intercept or hijack a satellite downlink. The model for this attack shown in Figure 3 is comprised of a satellite with multiple authorized users ($B_{1a}$ and $B_{N}$) and unauthorized eavesdroppers ($E_{1a}$ and $E_{M}$). In the presence of channel estimation error, the secrecy performance on a satellite communication can be improved through a mathematical analysis of the satellite waves [3]. The upside of this approach is that it can theoretically work against multiple eavesdroppers at the same time. However, it an implementation for it is not apparent and channel estimation error calculations can often be imperfect.

3.4 Proposed Solution

Based upon these solutions, the best way to combat eavesdropping on satellites would be to adopt a cross layer architecture that utilizes channel estimation error. While quantum key distribution is an enticing prospect for the future, it is the technology that is the furthest away from current adoption due to the current known limits of technology. It is important to keep it in the conversation so that when the technology does develop it can begin being applied to secure space transmission, however at the present time it is not feasible to include in this proposed solution. The concept of the cross-layer architecture is well designed and in order to increase transmission security revisiting the current network protocols will be imperative.

The most recent version of the "Overview for Space Communications Protocols" by the Consultative Committee for Space Data Systems (CCSDS) was released in 2014 [4]. This is a key player in the discussion of both governmental and quasi-governmental space system regulations and if this document has not been majorly revised in nearly a decade it is certainly worth revisiting and considering implementing additional security across the architecture layers. This could be done by adding checksums that check for two key bits of information. First, they would check to ensure all sensitive data in the packet is unaltered, similar to what the current model presents. Also, they could check to ensure the estimation error of the channel does not reach a level that might suggest tampering. Finding a way of adding channel estimation error calculations within the network stack could add even more security on top of the already suggested checksums. If tampering is detected the packet could not only drop, but temporarily drop all future packets to ensure data does not end up in the wrong hands. While there would be a delay before they are resent this would reduce the probability of the communication being intercepted.

These additions to the current communication protocols would certainly be impactfull against the threat of eavesdropper attacks and would lay the groundwork for adoption of quantum key technology in the future that would give an even more sure-fire method of detecting unauthorized communication interference.

4. Conclusion

Eavesdropping attacks are a large threat to satellites and one that is not being properly addressed. It is imperative that this or a similar solutions be explored soon, because as satellites continue to play a larger role in communication they will become a ever looming target for adversaries. This research analyzed multiple models that could solve the problem. At the end of the day a proposed solution would revisit the current network protocols and implement additional checksums. These checksums would ensure that communications from a satellite reach their destination without being manipulated or intercepted.

Disclaimer

The views expressed are those of the authors and do not reflect the official policy or position of the US Air Force, Department of Defense or the US Government.

References


Caleb Richardson, Mark Reith and Wayne Henry


