L3Harris: Satellite Cyberattack Detection

Purdue: Shrenick Gannamani, Vanessa Jan, Kabir Jain, Michelle Jyi – TA: Mahima Malhotra
UC Colorado Springs: Marlin Jaramillo, Dylan Truesdell
CU Boulder: Tate Charboneau, Vraj Patel
MSU Denver: Angela Fleenor

INTRODUCTION

Background

- Cybersecurity protects computers, data, and networks from unauthorized access and attacks
- Satellite networks are vulnerable to cyber threats, which can be monitored using:
  - **Deep Packet Inspection (DPI)** – Analyzes network traffic granularly
  - **Machine Learning (ML)** – Detects anomalies and potential cyberattacks

Motivation

- Why study onboard satellite communications?
  - Research exists on satellite-to-ground cybersecurity, but much less on onboard cybersecurity
  - Onboard satellite functions produce data that does not reach the ground. This data could hold a wealth of information that could inform cybersecurity
- Why satellite cyberattacks?
  - Satellite cyberattacks can disrupt critical global infrastructure essential for communication, navigation, national security, economic stability, and more
- Why simulated data?
  - As a generally protected/proprietary technology, satellite information is not publicly accessible
  - Simulation is used extensively in space operations for testing and modeling because of limited data accessibility.

The Goal

- Utilize machine learning models to analyze onboard satellite data to detect potential cyberattacks, preventing potentially catastrophic impacts.

RESEARCH AND PROJECT WORK

Satellite Day-in-the-Life Model

- Developed a day-in-the-life model representing a typical day for a CubeSat (a type of small satellite, as displayed in Figure 1) to help us simulate a satellite with a reasonable command set
- Researched messages/commands commonly sent between components
- Used SPARTA (Space Attack Research and Tactic Analysis shown in Figure 3), a matrix that defines and categorizes different kinds of cyberattacks specifically for satellites, to research common cyberattacks
- Developed sample use case:
  - Determined mission for our simulated satellite to carry out during cyber-attack simulation
  - Determined possible cyber-attacks that this satellite may experience in a real-world scenario

NOS3 Satellite Simulation

- Utilized NOS3, a small satellite simulator developed by NASA, to simulate our CubeSat model (Figures 1 and 2)
- Studied the space communication protocols used by NOS3
- Used our Day-in-the-Life model as a template for simulating data on NOS3
- Used Tshark, a network traffic analyzer, within NOS3 to capture satellite transmission packet data for training a machine learning model

Analysis of Packet Data

- Used Tshark and Wireshark, tools used to analyze network traffic, to understand and clean data gathered from the NOS3 simulation (shown in Figure 4), specifically for:
  - Scraping packet data to find keywords relating to satellite commands
  - Filtering and organizing packet data based on packet type
  - Cleaning the packet dataset by discarding corrupted packets and packets containing irrelevant information

Machine Learning Algorithms

- Researched effective machine learning algorithms and chose optimal algorithms to analyze satellite packet data and detect potential cyber threats:
  - Long Short-Term Memory (LSTM) Model – An effective model for working with time-series data and determining cyber anomalies through temporal (timing) data
  - Isolation Forest Model – A model well-suited for finding anomalies in a given set of data
- Utilized data extracted from network traffic to train the Machine Learning models

CONCLUSION

- Researched what a typical Day-in-the-Life of a small satellite looks like to build a dataset simulating a small satellite in a normal day
- Researched common cyberattacks that small satellites are vulnerable to in conjunction with the SPARTA Matrix
- Utilized NOS3 simulator to generate sample CubeSat data for machine learning algorithm training
- Used Tshark and Wireshark to analyze telemetry data
- Simulated cyberattack data on NOS3 satellite simulator
- Trained Isolation Forest and LSTM Machine Learning models

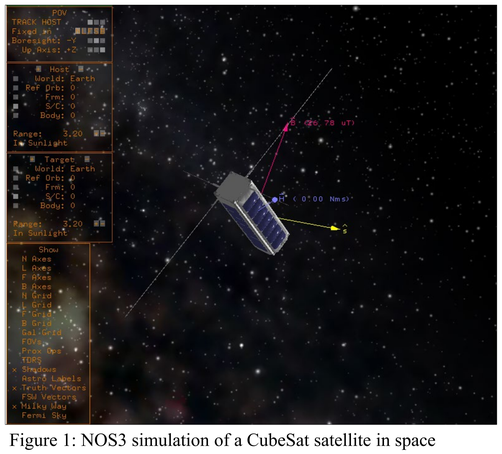

Figure 1: NOS3 simulation of a CubeSat satellite in space

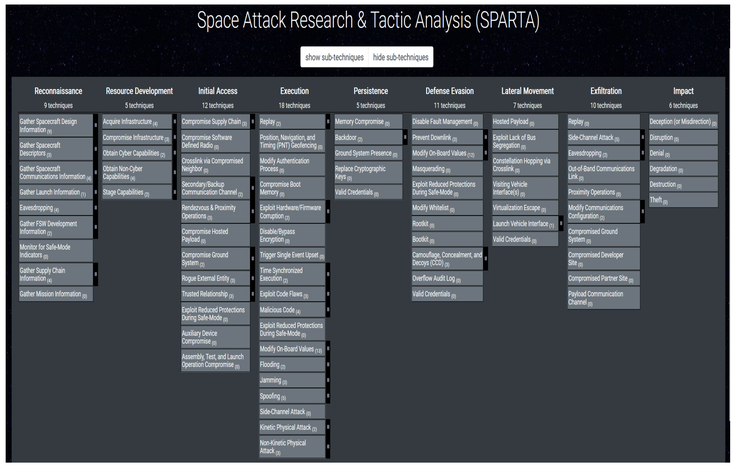

Figure 3: Image of SPARTA Matrix

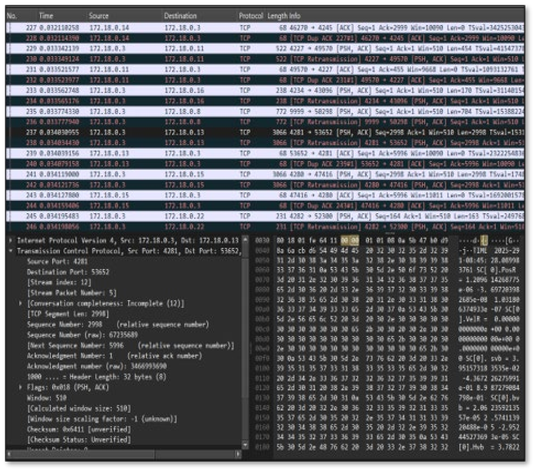

Figure 4: Example of network packet data analyzed using Wireshark

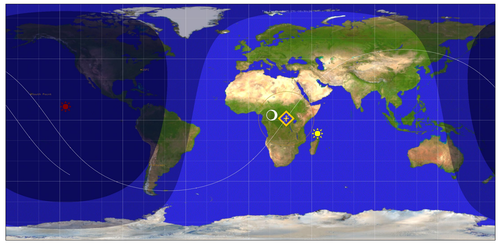

Figure 2: Map of the path for the simulated satellite

REFERENCES

- Cybersecurity framework. NIST. (2024, October 31). https://www.nist.gov/cyberframework
- Mitre ATT&CK®. MITRE ATT&CK®. (n.d.). https://attack.mitre.org/
- Sparta: The Aerospace Corporation.. (n.d.). https://aerospace.org/sparta
- He, J., Cheng, Z., & Guo, B. (2022, August 24). Anomaly detection in satellite telemetry data using a sparse feature-based method. MDPI. https://www.mdpi.com/1424-8220/22/17/6358
- Artificial Intelligence. NIST. (2024a, September 25). https://www.nist.gov/artificial-intelligehttps://github.com/nasa/nos3/wikince
- NASA Operational Simulator for Small Satellites (NOS3) Wiki. NASA. (2024, October 21). https://github.com/nasa/nos3/wiki

FUTURE GOALS

Explore other "Day in the Life" scenarios:

We analyzed anomalies in a satellite whose purpose was to photograph the earth. What would we find if we did the same in a satellite whose purpose was to measure space weather or boost radio communications? Exploring other DITL scenarios would help us understand how our model applies to different scenarios.

Test model on real-world satellite data:

Intra-satellite communications data is not readily available. We utilized simulated data for our project. We could work to gather private intra-satellite communications data. Training or evaluating our model using that data would expand our accuracy or give us further insight into our model's performance.

Explore applicability of model with other types of network traffic:

Currently, our model is designed to analyze the network traffic data of satellites, performing anomaly detection to identify potential satellite cyberattacks. However, satellites are not the only devices susceptible to cyberattacks, and although this is beyond the scope of our project, it could be interesting to explore the applicability of our model to the network traffic data of cellular devices.

Acknowledgements: Our team sincerely thanks the following people for supporting our project:
Dr. Tomás Peña, Paul Kroszczynski, Dr. Daniel Hirleman, Dr. Mark Daniel Ward, Jessica Jud, Kali Lacy, Mia Sartain, and the collective Data Mine team.

Data Mine of the Rockies Spring 2025