International Journal of Internet, Broadcasting and Communication Vol.15 No.4 128-133 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.4.128

IJIBC 23-4-14

A Survey for Vulnerability Attack and Defense Method of Satellite-Link Based Communication System

Isaac Sim‡*, Jinwoo Jeong‡*, Sangbom Yun*, Yunsik Lim**, Junghyun Seo*

**LIG Nex1, Cyber-Electronic Warfare R&D, Research Engineer*
***Yeoju Institute of Technology, Dept. of Electrical Eng., Professor*
*{isaac.sim, jinwoo.jeong, Sangbom.Yun, junghyun.seo}@lignex1.com,
*elecys@yit.ac.kr

Abstract

Satellite based communication is networks in which users in a wide area can access without wired-based ground infrastructure. In particular, the need is emerging due to the recent Ukraine-Russia war. Satellite network systems acquire data that is difficult to observe on Earth as well as communication networks and are also used for research and development, which allows additional data to be produced. However, due to the nature of communication networks existing in outer space, certain vulnerabilities are revealed, and attacks based on them can be exposed. In this paper, we analyze vulnerabilities that may arise due to the nature of satellite communication networks and describes current research, countermeasures, and future research directions.

Keywords: *Satellite Communication, Physics Layer Attack, Vulnerability Analysis*

1. Introduction

A satellite communication network is a air-hoc based network that allows users in a large area to communicate without utilizing the existing traditional ground-based infrastructure [1]. In Korea, there is already an existing ground communication infrastructure, and it is safer and cheaper to utilize it than satellite network, so few active research has been conducted. Recently, satellite communication system is emerging due to the Ukraine-Russia war.

The Ukraine-Russia war is serving as a testing field for many of the warfare conditions that must be considered in modern warfare [2-3]. While Russian forces attacked and neutralized the Ukrainian military's ground infrastructure-based communications network early in the war, Ukraine has since recovered and is actively utilizing a low-orbit satellite communications network from the U.S. company Starlink. The satellite communication network is the air-hoc based system that cannot be neutralized unless there is a means to strike a low-orbit satellite directly at an altitude of more than 100 kilometers, and it is possible to access and utilize

Manuscript Received: September. 10, 2023 / Revised:September. 15, 2023 / Accepted:September. 20, 2023
Corresponding Author: junghyun.seo@lignex1.com
‡ These authors contributed equally to this work.
Tel:*** - **** - ****
*Research Engineer, Cyber-Electronic Warfare R&D, LIGNex1, Korea
*Professor, Dept. of Electrical Engineering, Yeoju Institute of Technology, Korea

the communication network anywhere on the ground with portable base station [4-6].

In addition, analysis technologies for data that can collect on space area, satellite networks are also being studied Synthetic Aperture Radar (SAR) based land and sea image data, weather data outside the Earth, and near-field astronomical data, such as. This data is difficult to collect on the Earth but satellites and transmitting them to observation facilities on the ground for research [7].

2. Experiments

In satellite communication networks, initial authentication between satellite and base station must be implemented with downlink-based broadcasting, which can cause security problems when unauthorized users try to connect to the authentication. In addition, unlike the existing ground-based communication system, communication between network is connected by Radiofrequency (RF) wireless signals, so RF security measures that were considered only for terminal connections must be considered in whole network environments.

In this paper, we analyze the attack methods according to the connection layer of the satellite communication network and reviews the technologies to prevent them. We discuss the possibilities of disrupting the connection between the user and the network in some way or archive unauthorized access at each connection layer. As a direction for future research, we propose methods for securing satellite communication networks.

Figure 1 shows a block diagram of a satellite network-based communication system. To expand the range of connectivity, satellite networks operate multiple satellites, which are similar to traditional base stations, and RF based connection between them to realize a wide service area. Because of environment of space, the satellite network is not a fixed infrastructure based on wires, but a dynamic infrastructure in which the location of the base station moves continuously in real time. This is also true for geostationary orbit satellites, where the moving range is effective enough to phase the RF signal and must be accounted for. In addition, satellite network communications use RF signals only at every layer of communication network.

Depending on the communication initialization process of satellite network, we can define 4 different connection phases as below:

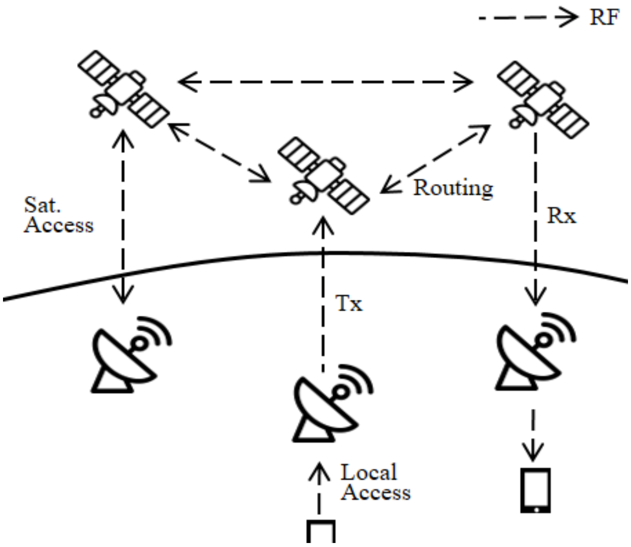

Figure 1. A hierarchy of satellite-based communication system

2.1. Access

The initial access can be separated with two steps: Satellite access, which connects to the satellite from the ground receiver, and Local access, which connects to the ground receiver from the ground terminal.

a) Satellite access

Satellite access is the initial connection between the satellite base station and the ground base station. The ground station calculates the QoS (Quality of Service) of all available satellite stations and approaches the station with the highest quality. After the initial contact, the QoS of each satellite is updated repeatedly, and a handover is performed when the QoS condition changes due to the location of the satellite and ground station [5]. Due to this access procedure, satellite base stations frequently broadcast with unencrypted signals. Due to characteristics of satellite communication networks that require long-distance communication over 500 kilometers, it is difficult to restrict the access of specific terminals within the service area, and vulnerabilities may occur using this [8].

b) Local access

This is the process of connecting a local terminal with a ground base station. Vulnerabilities of that are the same as those in the traditional terrestrial communication network.

2.2. Uplink Transmission

This is the stage where data is transmitted from the ground base station to the satellite base station. In the connection stage, satellite base station transmits information code of itself, and all satellite base stations within range receive that code. Since the exact location of the satellite cannot be determined on the ground, it transmits an uplink signal based on O-TFS (Orthogonal Time-Frequency-Space) with angle wider than 60°.

2.3. Satellite Routing

The signal received from the ground station is sent to the satellite station that is connected to the receiver's ground station. These steps are same way as TCP/IP/MAC address-based routing in a traditional communication network.

2.4. Downlink reception

During the initial connection, the ground station determines its location based on GPS and performs authentication based on data including metadata of itself. The satellite station knows the GPS coordinates of the ground stations connected to it and scans for handover conditions based on this data and QoS values.

Based on the characteristics of each connection layer, we suggest that vulnerabilities that can be occurred at each process and how they can be exploited.

3. Results

Table 1 shows the vulnerabilities that can occur in each communication phase analyzed in Chapter II, the attack methods based on these vulnerabilities, and the methods to counteract these attacks. Unlike traditional communication networks, satellite communication networks are located in outer space, so it is impossible for an attacker to access networks physically. In addition, even if an attackers connect on a ground base station, it is difficult to perform a network attack because only one satellite station is connected to a ground station. For these reasons, we focused on the vulnerabilities of satellite communication networks that can occur at the RF physical layer.

Table 1. Possible vulnerabilities, attack and methods of communication process

No.	Related chapter	OSI layer	Vulnerability	Method	Counter method	Ref.
1	2-1-a	PHY	Broadcasting access	Drone hijacking	SIS memory	[9]
2	2-1-b	NET	Network tapping	Packet shooting	Encryption	[10]
3	2-2	PHY	Orthogonal multiple access	Timing jittering	Timing recovery	[11]
4	2-3	PHY	Noise of global relay	Jamming satellite	Signal nulling	[12]
5	2-4	PHY	Downlink communication	GNSS spoofing	Anti-spoofing	[13]

1. Satellite Approach Phase: Drone-Based Approach Signal Hijacking

Figure 2. (a) illustrates a drone-based hijack that can be attacked during the satellite approach phase. The signal generated by the satellite station during the initial approach is a broadcast signal that can be seen all over the world and can be interpreted by any user who knows the specifications of the signal. This can be used to operate a malicious drone that is located physically between the two base stations. The malicious drone can intercept the access signal in the middle, and then use the Doppler effect to bypass the approach or connect to the malicious drone [9].

2. Local Access Phase: Tapping and over-shooting packets for induce network congestion

Figure 2. (b) illustrates the process of inducing network congestion by tapping a ground base station. Unlike traditional communication networks, satellite networks that perform routing based on RF wireless signals require much more resources for scheduling at the network layer [10].

It can make them much more vulnerable than traditional communication networks to packet attacks in the form of distributed denial of service (DDoS). If an attacker archives access to a ground station, then it is able to send packets, this can cause satellite communications to be disrupted in certain areas.

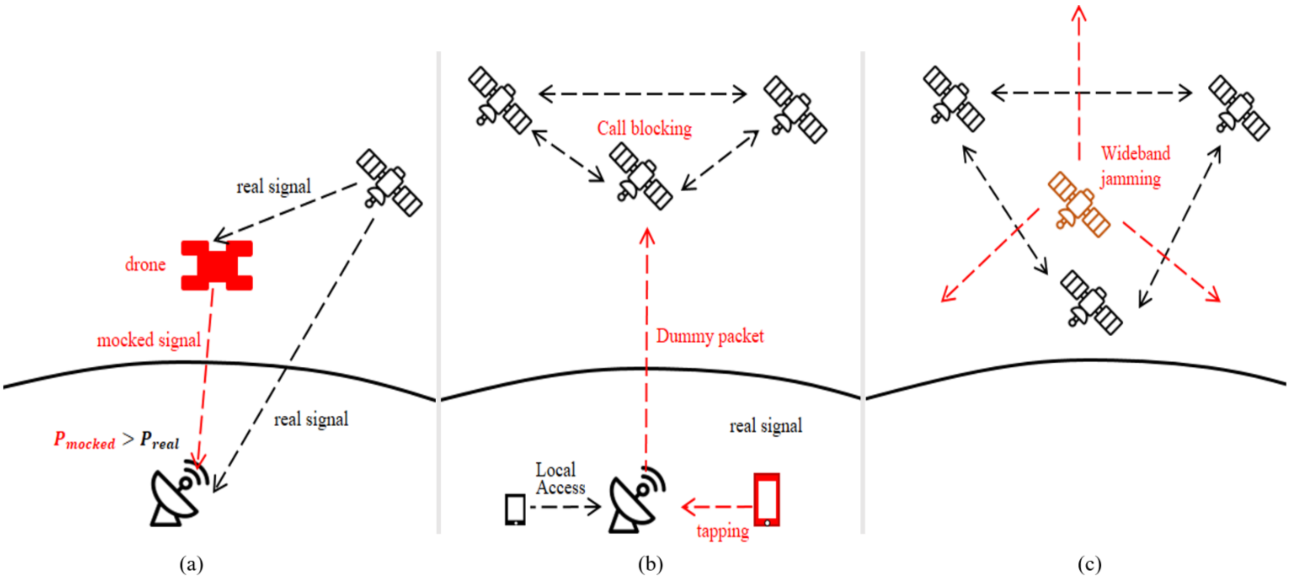

Figure 2. A Structure of Satellite Vulnerability attack method:
(a) Authentication Hijacking based on drone between base station.
(b) Network blocking through excessive packet transmission.
(c) Network neutralization through wideband jamming satellite.

3. Uplink Transmission Phase: Timing jittering

Due to the nature of the transmitter (ground station) not knowing the exact location of the receiver (satellite base station), the receiver is the one who compensates for the orthogonality of the signal. In this compensation process, quality degradation due to orthogonality degradation may occur, and the possibility of vulnerability attacks using it exists [11].

4. Satellite Routing Phase: Jamming Satellites

Satellite communication networks also perform routing between satellites, which uses relays that perform the same functions as traditional communication networks. Unlike traditional communication networks, there is a vulnerability that the relay amplifies not only the target signal but also the external RF signal. This can be a significant vulnerability due to the nature of satellite networks that rely on radio communications for routing [12].

Figure 2. (c) shows the process of neutralizing a communication network based on jamming satellites. A jamming satellite performs the same function as a traditional RF jammer. Unlike traditional communication networks, it operates at the same altitude as the satellite communication network and performs wideband jamming that can cover the entire bandwidth. Unlike traditional RF jammers, jamming satellites can be a powerful neutralization tool because satellite jamming can neutralize these wireless networks.

5. Downlink Reception Phase: GNSS Spoofing

When a satellite base station determines the location of a ground station and transmits a downlink to that location, there is a vulnerability that a GNSS spoofing technique can block the downlink by preventing the satellite base station from knowing the current location and condition of the ground station [13].

4. Discussion

In local access phase, the vulnerability comes from DDoS attack can be mitigated by continuous QoS scanning. By continuously collecting QoS conditions of satellite stations of nearby, ground stations can distinguish malicious signals from drones because lack of operation time of it. However, this method cannot be applied when the ground station operates initialization and makes the first access.

In uplink transmission phase, the demodulation of orthogonal signals shows a large performance difference even with a small amount of noise. In the QoS-based scanning technique used in existing satellite communication networks, nulling of code signals that do not exceed a certain threshold point is introduced to gain demodulation capability for uplink signals instead of losing connectivity.

In satellite routing phase, the vulnerability comes from jamming attack can be countered by expanding the coverage of the satellite network. Satellite jamming requires as many jamming satellites as the satellite network can service, and if the jamming satellites do not take down the entire satellite network, the network can be maintained with a QoS tradeoff through network bypass.

In downlink phase, a countermeasure to the vulnerability comes from spoofing attack is an anti-spoofing technique. When estimating location based on GNSS, the GPS satellite tracking should be closely spaced to detect GNSS signals from other than GPS satellites, ignore the signals from those satellites, and estimate the location based on other satellites to prevent degradation of location recognition performance by a single spoofer.

5. Conclusion

In this paper, we described the necessity and possibility of utilizing satellite communication networks and presented the types of vulnerabilities derived from the differences between satellite traditional communication networks. Unlike traditional communication networks, which use wireless communication only at the front line, the characteristics of satellite communication networks that use wireless communication between all nodes lead to vulnerabilities in physical measurements, and we presented how to respond to them. As future research, it is necessary to study how to authenticate users at the physical layer instead of authentication and attack response that is biased toward the network layer, so that the attack can be blocked without analyzing it.

References

[1] Y. Su, Y. Liu, Y. Zhou, J. Yuan, H. Cao and J. Shi, "Broadband LEO Satellite Communications: Architectures and Key Technologies," in IEEE Wireless Communications, vol. 26, no. 2, pp. 55-61, April 2019. DOI: 10.1109/MWC.2019.1800299.

[2] Choi S., "Analysis and Aspects of Space Warfare in the Russia-Ukraine War (Russian Invasion of Ukraine) and Considerations for Space Technology Development," J. Space Technol. Appl. vol.2, pp.169-186, 2022. DOI: https://doi.org/10.52912/jsta.2022.2.2.169

[3] M. Neinavaie, J. Khalife and Z. M. Kassas, "Acquisition, Doppler Tracking, and Positioning With Starlink LEO Satellites: First Results," in IEEE Transactions on Aerospace and Electronic Systems, vol. 58, no. 3, pp. 2606-2610, June 2022. DOI: 1https://doi.org/0.1109/TAES.2021.3127488.

[4] A. Guidotti et al., "Satellite-enabled LTE systems in LEO constellations," 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 2017, pp. 876-881. DOI: https://doi.org/10.1109/ICCW.2017.7962769.

[5] Adam Hudaib, Satellite Network Threats Hacking & Security Analysis, CreateSpace Independent Publishing Platform, 2016.

[6] Jeong, Won-Ho et al., "Performance Analysis of the Encryption Algorithms in a Satellite Communication Network based on H-ARQ," The Journal of The Institute of Internet, Broadcasting and Communication, vol. 15, no. 1, pp. 45–52, Feb. 2015. DOI: https://doi.org/10.7236/JIIBC.2015.15.1.45.

[7] Y. Yu, S. Liu, Y. Li and K. Shi, "Satellite Remotely Sensed Nighttime Lights Reveal Spatiotemporal Dynamics of the Ukrainian-Russian Conflict," in IEEE Geoscience and Remote Sensing Letters, vol. 20, pp. 1-5, 2023, Art no. 2503005. DOI: https://doi.org/10.1109/LGRS.2023.3290559.

[8] X. Wang, P. Hao and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," in IEEE Communications Magazine, vol. 54, no. 6, pp. 152-158, June 2016. DOI: https://doi.org/10.1109/MCOM.2016.7498103.

[9] Q. -Y. Fu, Y. -H. Feng, H. -M. Wang and P. Liu, "Initial Satellite Access Authentication Based on Doppler Frequency Shift," in IEEE Wireless Communications Letters, vol. 10, no. 3, pp. 498-502, March 2021.DOI: https://doi.org/10.1109/LWC.2020.3035811.

[10] Yiltas, D. and Zaim, A.H., "Evaluation of call blocking probabilities in LEO satellite networks," Int. J. Satell. Commun. Network., vol. 27, pp. 103-115, 2009. DOI: https://doi.org/10.1002/sat.928

[11] J. Hu, J. Shi, S. Ma and Z. Li, "Secrecy Analysis for Orthogonal Time Frequency Space Scheme Based Uplink LEO Satellite Communication," in IEEE Wireless Communications Letters, vol. 10, no. 8, pp. 1623-1627, Aug. 2021. DOI: https://doi.org/10.1109/LWC.2021.3072902.

[12] R. Han, L. Bai, C. Jiang, J. Liu and J. Choi, "A Secure Architecture of Relay-Aided Space Information Networks," in IEEE Network, vol. 35, no. 4, pp. 88-94, July/August 2021.DOI: https://doi.org/10.1109/MNET.011.2100076.

[13] M. G. Amin and Wei Sun, "A novel interference suppression scheme for global navigation satellite systems using antenna array," in IEEE Journal on Selected Areas in Communications, vol. 23, no. 5, pp. 999-1012, May 2005. DOI: https://doi.org/10.1109/JSAC.2005.845404.