Proceedings of the 2024 Winter Simulation Conference
H. Lam, E. Azar, D. Batur, S. Gao, W. Xie, S. R. Hunter, and M. D. Rossetti, eds.

SIMULATION OF LOW EARTH ORBIT SATELLITE COMMUNICATION DATA FOR CYBER ATTACK DETECTION

Laila Mashayekhi[1], and Michael E. Kuhl[1]

[1]Dept. of Industrial and Systems Engineering, Rochester Institute of Technology, Rochester, NY, USA

ABSTRACT

Satellites play a crucial role in the global infrastructure of internet communication, commerce, and society. However, they are vulnerable to cyber-attacks, with distributed denial of service (DDoS) attacks being among the most prevalent threats. These attacks disrupt normal operations by flooding a network's resources. In response to the increasing frequency of such threats, there is a growing need for predictive methods of detecting bad actor signals. This paper proposes a stochastic logging system designed to capture and analyze key metrics associated with DDoS attacks on Low Earth Orbit (LEO) satellites, including uplink and downlink speeds, spectrogram speeds, and latency. By logging these measures, the system aims to identify abnormal signal activity. The methodology involves generating synthetic data representative of LEO satellite communication metrics and validating these values against predefined acceptable ranges. These datasets could then be used to develop methods for detecting and mitigating attacks on satellite networks.

1 INTRODUCTION

In the growing world of internet communication, commerce, and society, satellites are an integral piece of global infrastructure. Low Earth orbit (LEO) satellites, like any piece of network-based technology, can be susceptible to cyber-attacks that may compromise their operations and integrity. Understanding and mitigating the risks posed by cyber threats to LEO satellites is not just a matter of technological security, but also one of safeguarding the essential functions of global communication which we rely on.

To effectively address these challenges, modeling communication networks has emerged as a crucial tool in assessing vulnerabilities and devising robust defense strategies. By constructing detailed simulations that replicate the complexities of satellite systems, researchers can analyze potential points of weakness and evaluate the effectiveness of various security measures. These models enable the exploration of different attack scenarios, ranging from traditional DDoS assaults to more sophisticated forms of cyber intrusion, allowing for proactive risk mitigation and response planning. Moreover, through the integration of advanced modeling techniques and real-world data, such as historical attack patterns and system performance metrics, these simulations can provide invaluable insights into the dynamics of cyber threats in satellite communication networks.

In particular, distributed denial of service (DDoS) attacks are one of the most commonly used forms of cyber-attacks launched against satellite infrastructure. The DDoS attack method works by flooding a network's resources and preventing normal operations on a large scale (Zhang et al. 2022).

For satellites, the communication flow between a ground station and a satellite typically follows the steps described in Figure 1. This communication includes an uplink transmission preparation step at the ground station; transmission of the signal to the satellite; signal reception and processing on the satellite; and a return signal to the ground station. DDoS attacks typically occur in the transmission and signal reception phases.

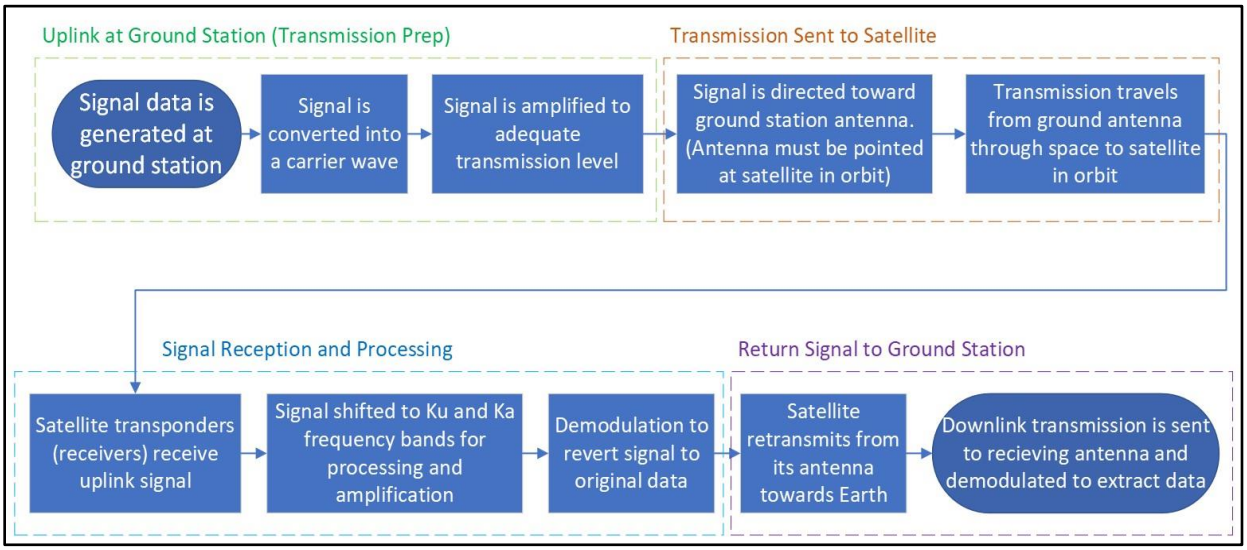

Figure 1: The flow of typical satellite communications without influence from bad actors.

In response to the growing prevalence of these threats, there is an increased need for a predictive method of bad actor signal detection. Simulation can be a powerful tool for modeling and analyzing the behavior of satellite communication systems under various conditions, including cyber-attacks such as DDoS. By constructing a simulated environment that accurately represents the network infrastructure, transmission protocols, and potential attack scenarios, researchers and engineers can observe how the system responds to different attack strategies and mitigation techniques. First, it allows researchers to emulate the characteristics of real-world DDoS attacks, such as the volume, intensity, and duration of malicious traffic, as well as the specific targets within the satellite communication network. By varying these parameters, simulation studies can explore the effectiveness of different defense mechanisms, such as traffic filtering, load balancing, and network segmentation, in mitigating the impact of DDoS attacks (Usman et al. 2020). Additionally, simulation enables the evaluation of the resilience and robustness of satellite communication systems against evolving cyber threats. Researchers can use simulation to assess the performance of detection algorithms and anomaly detection techniques in identifying malicious activities in real-time. By iteratively refining these algorithms based on simulation results, it is possible to develop more reliable and accurate intrusion detection systems for satellite networks.

In the context of modeling cyber-attacks, stochastic modeling plays a crucial role in capturing the inherent uncertainty and randomness associated with malicious activities. Stochastic models incorporate probabilistic elements to represent the variability in attacker behavior, network conditions, and system responses. By accounting for uncertainty in the simulation environment, stochastic models can generate more realistic and representative scenarios, enabling researchers to evaluate the effectiveness of defense mechanisms under different degrees of uncertainty. Furthermore, stochastic modeling facilitates sensitivity analysis, allowing researchers to assess the robustness of defense strategies to variations in key parameters and assumptions. Overall, the integration of stochastic modeling techniques enhances the fidelity and reliability of simulation-based studies on cyber security in satellite communication systems.

2 OBJECTIVES

This paper aims to develop a simulation model for satellite communication systems, focusing on generating and analyzing basic communication data. The objectives are twofold. The first goal is to design and implement a logging system capable of capturing and analyzing crucial metrics associated with satellite communication, including uplink and downlink speeds, spectrogram speeds, latency, satellite position, and

time of signal reception. The second goal is to establish a malleable simulation model capable of detecting abnormal values in real-time, thereby flagging suspicious signal activity and enabling timely identification and classification of potential cyber threats. By establishing baselines for normal network behavior, this simulation model aims to enhance the security and reliability of satellite communication systems.

3 RELATED WORK

With the proliferation of the Internet of Things (IoT), satellites serve as critical nodes in interconnected networks. In brief, IoT is any network of devices with the technological capabilities to collect and exchange data between them (Abdul-Qawy et al. 2015). Satellites connected in IoT networks facilitate data exchange, command transmission, and coordination of various tasks essential for seamless operations (Talbi et al. 2023). One approach to modeling Inter-Satellite Networks (ISN) is with a systematic approach by identifying key properties like satellite movement predictability and intermittent connectivity (Ruiz de Azúa et al. 2018). Rather than creating new protocols from scratch, they review existing network models (VT, VN, MLSN, MANET, WSN, DTN) to adapt relevant features for ISNs, prioritizing interoperability with current systems. However, they acknowledge the need for a tailored ISN model due to unique characteristics. Thus, they propose an in-depth analysis to develop a new model specifically addressing ISN requirements, streamlining the design of routing protocols and network architectures for satellite communication systems.

Wang et al. (2022) discusses using a technique called stochastic geometry (SG) to model and analyze satellite communication networks, especially in low Earth orbit systems. Instead of focusing on modeling each individual satellite, SG looks at the total system, making it easier to understand and analyze. SG doesn't rely on specific satellite positions or shapes, which is useful for dynamic networks. It's especially important for LEO systems, where there are many satellites at lower altitudes, leading to higher interference. Traditional models assume satellites are evenly distributed, but in reality, coverage varies. The SG model seems to perform better with dynamic systems, rather than the static system that is discussed in this paper. Additionally, SG provides a robust framework for calculating performance metrics such as signal-to-noise ratios and bit error rates, which can be incorporated into later iterations of our logging system.

4 METHODOLOGY

In a simulation of satellite communication systems, basic communication data can be generated through the emulation of standard network behaviors. This process typically involves the creation of virtual nodes representing satellites, ground stations, and other network elements (bad actor ground stations), each equipped with simulated communication hardware and software.

The portion of the script that generates nodes allows for scalability, meaning that the user can add/subtract satellites and ground stations from the system. The model begins with a satellite system setup where the user can indicate the system time, number of satellites, number of ground stations, and number of bad actors. The user can also choose the locations of ground stations and bad actors. These nodes interact within a simulated environment, exchanging data between themselves. By accurately modeling the fundamental principles of communication and network operation, simulations can generate basic communication data that mirrors the behavior of actual satellite systems, providing a foundation for more complex analyses and scenario testing.

A MATLAB script was constructed using the satellite add-on package. The initial phase of the script involves the generation of synthetic data representative of various performance metrics associated with LEO satellite communications. Each metric of interest is given a probable range of data points that may be seen from bad actors or genuine sources. The algorithm then selects random samples from that range to average. This ensures the generated data closely aligns with real-world scenarios and is truly random following a uniform distribution. These average values also provide a consolidated representation of the typical performance characteristics exhibited by LEO satellite communication systems. Moreover, the

script is designed to capture and store these average values along with raw data for further analysis and reference.

The next critical aspect of the methodology involves the validation of metric values against predefined acceptable ranges. These ranges, as shown in Table 1, are established based on industry standards and known values.

Table 1: Industry standard lower and upper bound values for the acceptable range of each metric.

Metric	Lower Bound	Upper Bound
Uplink Speed (Mbps)	0	20
Downlink Speed (Mbps)	0	120
Spectrogram Speed (Hz)	50	70
Latency (ms)	594	624

The script integrates robust validation mechanisms to compare generated metric values against these predefined ranges. Any discrepancies identified, where metric values exceed the acceptable thresholds, prompt the script to issue warning messages, thereby alerting users to potential deviations from expected performance norms. The model first outputs the specified metrics for each satellite in the system then, error messages are produced for each data point that is outside of the acceptable ranges.

The final step entails presenting the generated data and calculated metrics in a structured format conducive to interpretation and analysis. The output includes average metric values, satellite locations, and time stamps, meticulously organized for clarity and comprehensibility. Satellite locations and time stamps are provided in the output as a means of identification for the given signal.

This communication model was then integrated into a dynamic satellite trajectory model that tracks the movement of satellites and calculates spectrogram speeds and latencies for the signals sent by the satellites. The calculated values of the performance measures are then tested against the chosen acceptable ranges.

In the next section, we provide an example implementation of the simulation model and logging system.

5 EXAMPLE IMPLEMENTATION

The simulation was conducted with two ground stations and an initial satellite group. The ground stations were labeled as "Ground Station 1" and "Bad Actor", with the latter being designated as malicious. The satellite group consisted of five satellites. The simulation, running for 24 hours with a sample time of 60 seconds, was able to capture various parameters and metrics related to satellite communication. The geographical positions of the satellites were calculated and visualized, providing insight into their latitudes, longitudes, and altitudes (Figure 2). This visualization facilitated an understanding of the spatial distribution of the satellites throughout the simulation period.

Additionally, the simulation determined the access intervals between each satellite and ground station pair. This information was crucial for evaluating the availability of communication links between satellites and ground stations over time.

Next, the simulation calculated latency metrics for each satellite-ground station pair. Latency, measured in milliseconds, was analyzed over time to assess the performance of communication links. Doppler shift values were also computed, providing insights into the frequency shifts experienced during satellite communication.

Finally, the simulation computed various performance metrics for each satellite, including average uplink and downlink speeds, latency, spectrogram speeds, satellite locations, and time of signal transmission. These metrics were crucial for evaluating the overall performance of the satellite communication system.

Figure 3 is an example of the data output for each individual satellite in the system. The user then receives a report about which metrics are in and out of range. The sample LEO satellite has downlink speeds, spectrogram speeds, and latencies in range. However, the uplink speed is triggering an "out-of-range" warning message. This message should prompt whoever is monitoring the satellite activity to investigate the signal sent between the satellite and the ground station. To more easily track the data across multiple satellites and communications, the data is translated into a csv file as shown in Figure 4.

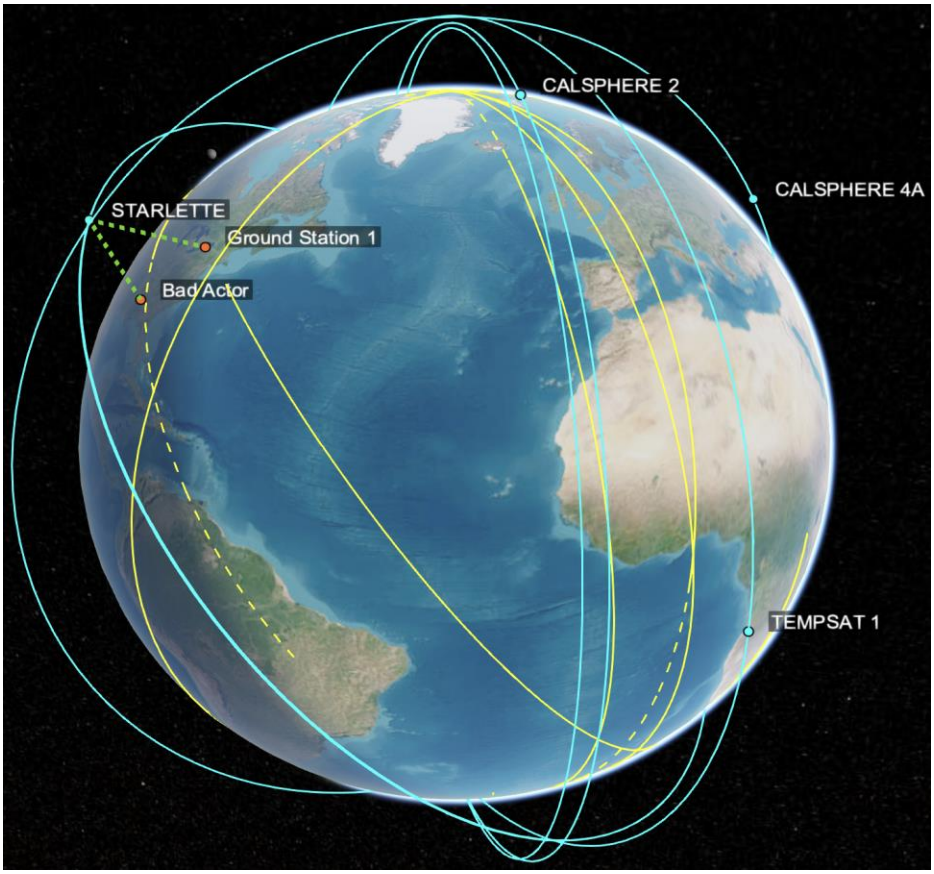

Figure 2: The network of nodes (satellites and ground stations) used in this model.

```
Metrics for Signal 1:
Satellite Name: CALSPHERE 1
Uplink Speed: 82.00 Mbps - Warning: Outside acceptable range (0 - 30 Mbps)
Downlink Speed: 182.00 Mbps - Within acceptable range (0 - 190 Mbps)
Latency: 10.45 ms - Warning: Outside acceptable range (4 - 7 ms)
Spectrogram Speed: 39.00 Hz - Within acceptable range (30 - 100 Hz)
Satellite Location (Latitude, Longitude, Altitude): (27.65, -53.63, 988193.32)
Time of Signal: 274.00 minutes
```

Figure 3: The command window output for the sample LEO satellite.

SatelliteName	UplinkSpeedMbps	DownlinkSpeedMbps	Latencyms	SpectrogramSpeedHz	Latitude	Longitude	Altitudekm	TimeOfSignalminutes	SuspiciousSignal
Number	Number	Number	Number	Number	Number	Number	Number	Number	Categorical
Satellite Name	Uplink Speed (Mbps)	Downlink Speed (Mbps)	Latency (ms)	Spectrogram Speed (Hz)	Latitude	Longitude	Altitude (km)	Time of Signal (minutes)	Suspicious Signal
CALSPHERE 1	82.00	182.00	10.45	39.00	27.65	-53.63	988193.32	274.00	Y
CALSPHERE 1	92.00	127.00	9.55	36.00	31.10	-53.90	987680.73	275.00	Y
CALSPHERE 1	28.00	110.00	8.75	97.00	34.55	-54.17	987264.42	276.00	Y
CALSPHERE 1	97.00	32.00	8.10	98.00	38.00	-54.43	986935.01	277.00	Y
CALSPHERE 1	96.00	98.00	7.65	86.00	41.44	-54.70	986682.28	278.00	Y

Figure 4: The output for sample signals represented in a csv file.

6 DISCUSSION

One notable aspect of the model is its flexibility in defining the simulation parameters. Users can specify the start time, stop time, and sample time, allowing for detailed investigations over specific time intervals with varying levels of granularity. This flexibility is crucial for studying satellite communication systems under different scenarios, such as during specific mission durations. Another key capability of the simulation is its ability to scale the model. Users can add multiple satellites and ground stations to the scenario, enabling the simulation of realistic network configurations. This feature is particularly valuable for evaluating the performance of satellite constellations and assessing their coverage, connectivity, and capacity.

The simulation's capability to calculate latency and other performance metrics is another significant strength. By simulating the delay between satellites and ground stations, users can theoretically analyze the latency of communication links and identify potential bottlenecks or performance limitations. Additionally, the simulation provides insights into key metrics such as uplink and downlink speeds, spectrogram speeds, and satellite locations, allowing for comprehensive performance analysis.

Moreover, the simulation facilitates data visualization and analysis through plots and log files. Visualization tools enable users to visualize the spatial distribution of satellites and ground stations, track satellite positions over time, and analyze latency trends. Log files provide a record of simulation results, enhancing traceability and enabling further post-processing and analysis of data.

In summary, the simulation code offers a powerful platform for studying satellite communication systems, providing flexibility, realism, and analytical depth. Its capabilities enable users to gain valuable insights into the performance of satellite networks, optimize their networks, and address various challenges in satellite communication applications.

The model currently assumes communication under ideal conditions. However, a real-world system would have other factors to consider such as atmospheric conditions or signal processing delays. Additionally, the randomization of metrics for simulation purposes, along with the aggregation of data to calculate metrics for each satellite, simplifies the analysis and neglects the diverse and dynamic nature of satellite communication networks. Furthermore, the model lacks comprehensive error handling mechanisms and performs limited range checking for metric values, potentially leading to misleading simulation results.

In terms of application limitations, the simulation does not account for specific communication protocols or network configurations. In particular, the model does not include some aspects that can significantly impact satellite communication performance in real-world scenarios. In addition, the assumption of a one-to-one mapping between satellites and ground stations is typically uncommon. In a real-life scenario, satellites typically communicate with many ground stations along their orbit. To that point, the static configuration of satellites and ground stations at the beginning of the simulation fails to capture the dynamic nature of satellite networks, which undergo continuous changes due to factors like satellite movement and ground station availability.

7 CONCLUSION AND FUTURE WORK

In the realm of cyber-attack modeling, stochastic modeling provides a nuanced understanding of the complex and dynamic nature of malicious activities. Unlike deterministic models, which assume fixed parameters and outcomes, stochastic models acknowledge the inherent unpredictability of cyber-attacks. By incorporating probabilistic distributions and random variables, stochastic models can simulate a wide range of potential attack scenarios, each with varying degrees of likelihood. This approach allows researchers to capture the diversity of attack behaviors, including their timing, intensity, and sophistication, which may evolve over time in response to changing network conditions and defensive measures.

Moreover, stochastic modeling enables the exploration of uncertainty in multiple facets of cyber security analysis. It can account for uncertainty due to attacker motivations and strategies, network traffic patterns, system vulnerabilities, and the effectiveness of defensive measures. This consideration of uncertainty can be built upon to provide valuable insights into the resilience and vulnerabilities of satellite communication systems to cyber-attacks. Although the tool created is not comprehensive of all aspects of satellite communication, it provides a foundation that can be built upon in the cybersecurity realm and transferred to other applications.

The current simulation model provides a solid foundation for logging satellite communication systems, but enhancements could further improve its capabilities. Future development could focus on incorporating advanced models to simulate atmospheric conditions and space weather's effects on signals, which can cause physical damage and signal interference (Welling 2010). Refining satellite orbit models and ground station positioning algorithms would improve simulation accuracy, particularly for complex satellite constellations. Satellites are crucial nodes in Internet of Things (IoT) networks, like Starlink (Starlink 2024), necessitating robust simulations to address cyber-attack risks. Finally, and perhaps the most useful future improvement, this model could be adapted to be a digital twin to the satellite system. This would allow the user to receive warnings about abnormal network activity in real time. Integration of advanced signal processing techniques and modulation schemes would broaden the simulation's applicability, while optimizing computational efficiency would enable larger-scale and more detailed analyses of satellite communication systems.

ACKNOWLEDGMENTS

Special thanks to Shanchieh Yang, Matthew Heller, Steve Wufeng, and Chanel Cheng from Rochester Institute of Technology for their support throughout this project.

REFERENCES

Abdul-Qawy, A. S., P. J. Pramod, E. Magesh, and T. Srinivasulu. 2015. “The Internet of Things (IoT): An Overview”. *International Journal of Engineering Research and Applications* 5(12):71-82.

Ruiz de Azúa, J. A., A. Calveras and A. Camps. 2018. “Internet of Satellites (IoSat): Analysis of Network Models and Routing Protocol Requirements”. *IEEE Access* 6:20390-20411.

Starlink. 2024. Starlink Technology. https://www.starlink.com/technology, accessed 21st June 2024.

Talbi, D., Z. Gal, and J. Sztrik. 2023. “Low Latency and High-Speed Communication Service with LEO Satellite Constellation”. In *2023 International Conference on Information and Digital Technologies (IDT)*, June 20th-22nd, Zilina, Slovakia, 251-256.

Usman, M., M. Qaraqe, M. R. Asghar and I. Shafique Ansari. 2020. “Mitigating Distributed Denial of Service Attacks in Satellite Networks”. *Transactions on Emerging Telecommunications Technologies* 31(6):e3936.

Wang, R., M. A. Kishk and M.-S. Alouini. 2022. “Ultra-Dense LEO Satellite-Based Communication Systems: A Novel Modeling Technique”. *IEEE Communications Magazine* 60(4):25-31.

Welling, D. T. 2010. “The Long-term Effects of Space Weather on Satellite Operations”. *Annales Geophysicae* 28(6):1361–1367.

Zhang, Y., Y. Wang, Y. Hu, Z. Lin, Y. Zhai, L. Wang, *et al*. 2022. “Security Performance Analysis of LEO Satellite Constellation Networks under DDoS Attack”. *Sensors* 22(19):7286.

AUTHOR BIOGRAPHIES

LAILA MASHAYEKHI is a dual degree Bachelor/Master of Science student in the Industrial and Systems Engineering Deparetment at Rochester Institute of Technology. Her research interests include simulation modeling and analyiss of supply chain, manufacturing, and cyber security systems. Her email address is lam3020@rit.edu.

MICHAEL E. KUHL is a Professor in the Industrial and Systems Engineering Department at Rochester Institute of Technology. His research interests include modeling and simulation of stochastic arrival processes, and the application of simulation to autonomous material handling, healthcare, and manufacturing systems. He has served on the WSC Board of Directors representing the INFORMS Simulation Society (2016-2023). He has also served WSC as Proceedings Editor (2005), Program Chair (2013), and Mobile App Chair (2014-2019, 2022-2024). His email address is mekeie@rit.edu.