University of Science & Technology, Beijing

Digital Communications

To discuss the security challenges and vulnerabilities associated with 6G SAGIN.

Name: Vandeane Smith

Institution:

Professor: Du Bing

Date: December 2, 2022

Abstract:

Within the last decade, we have seen how satellites have emerged to have an ever-more-important function in modern science, from mapping to commerce to GPS to national security information gathering. Since the satellite sector has had a comeback in recent years, it is now well-positioned to help fulfill the market's expanding expectations, including those for 6G infrastructure and the Internet of Everything (IoE).

But as the number of satellites being deployed has increased, space-based assets have become a target for cybercriminals attempting to steal confidential data, with potentially disastrous results. Security must not be an afterthought when it comes to safeguarding the data that satellites transmit. It must be an essential component of the actual system design. Stremlau (2021).

Introduction:

Stremlau (2021) claims that we are currently witnessing the early research and development of 6G beginning due to the constantly increasing connectivity requirements. This has resulted in a fresh space race among technological corporations to install constellations that give the high-speed connectivity, bandwidth and capacity, that is needed to satisfy demand. Users anticipate having the same level of connectivity whenever and wherever they go, and satellite communications will bring 6G networks to remote and difficult-to-reach locations like the ocean, the desert, and the forest. Satellites will play a significant role in the development of a safe and secure connected experience, and security decisions will need immediate responses.

Satellite ground technology is also advancing with more innovation and scalability, as it tries to harness virtualization, orchestration and network splicing to offer 6G connection. A requirement for the industry now to support future expansion is software-defined satellites that can be reprogrammed to change capacity based on market demand. Satellites are the key entry point because there are so many new 6G and IoT application connections that could serve as entry points for hackers.

However, amongst the innovation and excitement, security can frequently be left behind. As more satellites are launched, it becomes increasingly important for corporations to think about how their systems can be vulnerable to hacker attacks. Satellites were once thought to be nearly impenetrable, but today it is comparatively easy for hackers to get and use the proper equipment for harmful purposes. A trust level must be established between earth-based devices and satellites because just about anyone could point an antenna at one and communicate with it.

Drone-To-Satellite Network

Drones, also known as unmanned-aerial-vehicles (UAV), have gained popularity in recent years in both the academic and industrial sectors. The provision of secure transmission between small/commercial UAVs and satellites is one of the most crucial difficulties in SATCOM. Researchers have proposed a physical layer security framework for space-air-ground (SAGIN) downlink multi-beam satellite-enabled vehicle communications, in which the UAV is used as a cooperative node, interacting with the authorized user and serving as a source of artificial noise to reduce eavesdropping. Researchers have explored the IoT computing offloading issue in the same network configuration by putting forth a reinforcement learning strategy to effectively distribute the UAV edge server's resources. The authors in the same field presented a software-defined architecture that supports various vehicles effectively. In keeping with recent research, a wide range of enticing drone and satellite applications is anticipated. Users can control drones remotely, transmit video from the drone's camera, utilize the drone to gather data from distant satellites, and use remote sensing optical applications using satellite connectivity. We anticipate increased study in this area in the following years due to the well-documented cybersecurity, personal security, and anonymity challenges created using drones as well as due to the vital role that drones will play in the advancement of the upcoming 6G communication networks. (Tedeschi et al., 2022)

What are some Satellite Security Threats?

The ability of the satellite to communicate with ground stations and space segments depends on links in both directions. If the uplink, such as the telecommand connection, is compromised, the satellite shall lose power and cease providing the intended services. The satellite’s transmitted output won't be acquired by ground stations if the downlink is disrupted. As a result, the satellite's availability will be impacted. A direct assault on satellites will also be included in this category of issues.

Confidentiality is breached if the data transmitted through the satellite and ground station shared channel is copied in an unauthorized manner.

The integrity of the information in the system is impacted if transmitted data is altered unlawfully.

Controlling who has admission to the space and terrestrial segments and granting them only curtailed access rights are two steps that can be taken to strengthen security. Another measure is to authenticate the source of information.

Regarding the safety of telemetry and telecommand data, in addition to data in the ground data system, security requirements for various space missions vary considerably. The attack vectors enforced by a threat can be divided into (i) assaults at the network level or (ii) attacks that target end-points when taking into account the general satellite operation arrangement shown below in Figure 1.

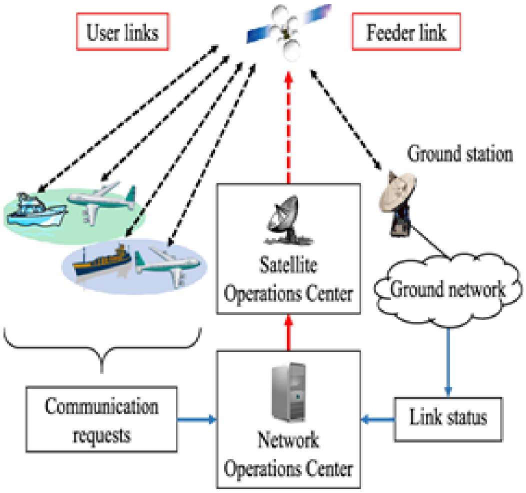

Figure 1: Showing SATCOM System.

network-based assaults. Attacks at the network level target communication between communicative entities, such as command and control or inter-satellite communication. Both passive and active attacks fall under this category. In passive attacks, the threat is only capable of passive eavesdropping, which involves intercepting and interpreting the transmitted signals and packets.

Eavesdropping can lead to the unauthorized copying of transmitted data, which violates the need for confidentiality.

The capability of an attacker to execute adversary activities, such as to drop or jam, inject, edit, or repeat formerly captured packets and/or signals, makes an attack active. Active attacks are more sophisticated.

Denial-of-Service (DoS) or "drop" attacks: Attacks that enable information loss by an adversary cause service interruptions and jeopardize the system's requirement for availability. Jamming and flooding with an excessive volume of packets to clog the network are examples of such attacks on satellite systems.

Injection, also known as spoofing: Spoofing attacks cause illicit messages to be inserted into transmission.

For instance, 20 US ships in the Black Sea were the target of GPS spoofing attempts. Notably, since it seems that the GPS is operating as designed, faking GPS satellite signals is far riskier than jamming. The authenticity criterion is compromised by this attack method. (Schilling & Dmitrienko, 2021).

Alteration attacks compromise the system's requirement for integrity by modifying transmitted data in an unauthorized manner. An adversary must be able to suppress the original signal and inject the new, fake version in order to successfully carry out such an assault.

Attacks known as replays combine passive listening and aggressive injection. In this scenario, an enemy records conversation and replayed it later. Such assaults compromise the necessity for freshness.

The network-level attacks that were outlined above, both passive and active, can be employed as basic elements needed to accomplish other high-level attack objectives:

Impersonation of end-points: An attacker commits an act while posing as another entity, for example, to gain access to a system without authorization (undermining its authenticity) or to cause harm without being held responsible (undermines accountability).

Deanonymization: Systems that provide anonymous communication should be aware of this attack vector. Here, a threat actor reveals the identities of communication endpoints. This attack method compromises the anonymity of the communication. This threat appears to be less applicable to satellite networks. But in the future, it might matter if, for instance, SAT phones offer their users anonymous communication channels.

Endpoint threats attack communication endpoints like satellites or terrestrial stations.

Terrestrial stations may be vulnerable to similar types of attacks just like any ground system should they be remotely reachable via the Internet.

the satellites

Kinetic-physical and non-kinetic physical assaults are two examples of denial-of-service (DoS) attacks.

Kinetic-physical threats aim to directly hit targets such as satellites or ground stations. An attempt to harm something permanently. Attacks that don't involve immediate physical contact with a target are called non-kinetic attacks.

These include high-powered microwave emissions, for example, can disrupt satellite systems and harm them permanently or temporarily.

Remote software-based attacks: Using software flaws as a means of infection, an adversary uses this system vulnerabilities to assault the target. With the increased usage of commercially available technology, this threat becomes increasingly pertinent for satellite vehicles.

Physical capturing: During a physical capture assault, the adversary attempts to physically reach the target and tamper with it in order to take control of it.

An adversary might, for example, listen in on communication busses, extract sensitive information from memory, introduce backdoors, replace the control logic with malicious code, roll back software versions to older or more susceptible versions, brick the target, etc. Although this is a very potent attack vector that simultaneously violates many security requirements (such as confidentiality, integrity, freshness, authenticity, and availability), its applicability to satellite vehicles is constrained because it is highly unlikely that an adversary would physically gain access to a satellite during its operational phase. However, such attacks are still a possibility during the pre-launch phase and might be used to, for example, render the satellite inoperable or even seize complete control of it.

Cloning attacks: In this type of attack, the enemy makes an exact replica of the target, usually so they can impersonate it. If the target uses any cryptographic security measures, an adversary will have to reveal the secrecy of any cryptographic keys kept on the target. If the enemy can create numerous copies, one can launch a so-called Sybil attack in which numerous entities pose as one another. Presently, this method of attack does not appear to be significant for satellites.

Addressing threats on the network level.

The most cutting-edge method for fending off both passive and active network-level attack channels is to use cryptographic methods, like message authentication and encryption. They rely on cryptographic secrets, or keys—small bits of private information that must either be kept private, in the case of Public Key Cryptosystems (PKC), or securely transmitted between communication parties, relating to Secret Key Cryptosystems (SKC).

Based on quantum technologies, novel methods for secure communication are being researched, which may be suited for the distribution of key information. Entangled photons will be used to disseminate generated quantum keys. In this case, fiberglass connections are limited to distributing keys over a few hundred-meter distances. Satellites appear to be the only means of transferring quantum keys created on-board the satellite to remote communicating parties via optical lines for quantum key distribution at intercontinental distances.

In terrestrial systems, a substantial set of authentication mechanisms was established to address the issue of end-point impersonation. However, most of them rely on computationally expensive PKC and demand the implementation of Public Key Infrastructure (PKI). This is not best suited for satellite vehicles with limited resources.

As a result, authentication methods used in satellite systems make use of more effective SKC or even only rely on effective one-way functions. The anonymity of operators in mobile satellite networks is another issue that certain protocols attempt to address.

Addressing end-point level threats.

It is difficult to deal with end-point threats relating to satellite systems because of the related costs, such as management and computational overhead. For instance, maintaining software patches and tracking vulnerability information are typical approaches for addressing the issue of software vulnerabilities, which suggests the necessity of supporting software update techniques. Such techniques create new, potent attack vectors while also adding to the (storage) burden. Address space layout randomization (at various levels of granularity) is one preventive measure.

Conclusion

Privacy and security for 6G. Satellites, UAVs, and underwater communications will all work on 6G networks. Any security proposal made in this context must be sure to safeguard communications while ensuring dependability, minimal latency, and efficient and secure transmission services. The first potential line of defense for these advances in technology is physical layer security, but if forthcoming cryptography-based solutions are rigorously systematized and coordinated with the existing services, they may also have a role to play. The reliability and security of data communication must be improved immediately in space. Shifting to the extraterrestrial environment and offering enormous application potential are added benefits of the already existing economic value in ground network solution approaches. Satellite-based quantum key distribution offers innovative methods for secure communication.

Reference

Cao, H. *et al.* (1970) *Analysis on the security of satellite internet*, *SpringerLink*. Springer Singapore. Available at: https://link.springer.com/chapter/10.1007/978-981-33-4922-3_14 (Accessed: November 18, 2022).

Diagram of a satcom system. the network and satellite operations ... (no date). Available at: https://www.researchgate.net/figure/Diagram-of-a-SATCOM-system-The-network-and-satellite-operations-centers-serve-as_fig1_329349929 (Accessed: November 22, 2022).

Schilling, K. and Dmitrienko, A. (2021) *(PDF) increasing security in satellite networks - researchgate*, *ResearchGate*. Available at: https://www.researchgate.net/publication/357606031_Increasing_Security_in_Satellite_Networks (Accessed: November 21, 2022).

Stremlau, T. (2021) *The vulnerability of satellite communications*, *Security Magazine RSS*. Security Magazine. Available at: https://www.securitymagazine.com/articles/94689-the-vulnerability-of-satellite-communications (Accessed: November 21, 2022).

Tedeschi, P., Sciancalepore, S. and Di Pietro, R. (2022) *Satellite-based Communications Security: A survey of threats, solutions, and research challenges*, *arXiv.org*. Available at: https://arxiv.org/abs/2112.11324 (Accessed: November 25, 2022).