



Threat Data Generation for Space Systems

Meghan Galiardi Sahakian, Srideep Musuvathy,
Jamie Thorpe, Stephen Verzi, Eric Vugrin,
Matthew Dykstra

2021 IEEE Space Computing Conference (SCC)

August 23-26, 2021



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Outline



1. Background
2. Motivating Example
3. Data Generation Methods
4. Evaluation Metrics
5. Motivating Example Results
6. Future Work

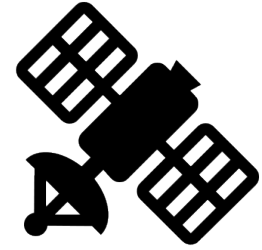


- United States government critically depends on space systems for government and commercial applications
- As cost and accessibility barriers to space decrease, threats to US space systems increase including cyber-attacks aimed to disrupt, deny, deceive, and degrade national security functions
- Technologies implementing intrusion detection systems and automated threat responses are needed to increase the cyber resilience of space systems
- A key challenge to the development of cyber resilience technologies for space systems is the sparsity of threat data needed for processing or training sets

Research consists of two main components:
(1) the algorithms for data generation
(2) qualitative and quantitative metrics for evaluating the generated data

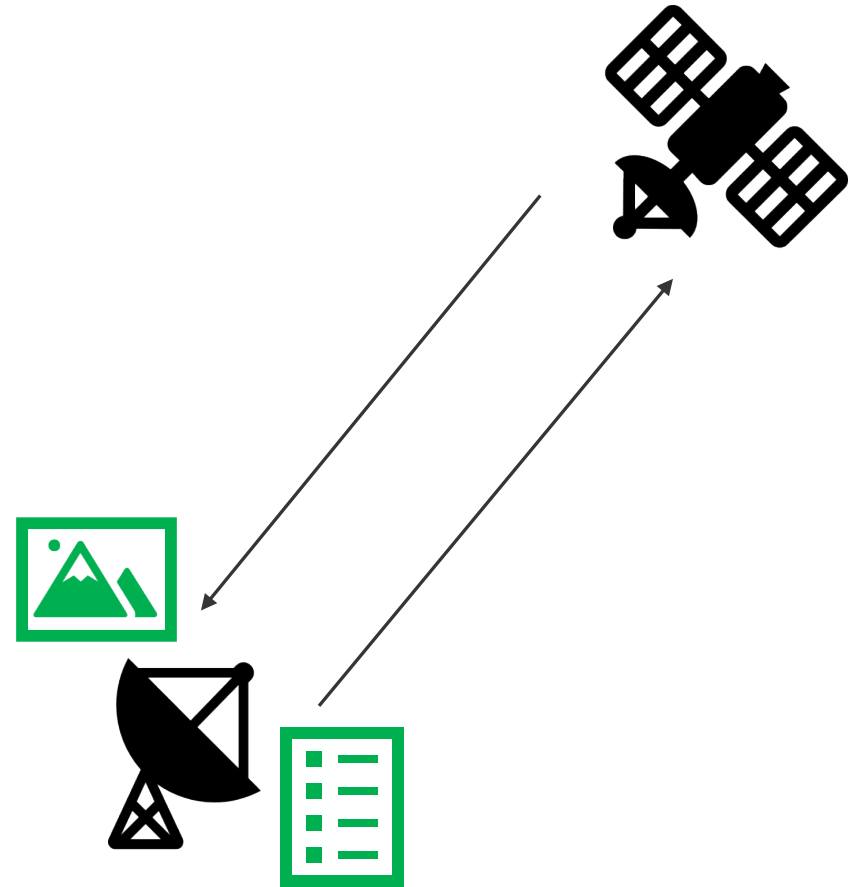
Motivating Example: System of Interest

- CubeSat in low Earth orbit



Motivating Example: System of Interest

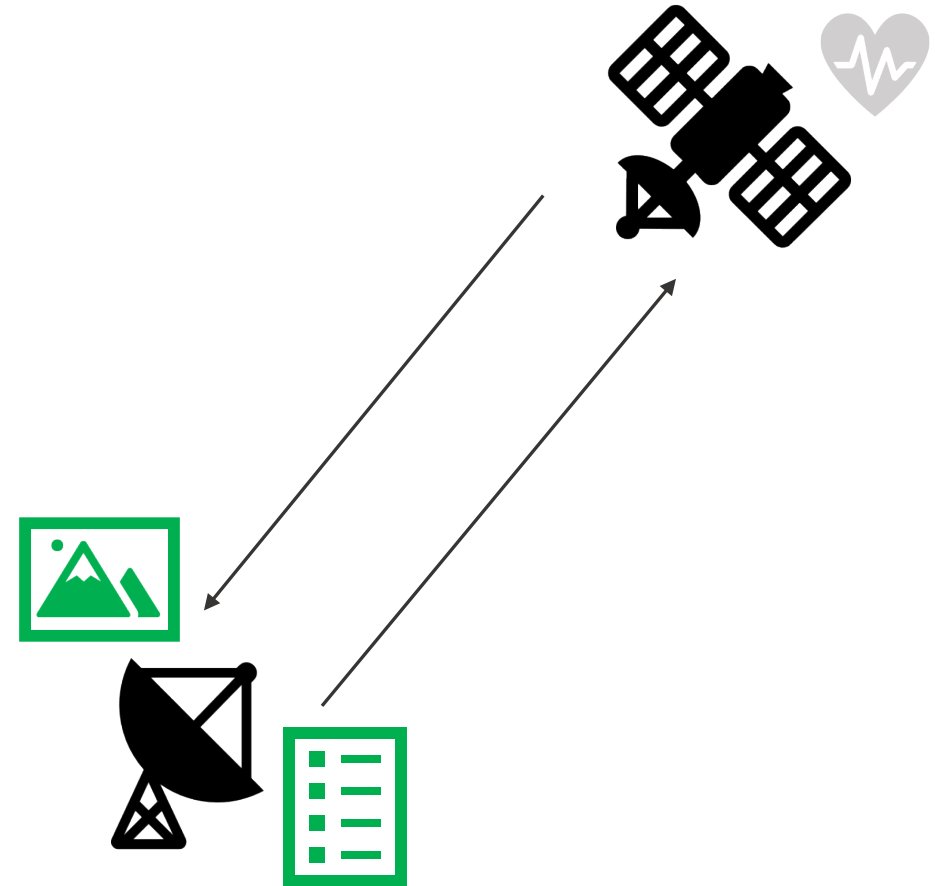
- CubeSat in low Earth orbit
- Equipped with a camera payload
- Command table updates from ground station specify when the camera payload should take images and downlink the data to the ground station



Motivating Example: System of Interest



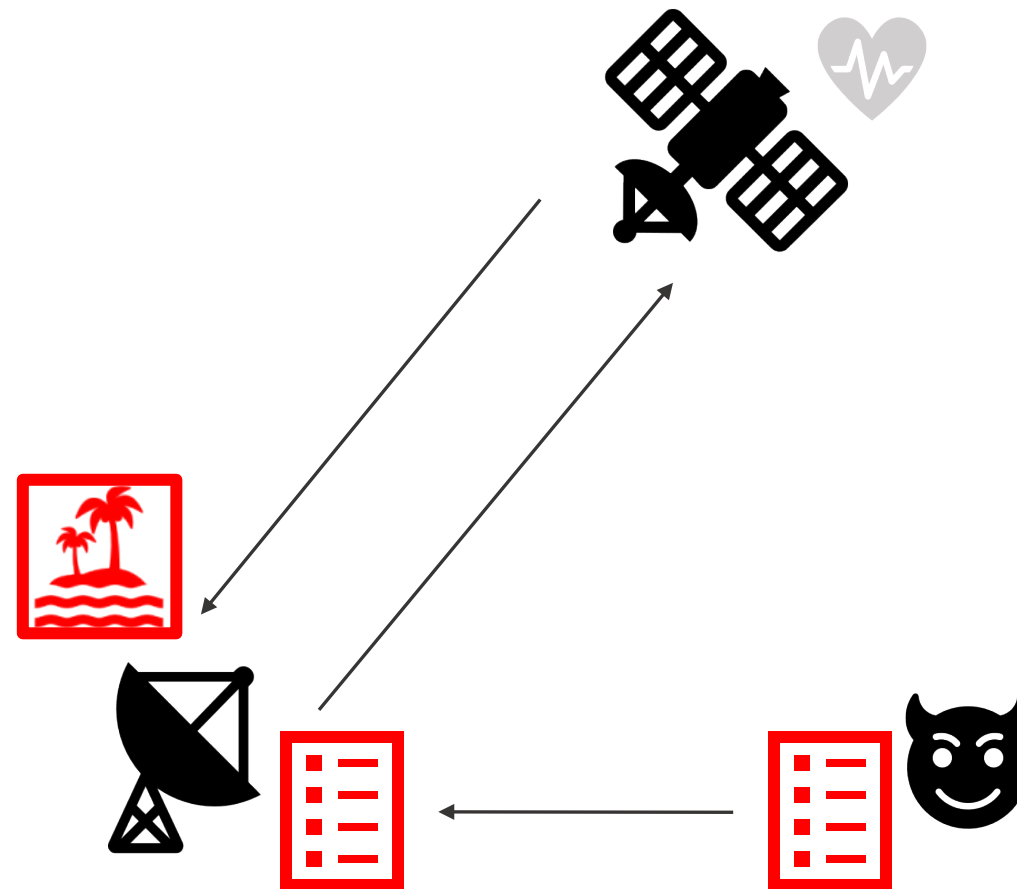
- CubeSat in low Earth orbit
- Equipped with a camera payload
- Command table updates from ground station specify when the camera payload should take images and downlink the data to the ground station
- State of health monitoring system that tracks various telemetry fields, including:
 - satellite position, velocity
 - camera status
 - memory buffer
 - images transmitted to ground station



Motivating Example: Attacks



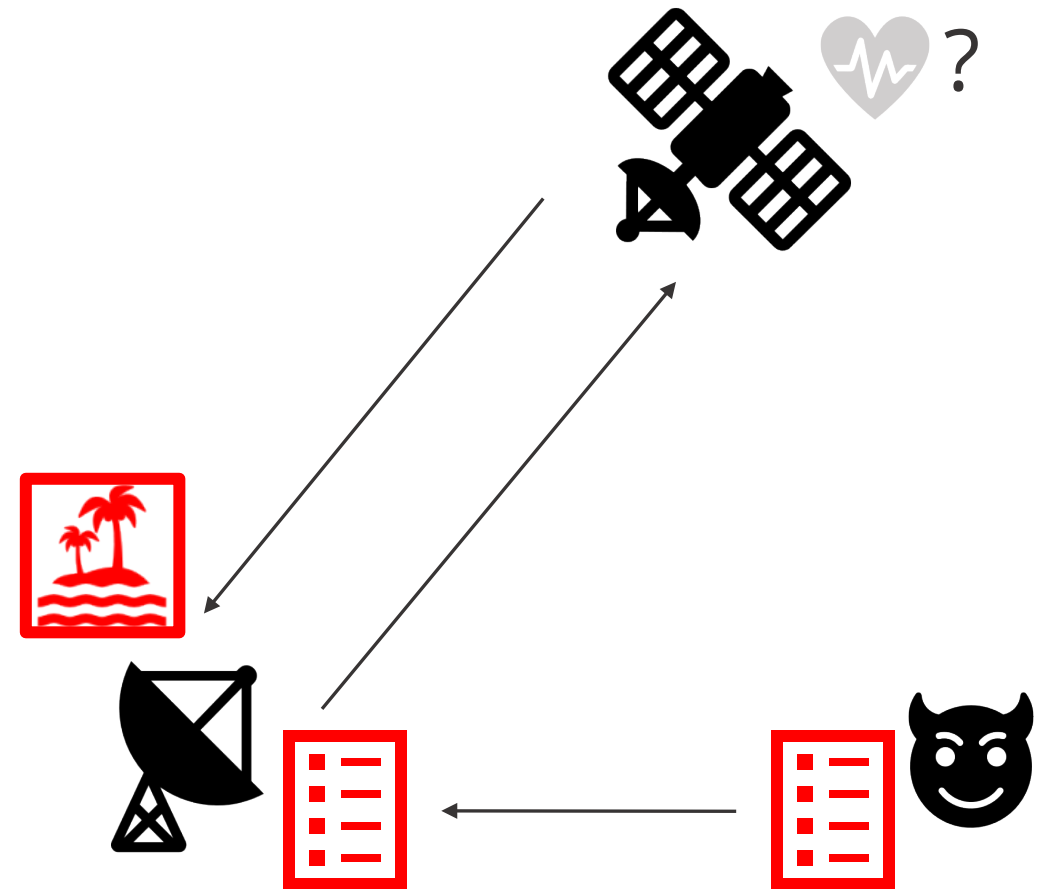
- Operators are concerned about an insider executing a command table corruption attack
- Attack could compromise mission by
 - preventing the camera from powering on
 - operating the camera at the wrong time so the image collected is useless
 - operating the camera so much so that the memory buffer is full



This scenario is illustrative and does not intend to describe a real system or real threats

Motivating Example: Mitigation

- Operators are interested in the development of an anomaly detection algorithm that
 - uses state of health data
 - detects the command table corruption
 - implements mitigating actions
- Algorithm development requires threat data for testing
- Operators have no real threat data and only a real-time testbed of their system



What can be done to help the testing of the anomaly detection algorithm with a lack of data?

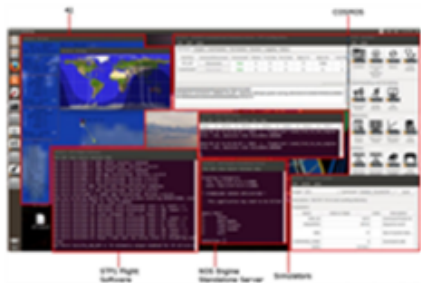
NOS³ Emulation



Data Generation Methods



NOS³
Emulation



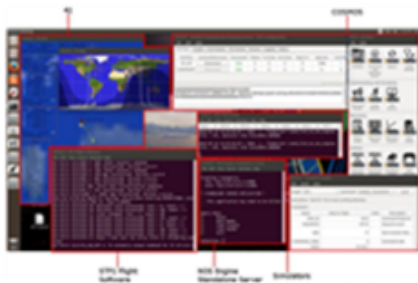
“Real” Threat
Data



Data Generation Methods



NOS³
Emulation



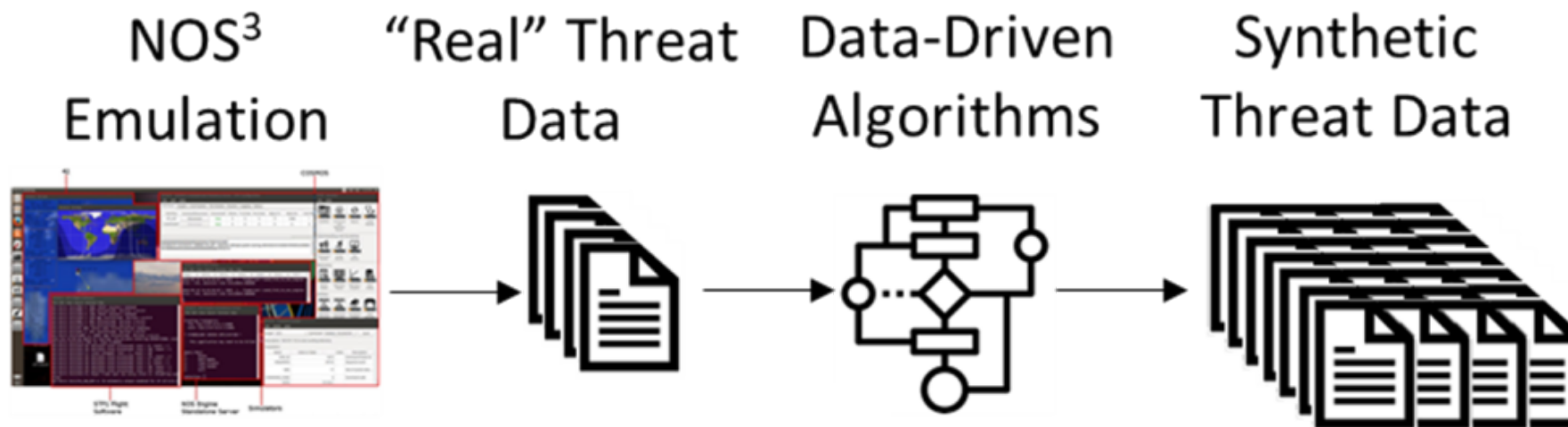
“Real” Threat
Data

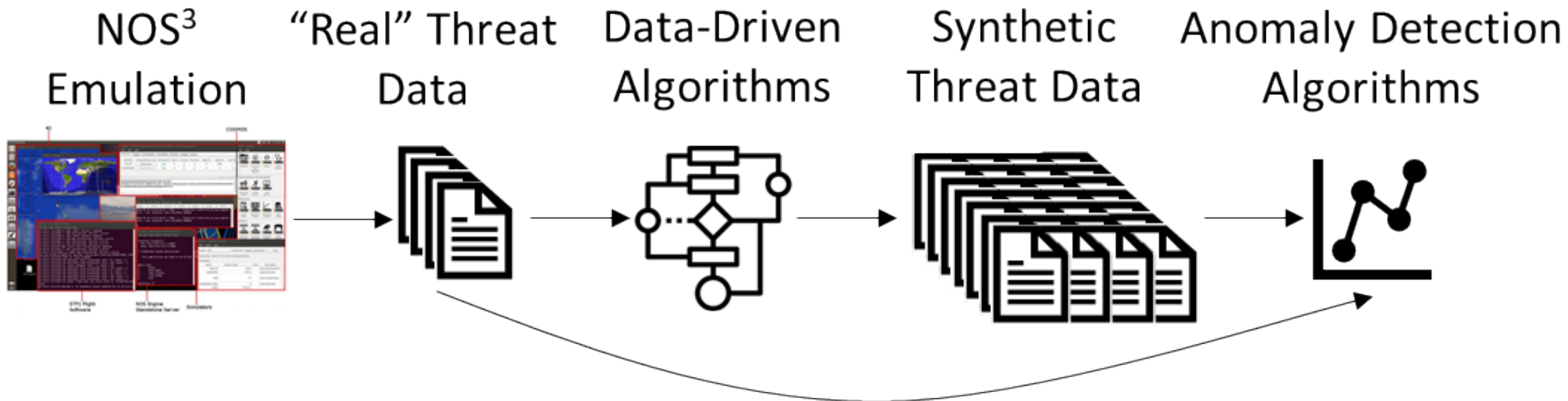


Data-Driven
Algorithms



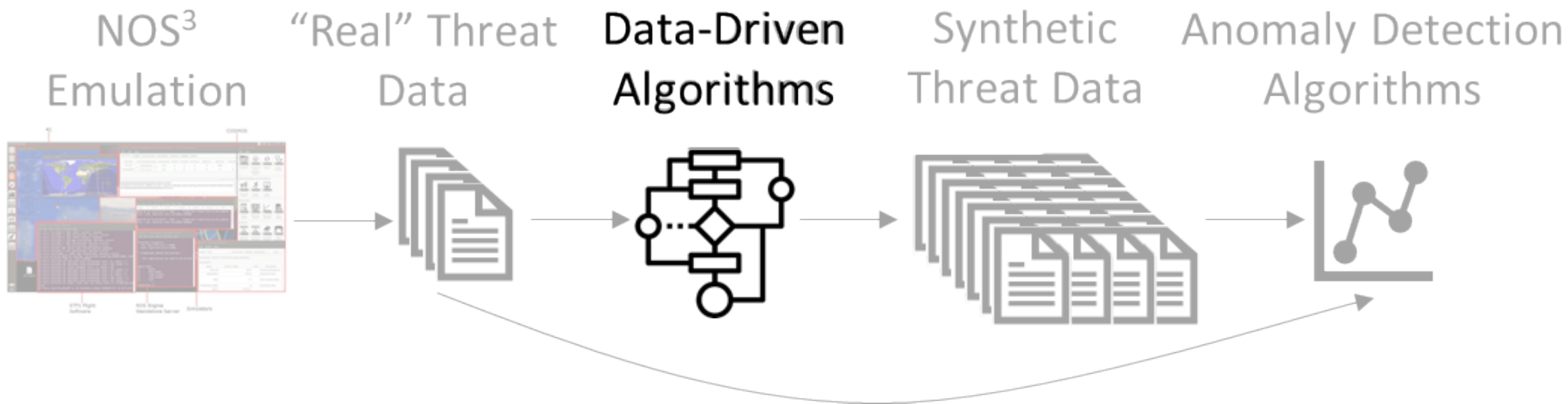
Data Generation Methods





Approach: Augment small data set collected from emulation and with large synthetic data set generated by data-driven models

Data Generation Methods: Data-Driven Algorithms



Data-Driven Algorithms

- Generative Adversarial Networks (GANs)
- Variational Auto-Encoders (VAEs)
- Generative Algorithm for Multi-Variate Timeseries (GAMVT)

Data Generation Methods: GAMVT Deep Dive

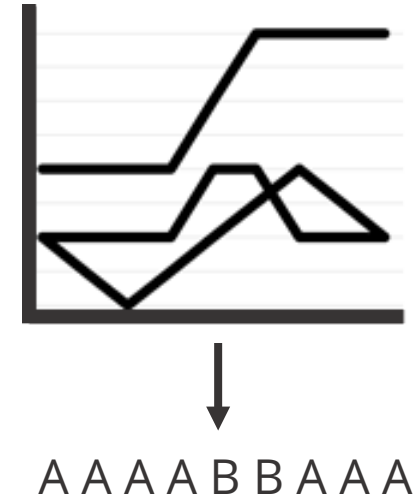


1. Pre-process data

Data Generation Methods: GAMVT Deep Dive



1. Pre-process data
2. **Characterize “real” data**
 - a) **Apply TICC¹**
 - b) Develop cluster patterns
 - c) Develop section statistics
 - d) Develop value statistics

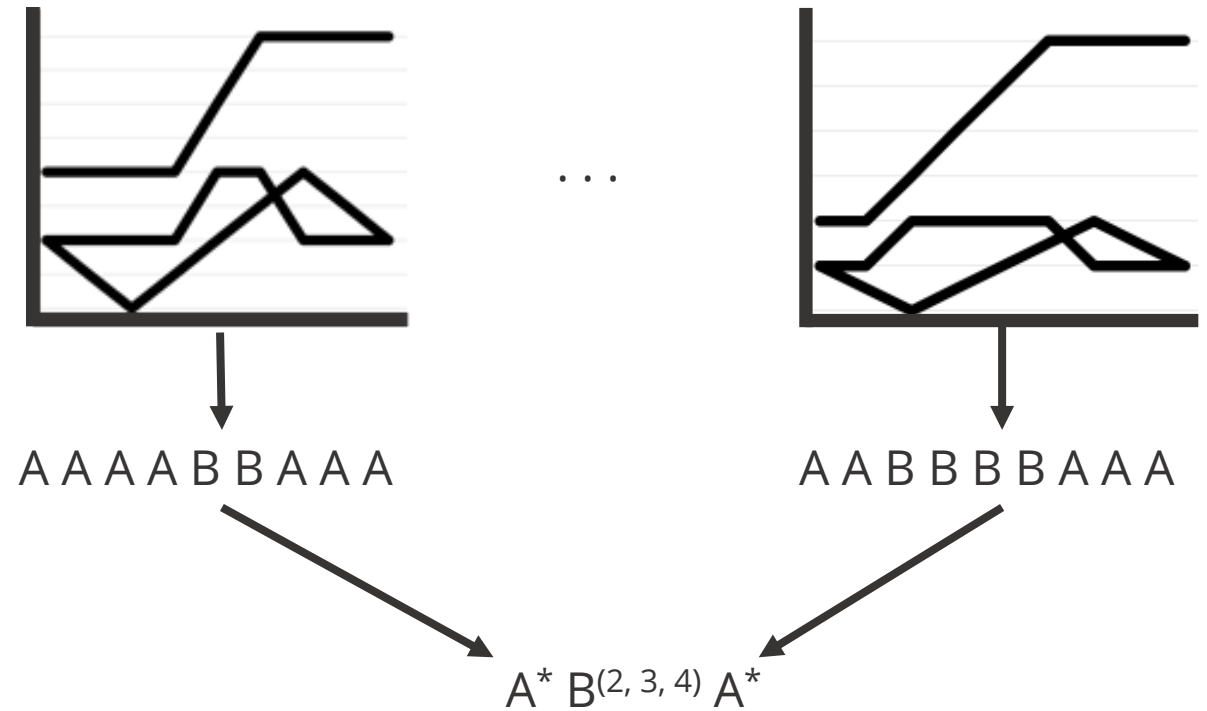


¹ D. Hallac, S. Vare, S. Boyd, and J. Leskovec, “Toeplitz inverse covariance-based clustering of multivariate time series data,” in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.

Data Generation Methods: GAMVT Deep Dive



1. Pre-process data
2. **Characterize “real” data**
 - a) Apply TICC¹
 - b) Develop cluster patterns**
 - c) Develop section statistics
 - d) Develop value statistics

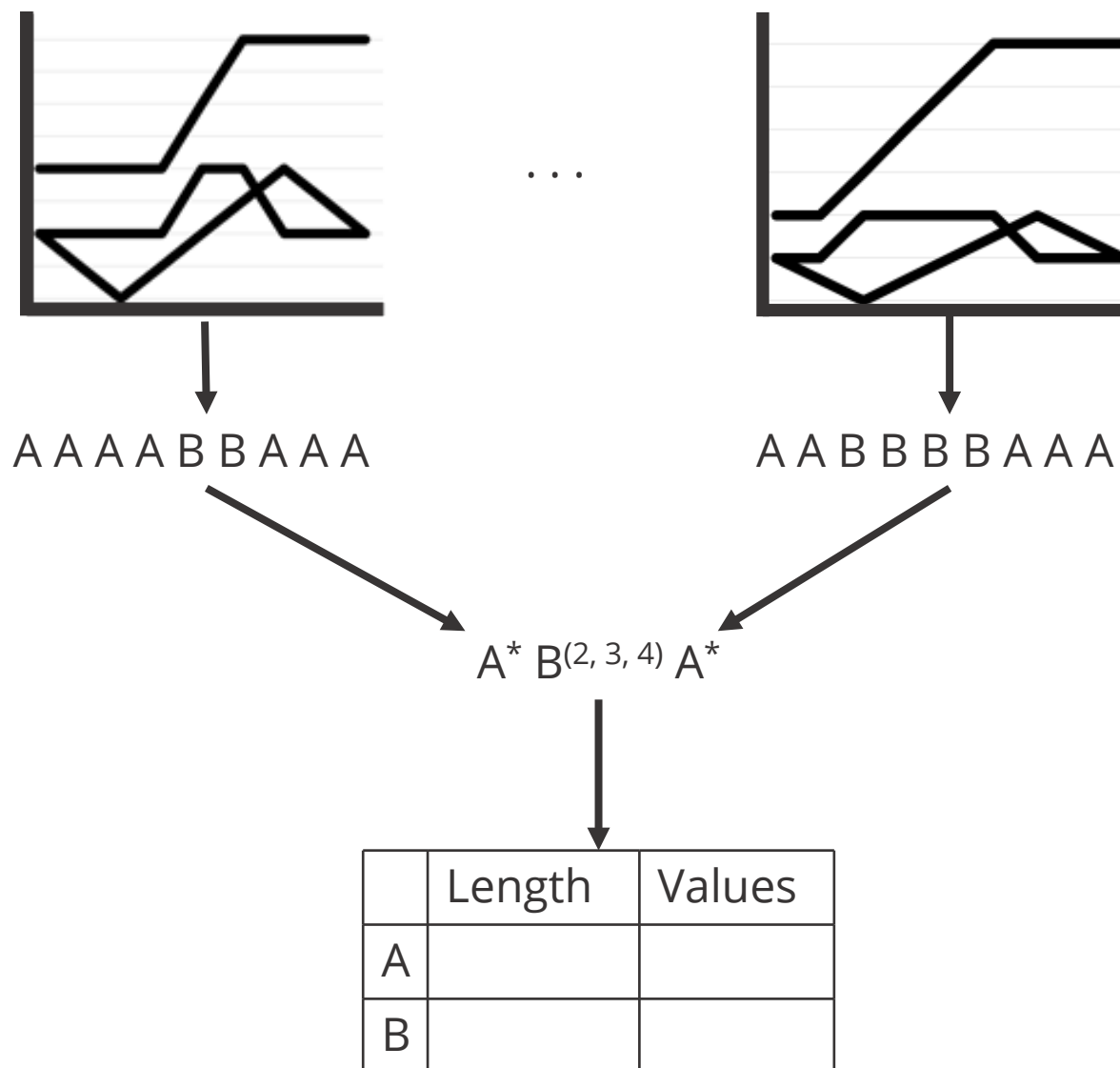


¹ D. Hallac, S. Vare, S. Boyd, and J. Leskovec, “Toeplitz inverse covariance-based clustering of multivariate time series data,” in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.

Data Generation Methods: GAMVT Deep Dive



1. Pre-process data
2. **Characterize “real” data**
 - a) Apply TICC¹
 - b) Develop cluster patterns
 - c) **Develop section statistics**
 - d) **Develop value statistics**



¹ D. Hallac, S. Vare, S. Boyd, and J. Leskovec, "Toeplitz inverse covariance-based clustering of multivariate time series data," in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.

Data Generation Methods: GAMVT Deep Dive



1. Pre-process data
2. Characterize “real” data
 - a) Apply TICC¹
 - b) Develop cluster patterns
 - c) Develop section statistics
 - d) Develop value statistics
3. **Generate synthetic data**
 - a) **Select cluster pattern**
 - b) Apply section statistics
 - c) Apply value statistics

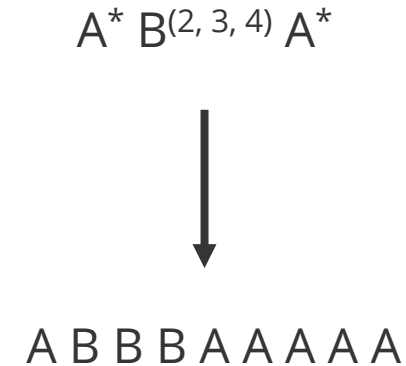
$$A^* B^{(2, 3, 4)} A^*$$

¹ D. Hallac, S. Vare, S. Boyd, and J. Leskovec, “Toeplitz inverse covariance-based clustering of multivariate time series data,” in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.

Data Generation Methods: GAMVT Deep Dive



1. Pre-process data
2. Characterize “real” data
 - a) Apply TICC¹
 - b) Develop cluster patterns
 - c) Develop section statistics
 - d) Develop value statistics
3. **Generate synthetic data**
 - a) Select cluster pattern
 - b) **Apply section statistics**
 - c) Apply value statistics

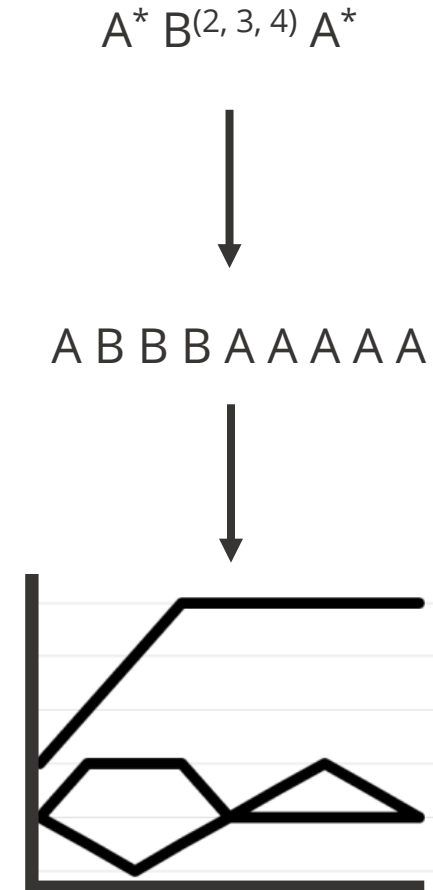


¹ D. Hallac, S. Vare, S. Boyd, and J. Leskovec, “Toeplitz inverse covariance-based clustering of multivariate time series data,” in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.

Data Generation Methods: GAMVT Deep Dive



1. Pre-process data
2. Characterize “real” data
 - a) Apply TICC¹
 - b) Develop cluster patterns
 - c) Develop section statistics
 - d) Develop value statistics
3. **Generate synthetic data**
 - a) Select cluster pattern
 - b) Apply section statistics
 - c) **Apply value statistics**



¹ D. Hallac, S. Vare, S. Boyd, and J. Leskovec, “Toeplitz inverse covariance-based clustering of multivariate time series data,” in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.

Data Generation Methods: GAMVT Deep Dive



1. Pre-process data
2. Characterize “real” data
 - a) Apply TICC¹
 - b) Develop cluster patterns
 - c) Develop section statistics
 - d) Develop value statistics
3. Generate synthetic data
 - a) Select cluster pattern
 - b) Apply section statistics
 - c) Apply value statistics
4. **Post-process synthetic data**

¹ D. Hallac, S. Vare, S. Boyd, and J. Leskovec, “Toeplitz inverse covariance-based clustering of multivariate time series data,” in Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017, pp. 215–223.



- Quality Metric
 - How similar is the synthetic data to the real data?
- Diversity Metric
 - How different is synthetic data from the real data?
 - How different is the synthetic data from itself?

Ideal synthetic data should balance both quality and diversity.



- Quality Metric
 - How similar is the synthetic data to the real data?
- Diversity Metric
 - How different is synthetic data from the real data?
 - How different is the synthetic data from itself?

$$Q(T, G) = \frac{\text{Accuracy}(M(G))}{\text{Accuracy}(M(T))}$$

$$D_1(T_i, G_i) = \frac{\frac{1}{|G_i|} \sum_{x \in G_i} \min_{y \in T_i} d(x, y)}{\frac{N}{|T_i|} \sum_{x \in T_i} \min_{y \in T_i - x} d(x, y)}$$

$$D_2(T_i, G_i) = \frac{\frac{1}{|G_i|^2} \sum_{x \in G_i} \sum_{y \in G_i} d(x, y)}{\frac{1}{|T_i|^2} \sum_{x \in T_i} \sum_{y \in T_i} d(x, y)}$$

Ideal synthetic data should balance both quality and diversity.

Back To Motivating Example

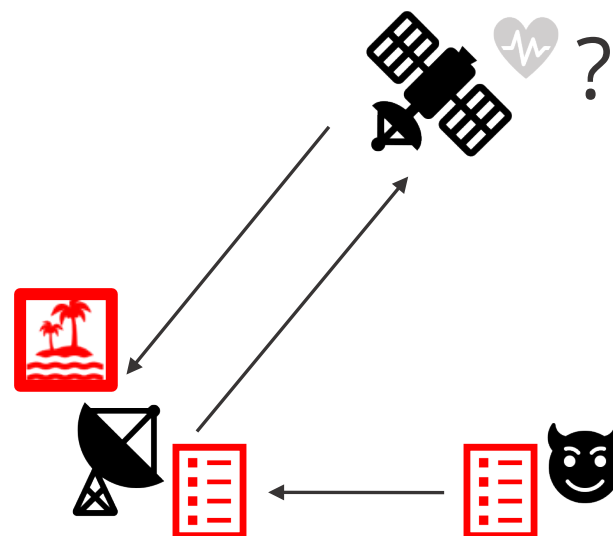


Scenarios

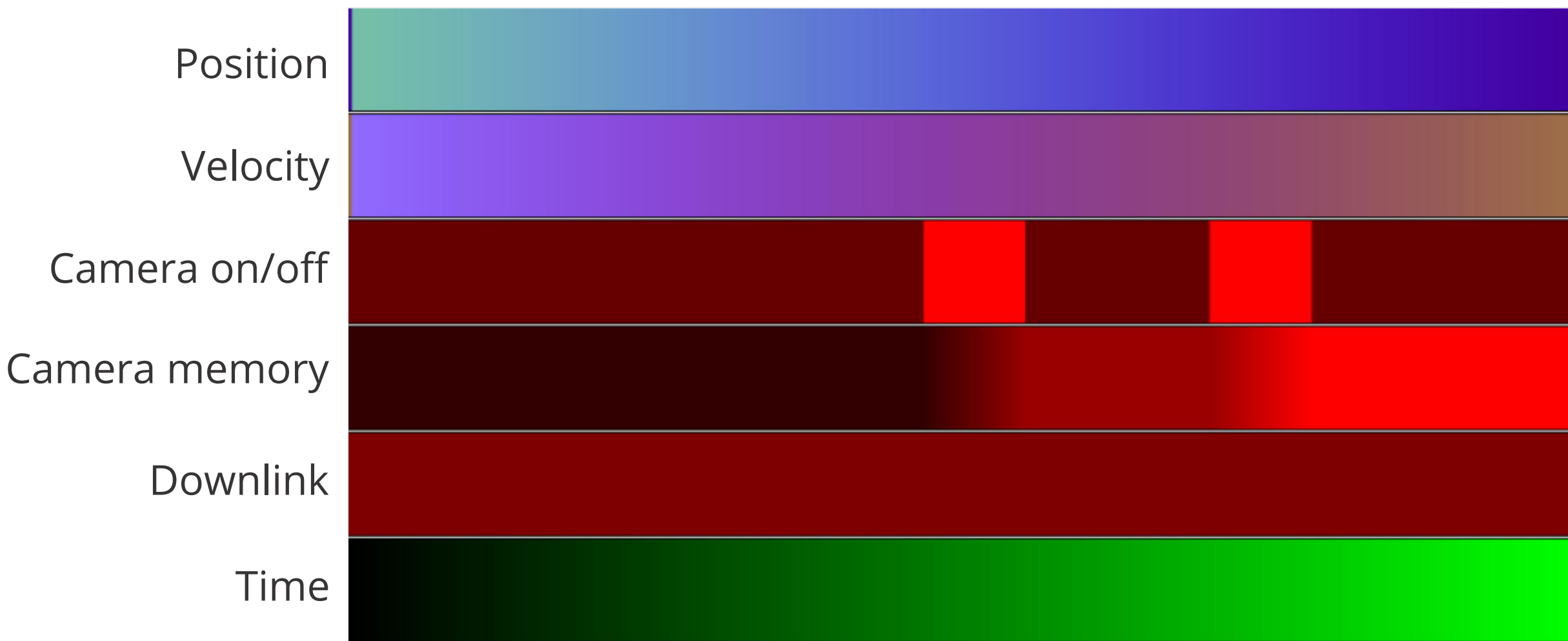
Class	Effect	Samples
Class 0	No attack. Expected behavior is to have two camera experiments execute at times 14 minutes and 21 minutes, respectively.	5
Class 1	Camera experiments do not execute.	3
Class 2	Camera experiments executed, but were performed at the wrong time, resulting in an image over the wrong location.	20
Class 3	Additional camera experiments executed in attempts to run the camera buffer out of memory.	20

Data Collection

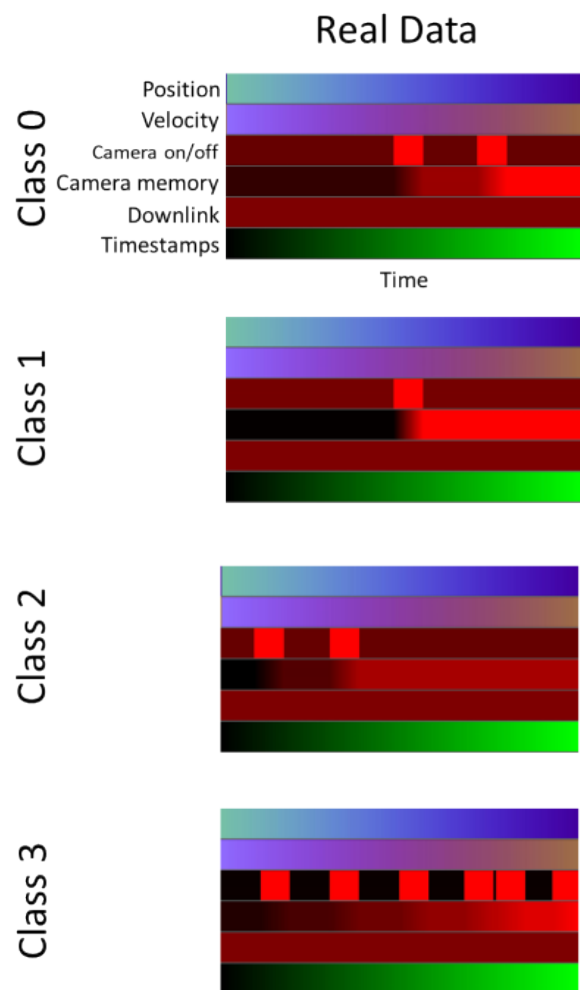
- Spacecraft x, y, and z position
- Spacecraft x, y, and z velocity
- Camera on/off status
- % of camera memory used
- Status of downlink to ground station
- Timestamp



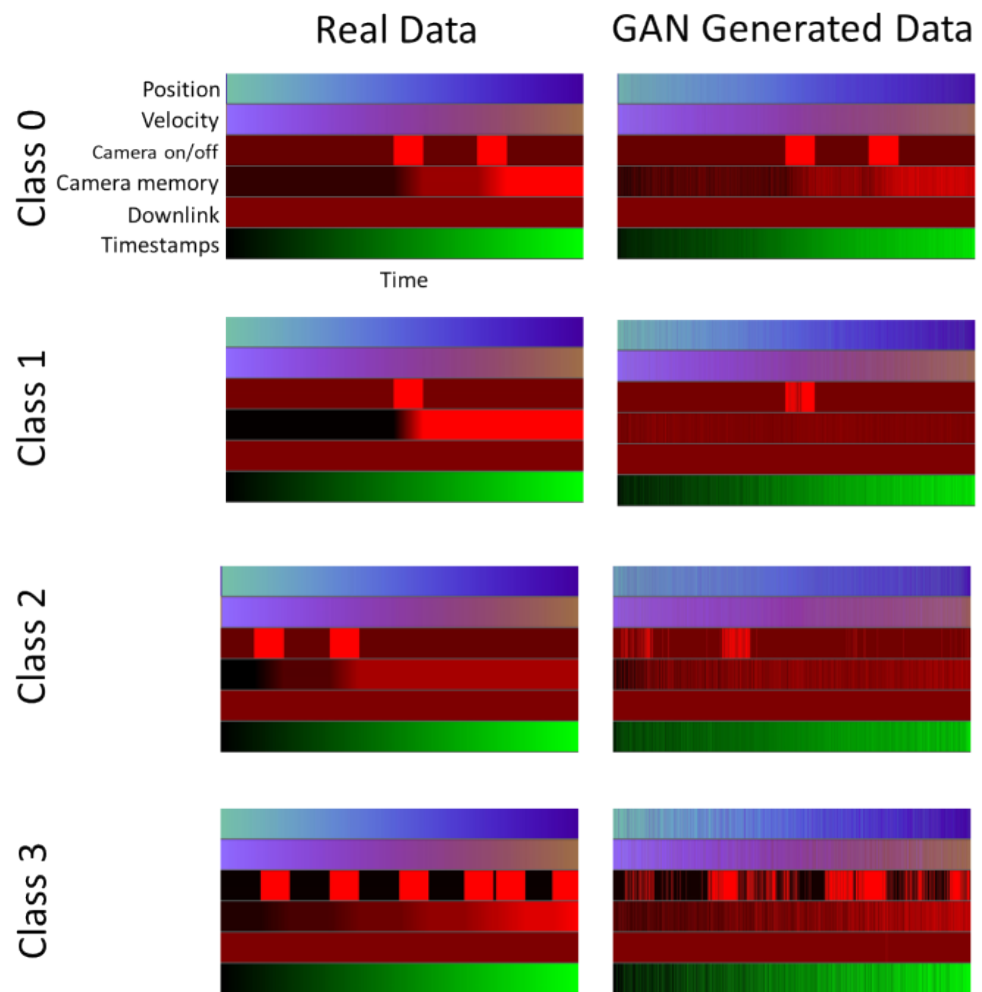
Qualitative Results



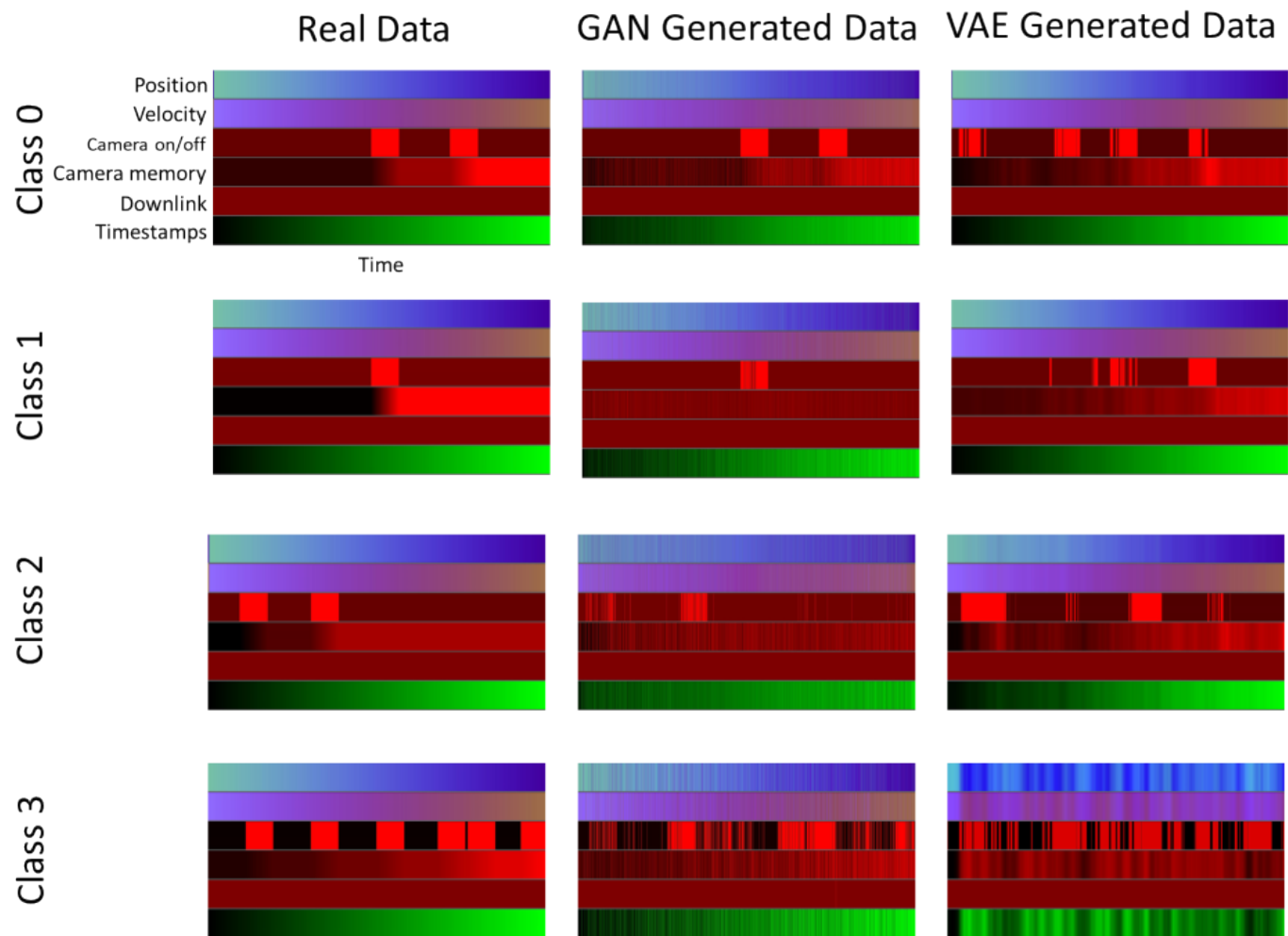
Qualitative Results



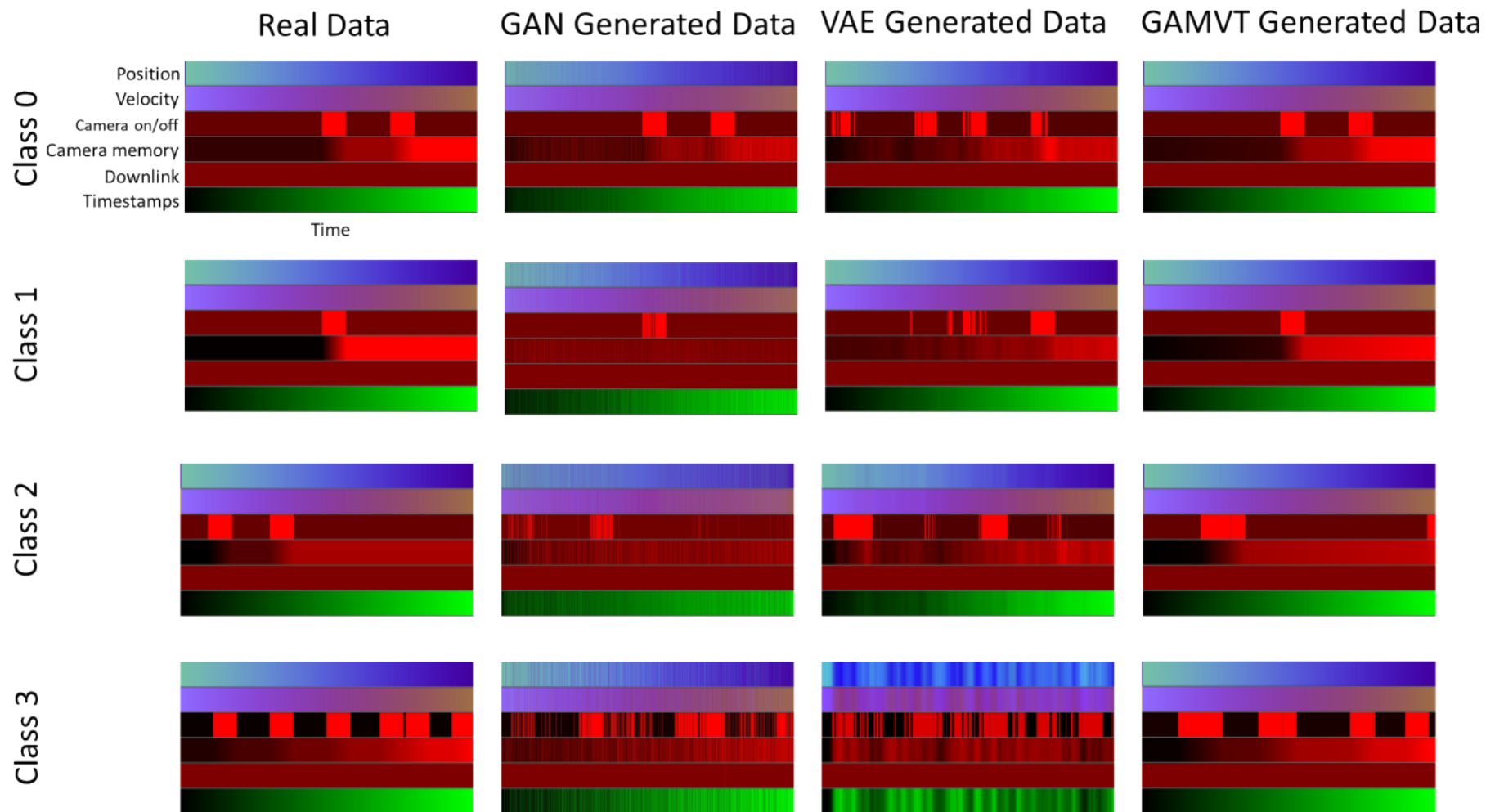
Qualitative Results



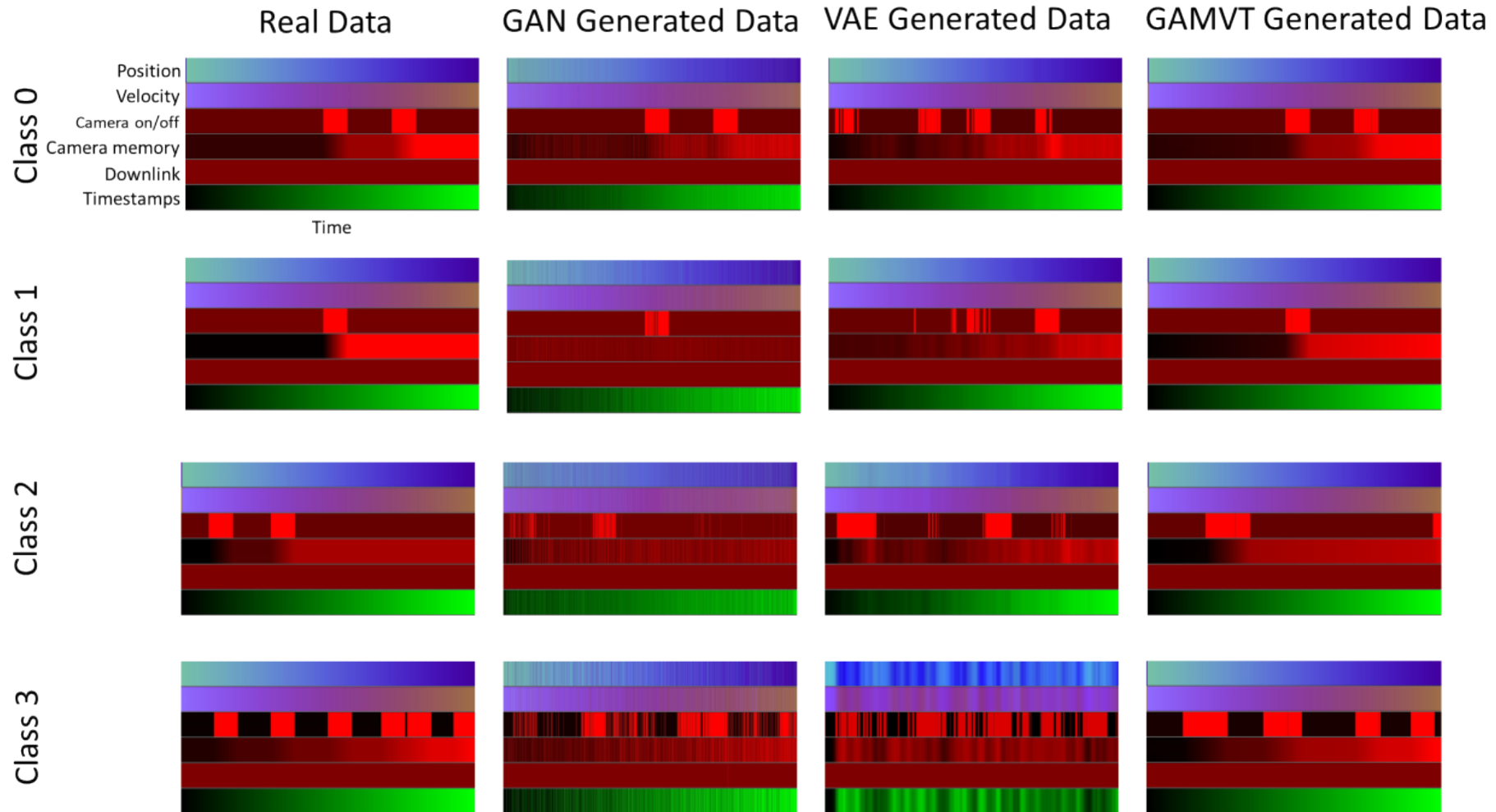
Qualitative Results



Qualitative Results



Qualitative Results



All algorithms produced reasonable data.
Some features were better captured by particular algorithms.

Quantitative Results



GAMVT generated data with best balance of both quality and diversity.



- Algorithm refinement
- Increase fidelity of the use case by gathering more real data, both for the attacks already considered as well as new attacks
- Evaluate algorithms on additional space systems platforms
- Evaluate benefit synthetic data contributes to the development of intrusion detection systems

Larger threat data sets are a necessary first step for many other cyber resilience technologies for space systems.

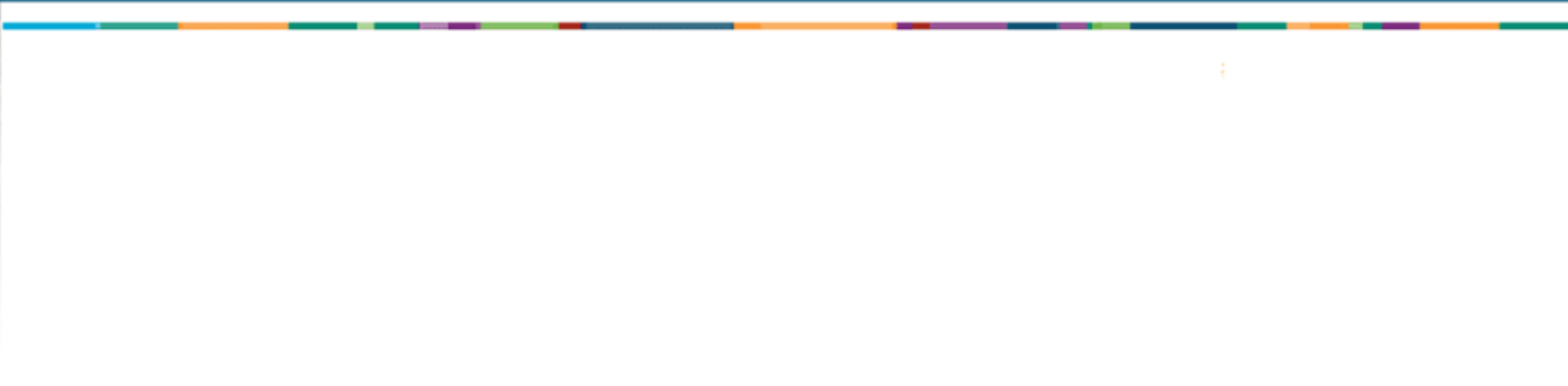


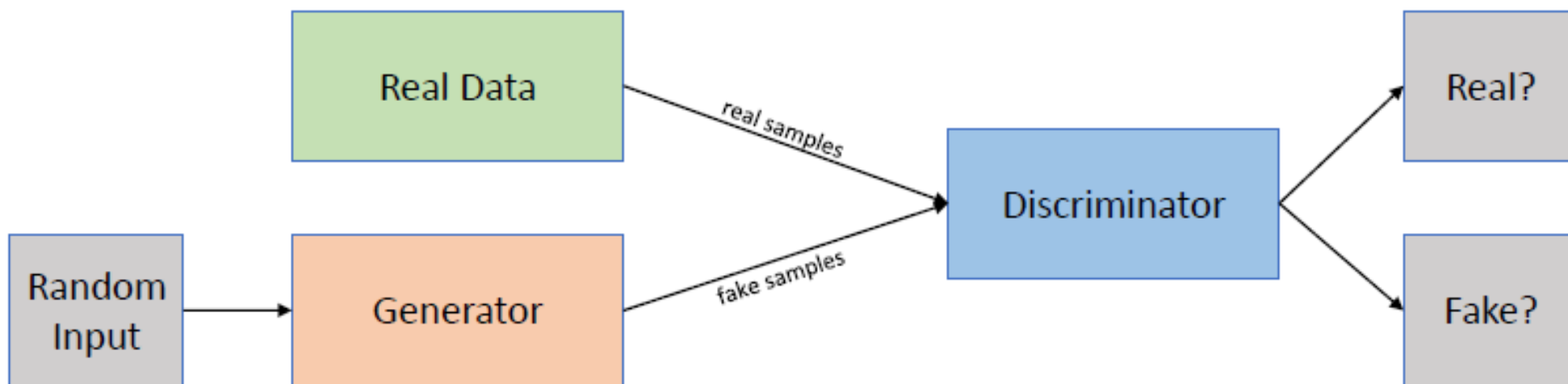
Questions

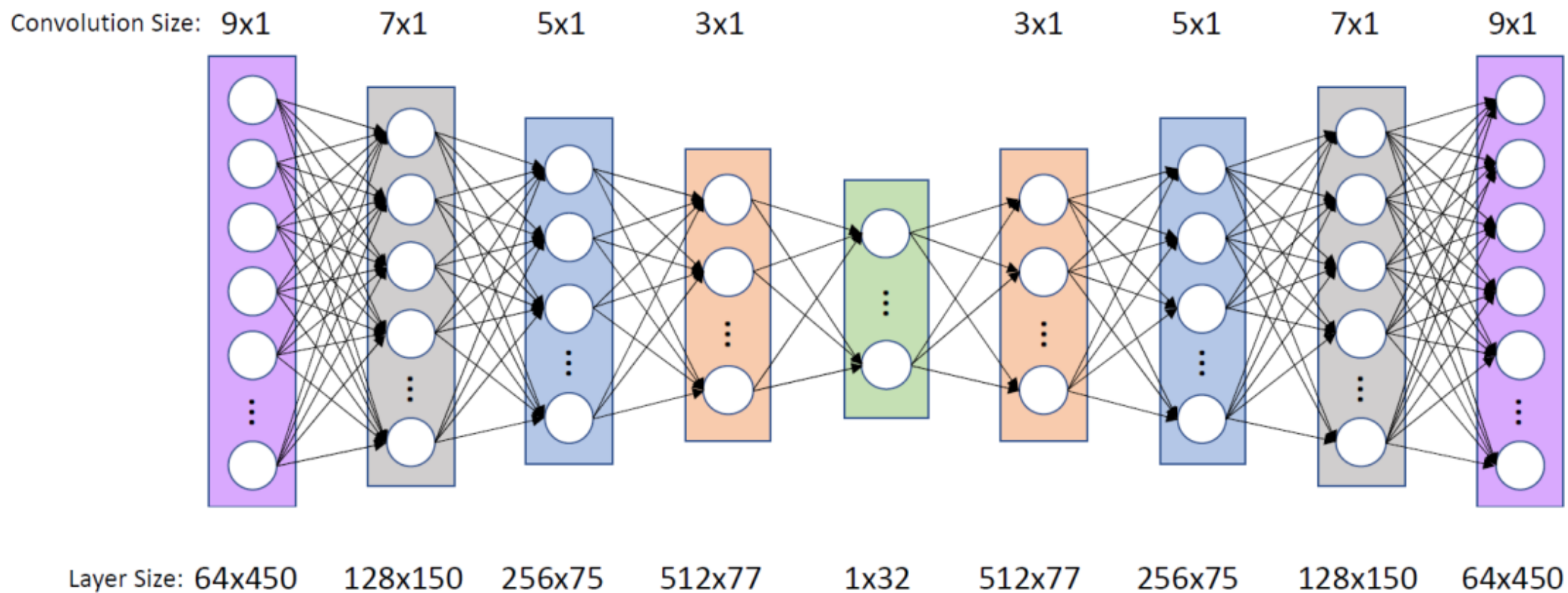




Backups









Distance Metric

$$d(x, y) = \sqrt{\sum_i \sum_j \left(\frac{x_{ij} - y_{ij}}{N_i} \right)^2}$$

Quality Metric

$$Q(T, G) = \frac{\text{Accuracy}(M(G))}{\text{Accuracy}(M(T))}$$

Diversity Metric

$$D_1(T_i, G_i) = \frac{\frac{1}{|G_i|} \sum_{x \in G_i} \min_{y \in T_i} d(x, y)}{\frac{1}{|T_i|} \sum_{x \in T_i} \min_{y \in G_i} d(x, y)}$$

$$D_2(T_i, G_i) = \frac{\frac{1}{|G_i|^2} \sum_{x \in G_i} \sum_{y \in G_i} d(x, y)}{\frac{1}{|T_i|^2} \sum_{x \in T_i} \sum_{y \in T_i} d(x, y)}$$

$$D(T, G) = \frac{1}{2|C|} \sum_{i \in C} D_1(T_i, G_i) + D_2(T_i, G_i)$$