Sandia National Laboratories | PURDUE UNIVERSITY | NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY | QoSient

Emulation Modeling for Testing Cyber Defense Capabilities for Joint Ground Station / Satellite Systems

Presenter: Robert G. Cole (Sandia)
Authors: R. Cole, J. Fustos, B. Hart, B. Hill, S. Wade (Sandia)
D. Cardona, A. Sabbaghi (Purdue)
A. Cooper (NC A&T State)
C. Bullard (QoSient)

A Presentation to the Workshop on Ground Station Architectures (GSAW) 2022

U.S. DEPARTMENT OF ENERGY | NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

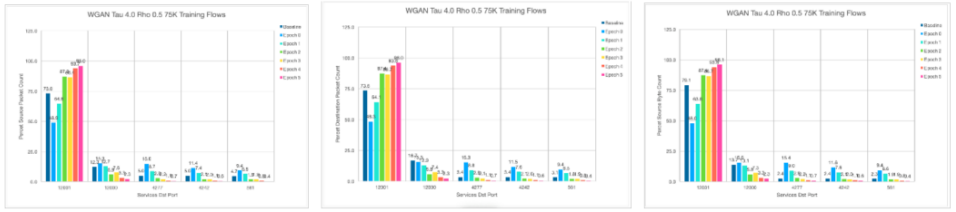
Sandia National Laboratories

Objective and Challenges

- **Objective** is to develop an emulation model of Ground Stations (GSs) and Satellites for the purpose of executing experiments on the impact of cyber attacks against these systems.
- **Challenges** include:
  - Training and testing Behavioral Analytics (BAs) and Machine Learning (ML) algorithms for cyber detection and defense requires large (really large) volumes of labeled data (benign or malicious) and
  - Large volumes of labeled data do not exist from deployed Ground Station/Satellite domains due to the sensitivity of data from space systems critical to National Security.

A Posited Solution – synthetically generated data sets

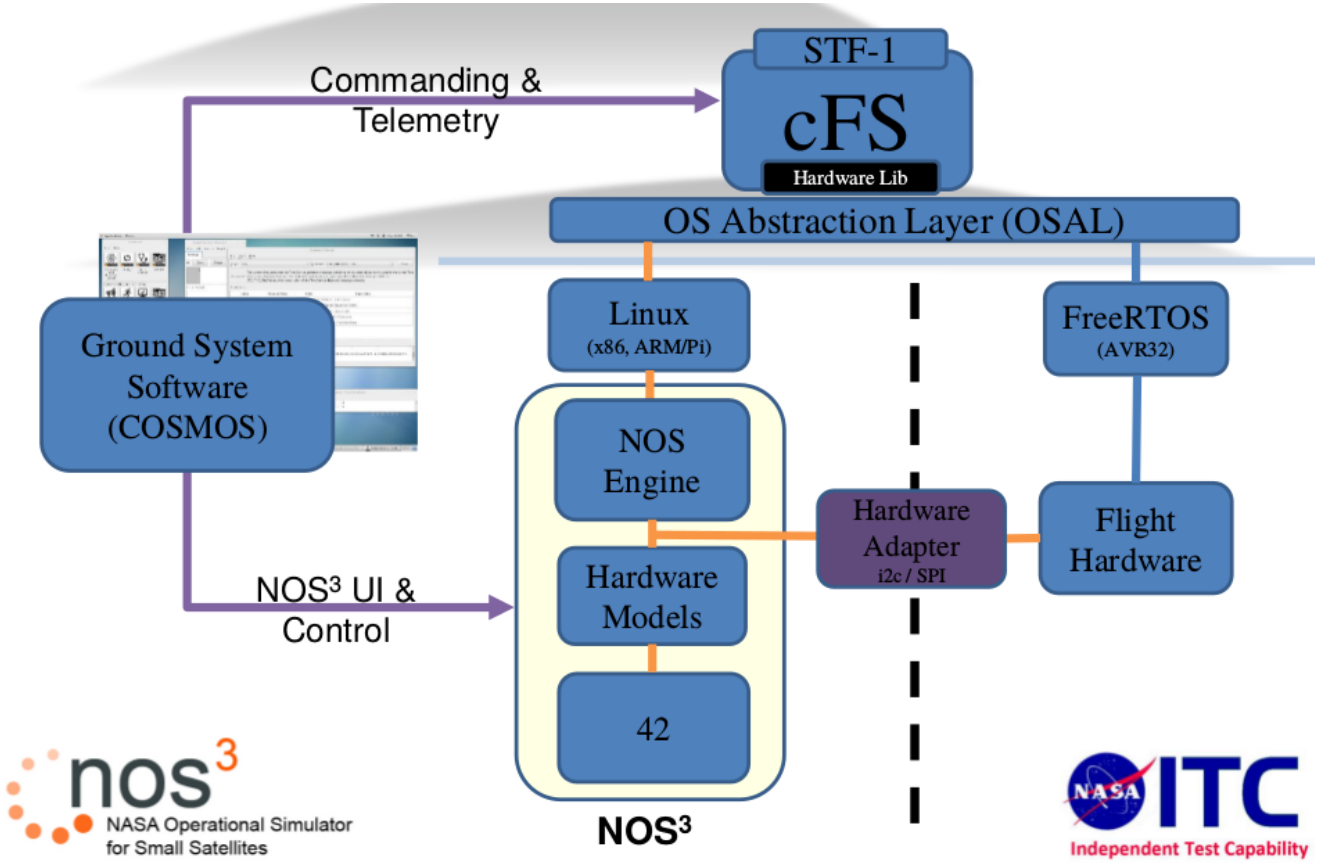
- Sandia has a long history in the application of simulation and emulation models of systems for cyber modeling and development.
- This expertise at Sandia has not previously been extended to the domain of GS and Satellite systems.
- The purpose of this project was to develop a joint GS/Satellite emulation system capable of generating large amounts of test data for training and testing of ML cyber defense algorithms.



- Our approach was to leverage NASA's open source Operational Simulator for Small Satellite (NOS3) system developed by the Katherine Johnson Independent Verification and Validation (IV&V) program in West Virginia [4].
- Then enhance the NOS3 code for Emulation modeling of representative missions, specifically,
  - Improved Data Collection,
  - HITL capabilities for higher fidelity cyber attack modeling against, e.g., serial buses and mission payload HW and SW and
  - Mission Planning SW based upon an 'archaeological' discovery of the Multispectral Thermal Imaging (MTI) systems Operational and Telemetry Logs.

NOS3

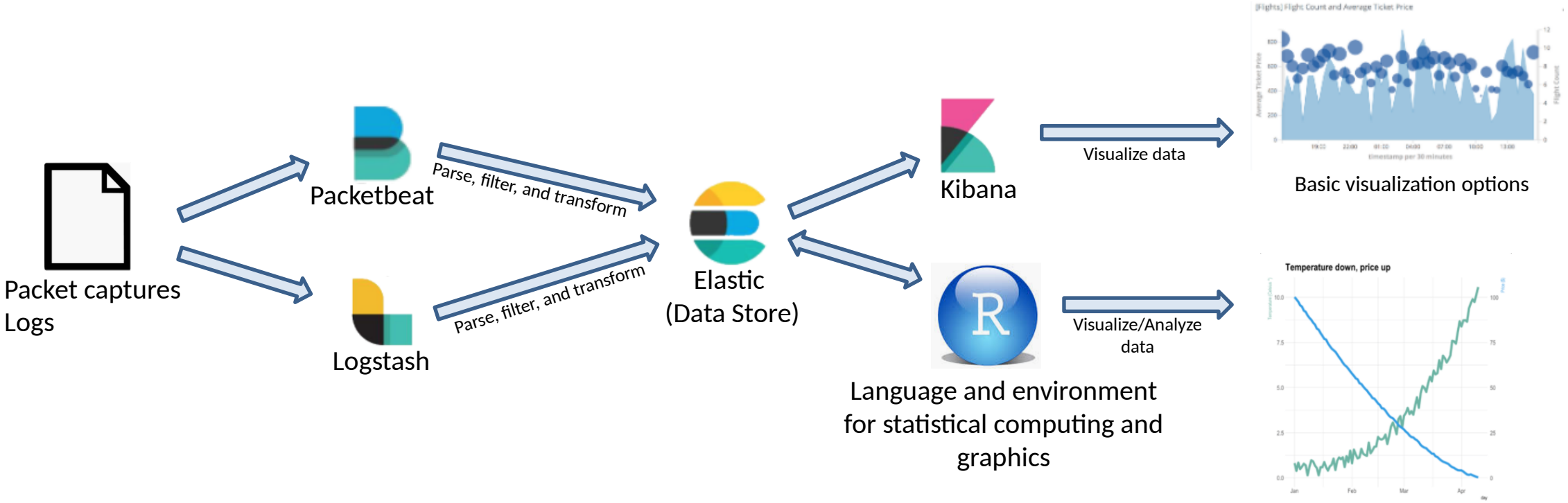
- We leveraged NASA's open source Operational Simulator for Small Satellite (NOS3) system.
- Significant capabilities include
  - Ball Aerospace's open source COSMOS GS software [5],
  - NASA-Glen's open source core Flight Software (cFS) [6],
  - The NOS Engine for serial BUS emulation modeling and
  - The open source physics modeling package 42 developed by NASA [7].



The system under study in our project is a joint model of the Ground Station mission execution platform and associated deployed satellite. Figure taken from Ref. [4].

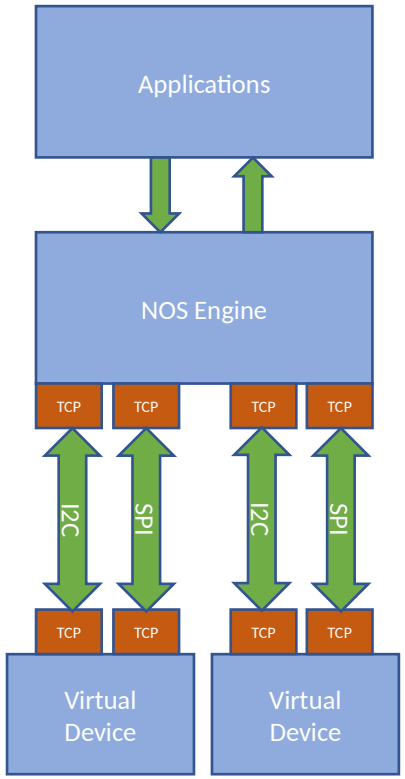
Enhanced Data Collection and Analysis

- We improved Data Collection including Serial Bus Interception for data collection and data manipulation, extensive Logstash scripts for ingesting data into Elasticsearch and GS-Satellite packet collection and flow characterization using the Argus toolkit from QoSient [8].

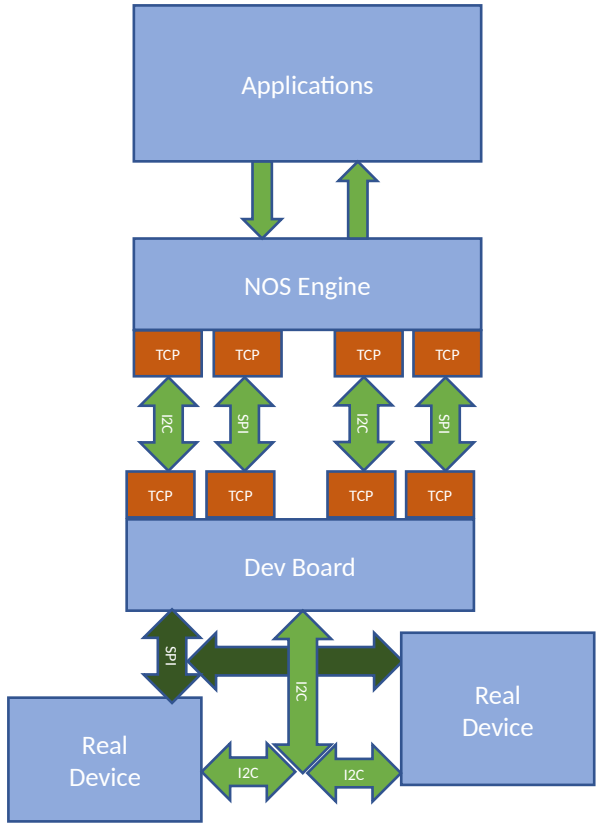


Hardware in the Loop

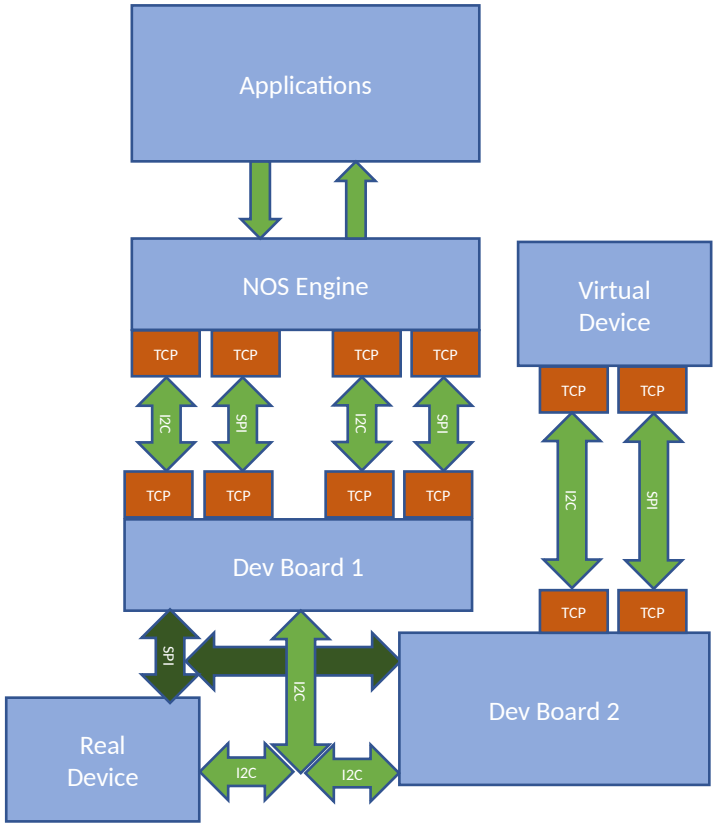
- We developed multiple HITL configurations for higher fidelity cyber attack modeling against, e.g., serial buses and mission payload HW and SW.



Current NOS3 design



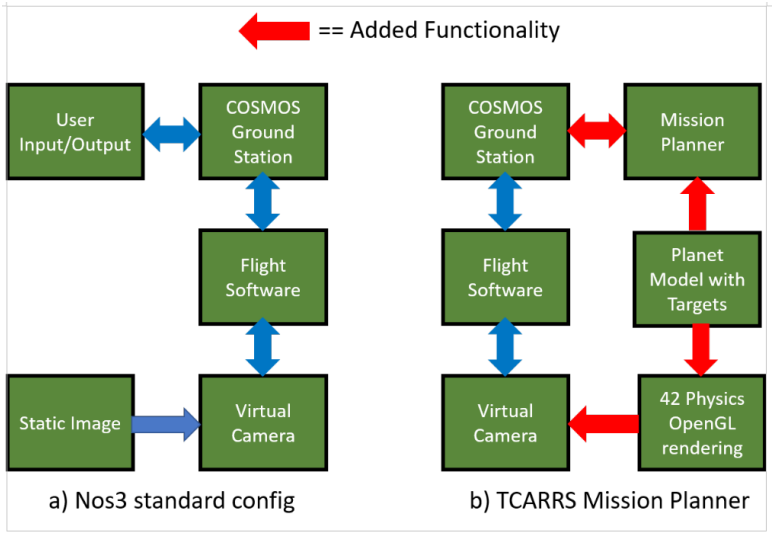
Supports real devices

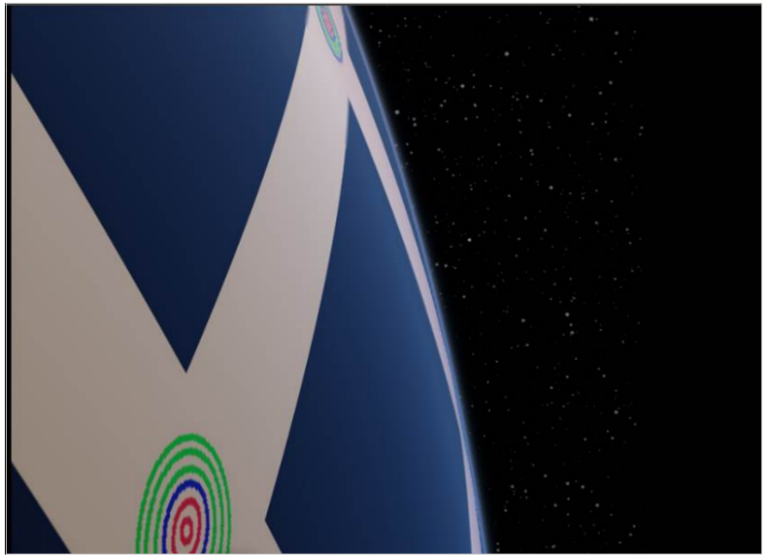


Dev Board 2 offers greater flexibility in bus attacks

Mission Planning System SW Development

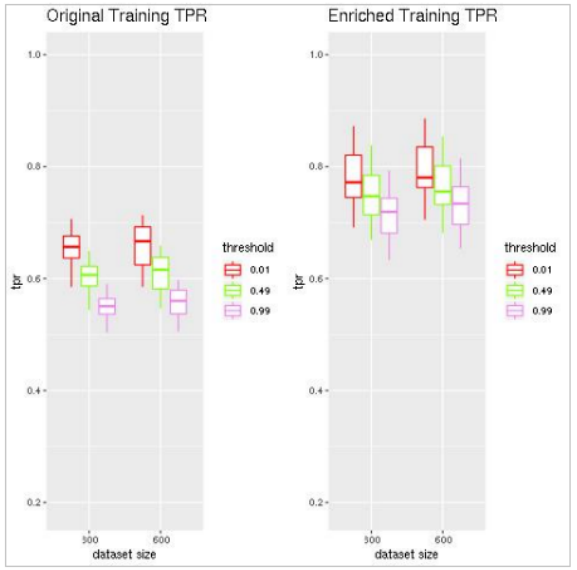
- Multispectral Thermal Imager (MTI) satellite [9] operated by Sandia and launched in 2000.
  - Archaeological discovery of the MTI satellite 'Operational' and 'Telemetry' data logs within Sandia's evolving organizational structure/organizations/staff.
  - Data parsing of Operator logs and decoding of Telemetry logs and data ingested into Elasticsearch.
  - Containerized for distribution to folks interested in future data analysis on this system.
- We developed a 'Mission Planner' software package, leveraging additional applications within the cFS system, to exercise NOS3 and allow for
  - Operationally relevant data collection and
  - Ability to verify imaging operations in the presence of potential malicious actors.



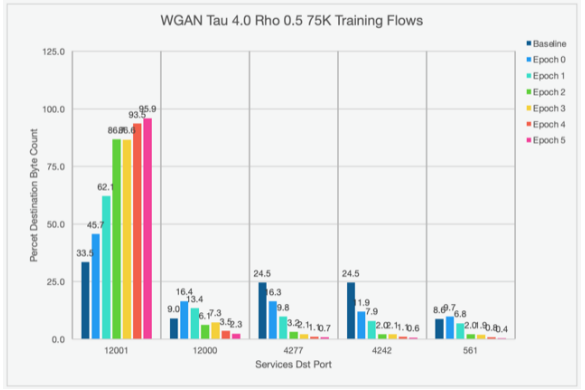


Synthetic Data Set Generation

- We ran a number of experiments to explore synthetic data set generation within the context of our GS/satellite emulation.
- With high fidelity emulation modeling it is difficult to generate large data sets for BA evaluation and ML training, e.g.,
  - Large variations in the GS/satellite models,
  - Varieties of mission payloads,
  - Variations in the environmental models and effects and
  - Variations in cyber-malicious attack modeling, …
- Still left with relatively sparse data sets for analysis, so we:
  - Started with proof-of-concept studies training classifiers on synthetic data sets generated via Extreme Learning Machines, then
  - Investigated synthetic data set generation via Generative Adversarial Networks (GANs) trained on our emulated GS/satellite data.



First studies generated synthetic digit datasets from the MINST [11] data.



Second studies generated synthetic packet flow record datasets from the GS to Satellite communications link in our emulation models.

An Initial Proof of Concept

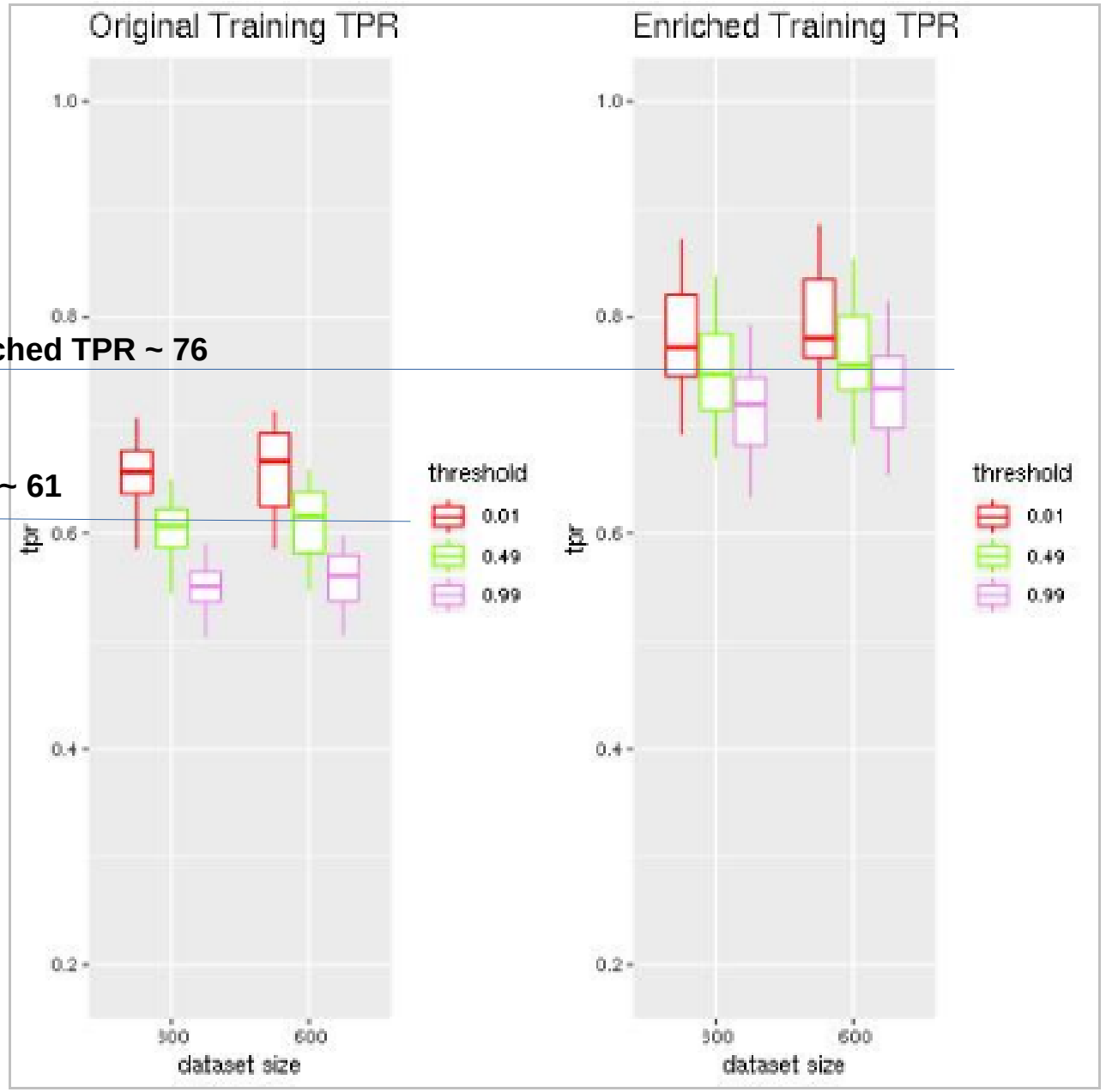
- We started with a Proof of Concept exercise based upon:
  - Using an Extreme Learning Machine (ELM) [10] for synthetic Data Set generation and
  - Training and testing a Logistic Regression classifier on the MINST digit data set [11].
- We looked at varying hyper-parameters on the ELM as well as varied:
  - Sparse data set size,
  - Classifier threshold values,
  - Scarcity of minority class and
  - Enrichment levels for the minority class.

The True Positive Rates (TPR) of the classifiers trained on the synthetically enriched data sets showed roughly a

100x(76-61)/61 = 25%

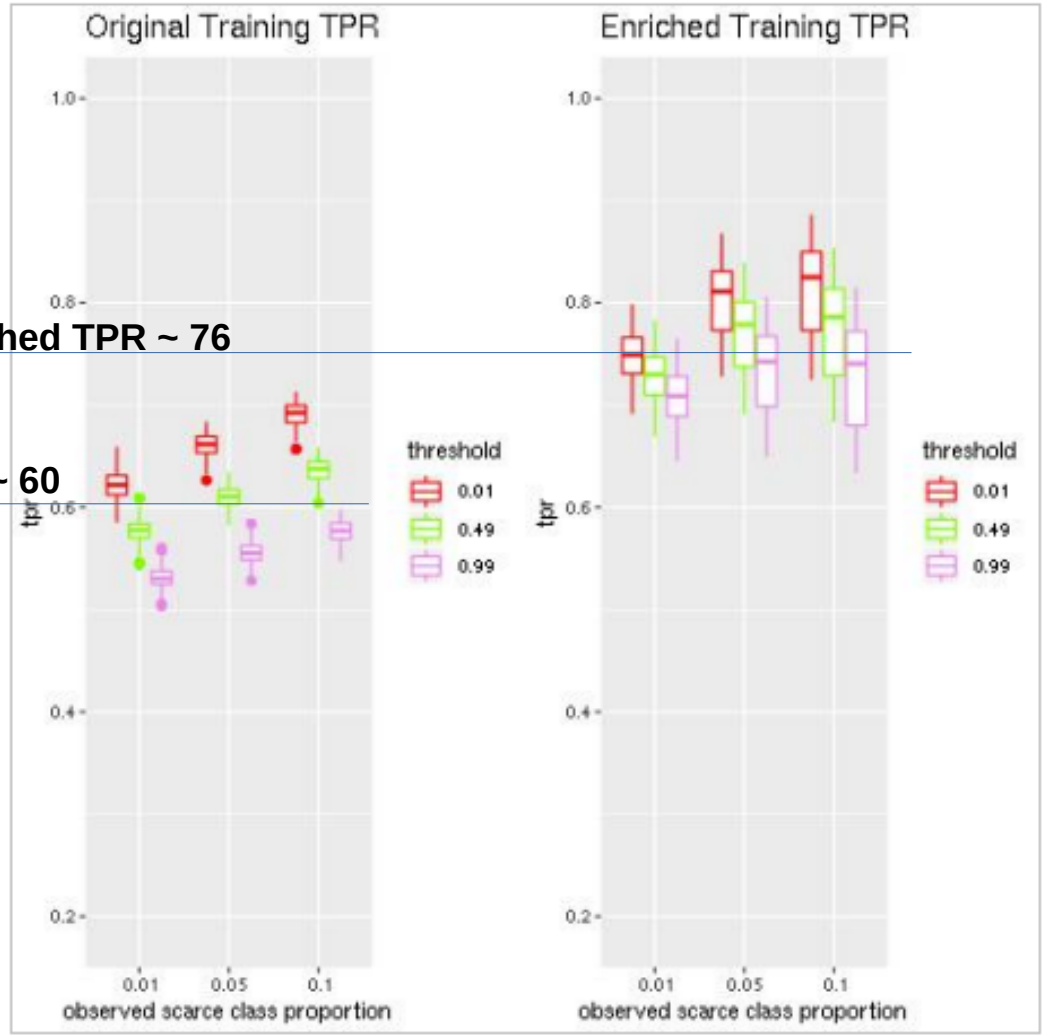
improvement in performance over those trained on the sparse data sets.

Impact of Data Set Size



ELM Proof of Concept – example results

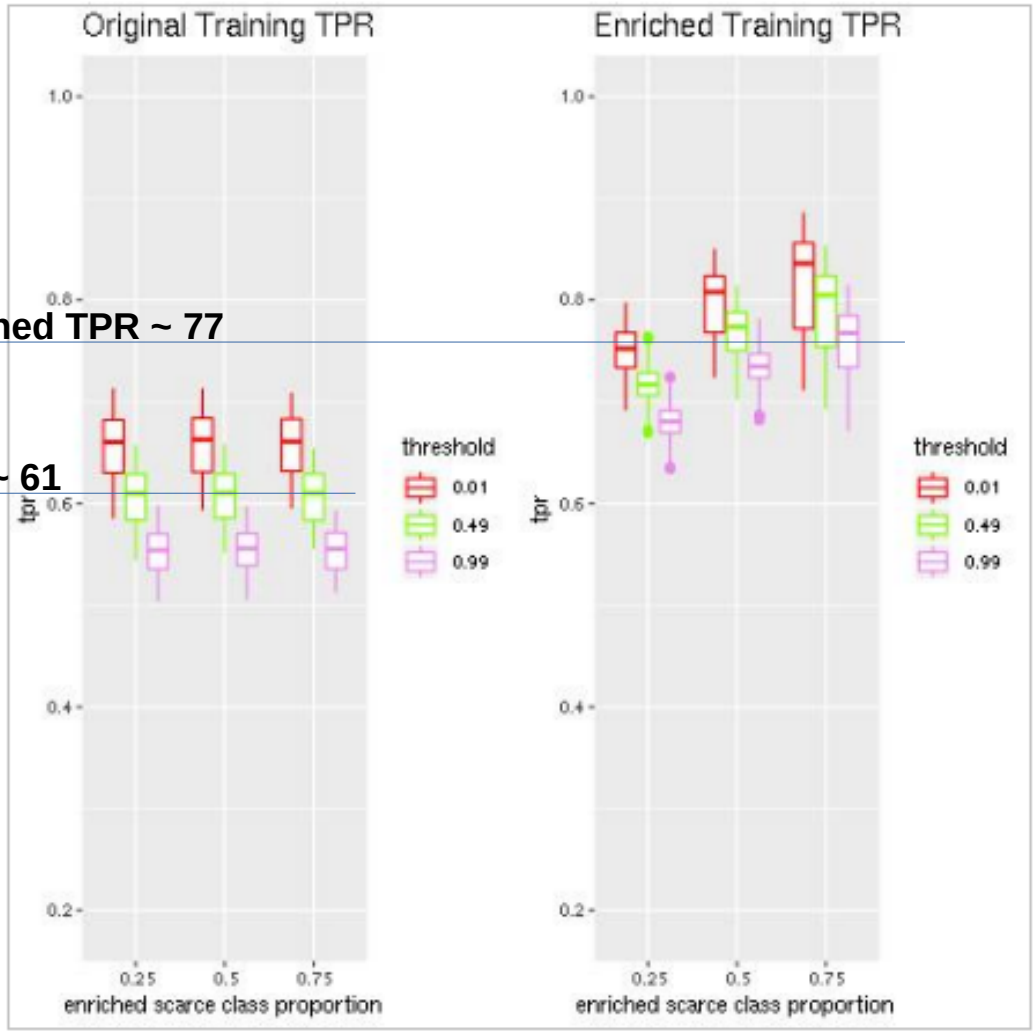
Impact of Minority Class Size



Enriched TPR ~ 76

TPR ~ 60

Impact of Minority Class Enrichment

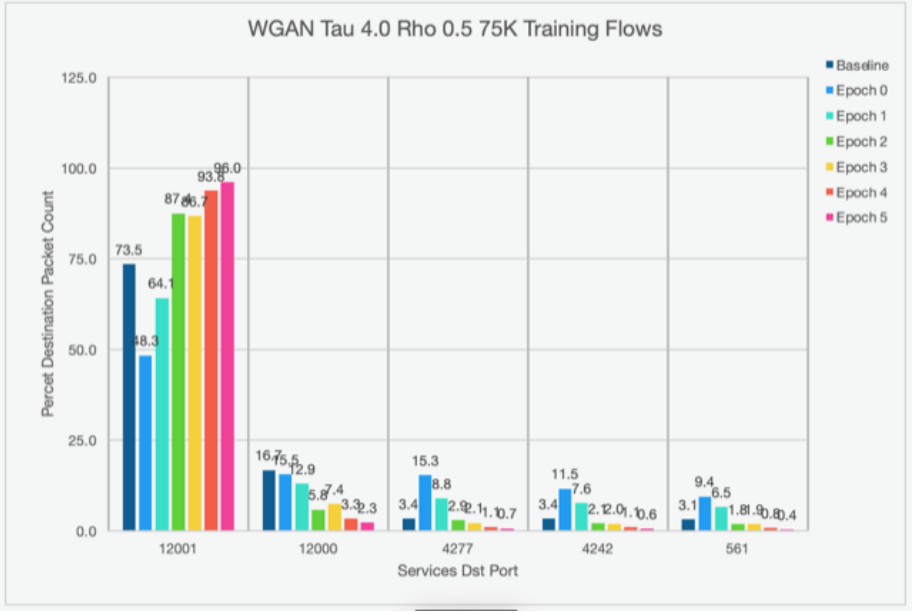


Enriched TPR ~ 77

TPR ~ 61

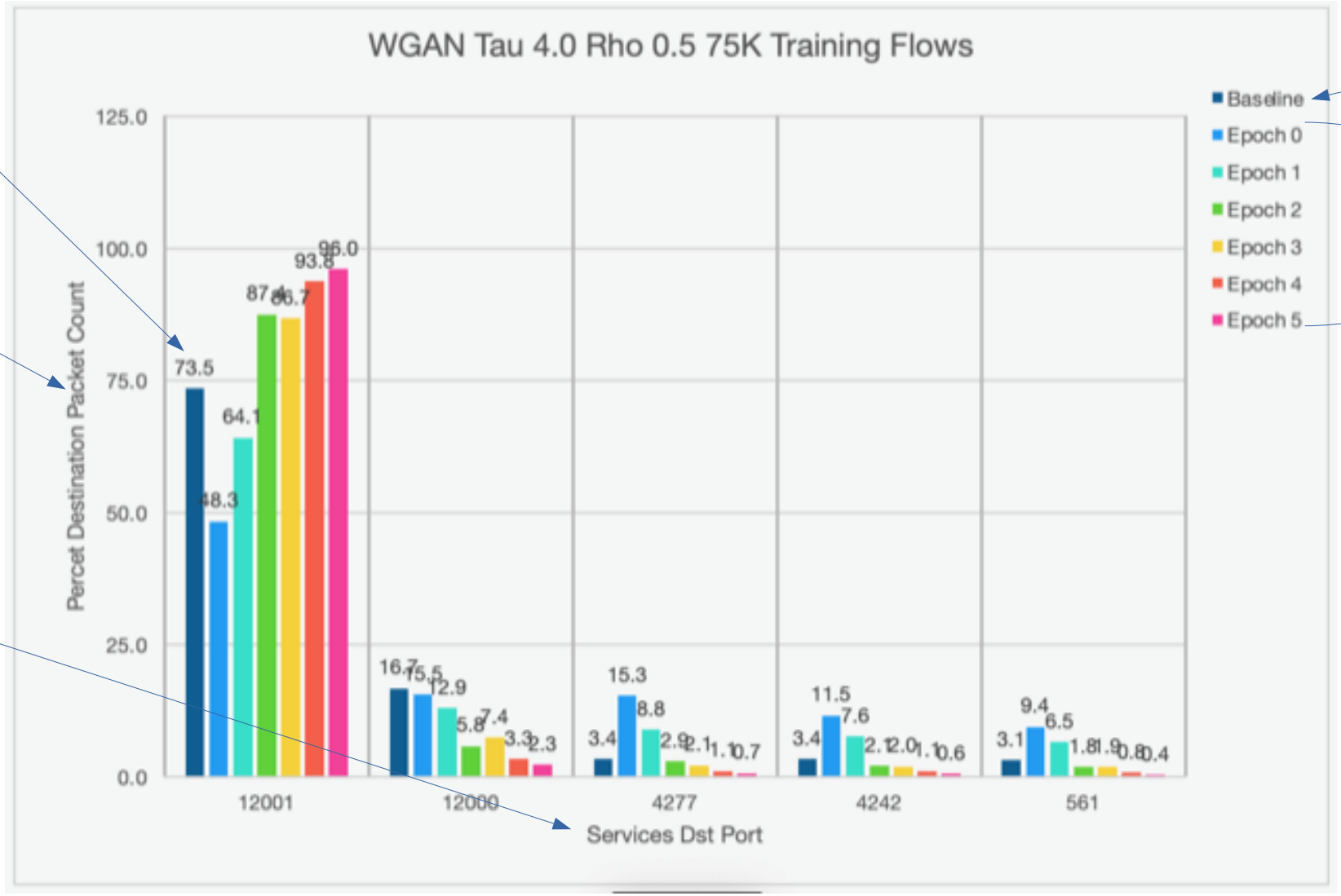
W-GANs on Emulated GS-to-Satellite Traffic Flow Records

- We installed the open-source Argus flow system [8] on the GS to satellite link within our NOS3 based emulation system.
- We collected metadata enhanced flow record, data sets while running our Mission Planner software on the emulation system (~ 1K flow records).
- We had to develop a set of ‘expert witnesses’ to discard nonsensical synthetic flows.
- We implemented and trained a Wasserstein GAN (WGAN) [12] on the aggregated flow record data sets from Argus.
- The resulting, trained WGAN was then used to generate synthetic flow record data which compared to the original collected records from the emulation model (see plots on the left and following slides).



(See Key on following slide)

W-GANs on GS/Satellite Emulated Data Sets - Key



Baseline

Dst Pkt Count

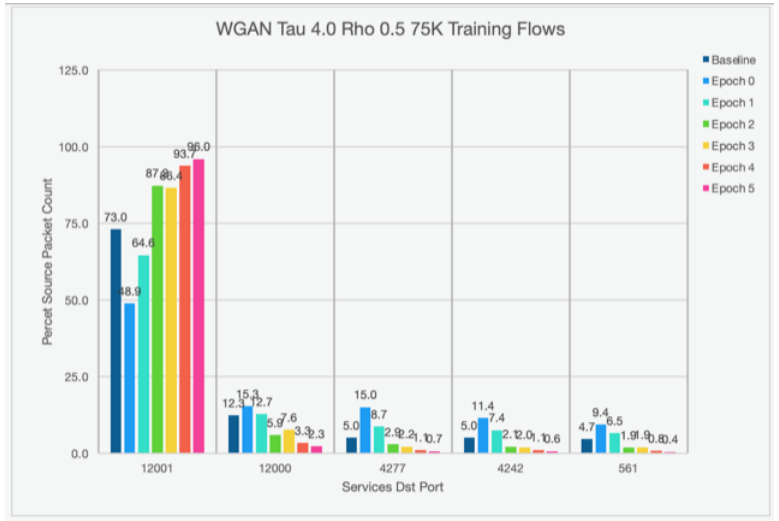
Dst Ports

Baseline

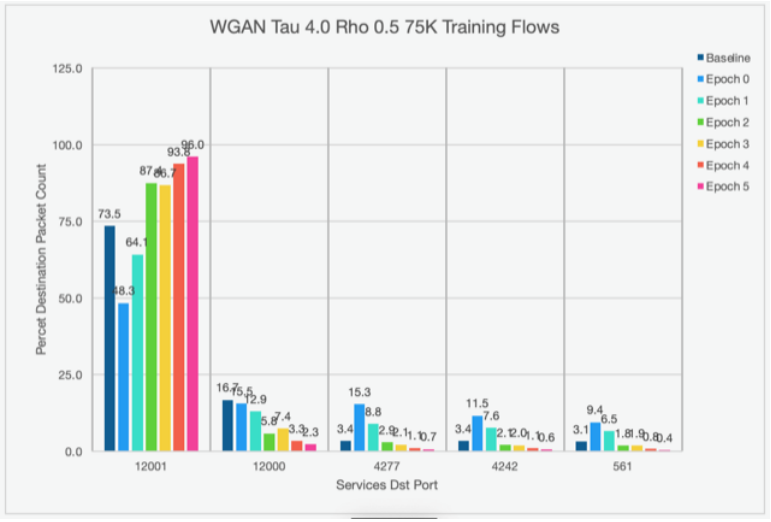
Data Generation Runs

W-GANs Generation on Emulated Flow Records

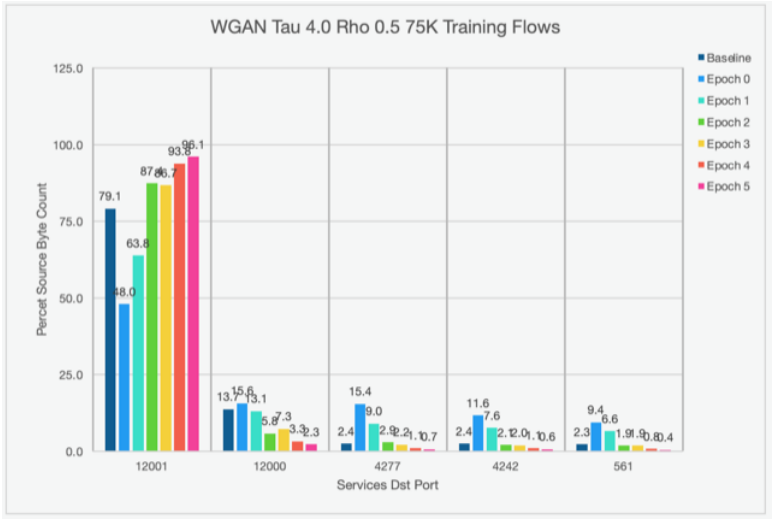
Src Pkt Count



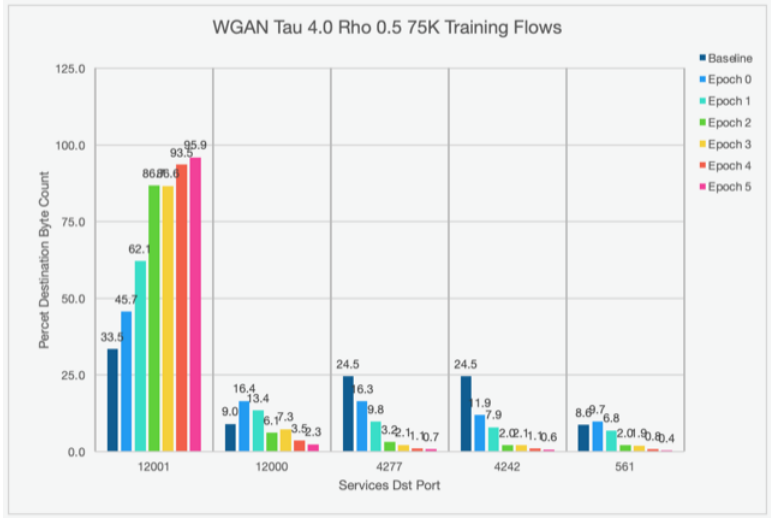
Dst Pkt Count



Src Byte Count



Dst Byte Count



Conclusions and Future Work

Conclusions

- We believe **there is a place for Emulation platforms** to help develop, test and train BAs and ML algorithms for cyber defense of GS/satellite systems, but much more work is necessary.
- We are **encouraged by our initial results on synthetic Generative Methods** for improved ML training.

Areas for future work include

- More work is required to **improve realism in our emulation tools** results through further mission development based on the analysis of the MTI (or other satellite) historical data.
- We **would like to see cyber experiments** performed to design, code and experiment with attacks against our satellite Emulytics™ platform in order to develop a better understanding of the utility of a satellite Emulytics™ tool for such future cyber studies.
- We believe **more studies of the Generative Methods are necessary.**
- It would be useful to perform extensive studies of **the notion** (and code developed as part of this study) **that a WGAN is a novel and sophisticated Anomaly Detection system** for traffic collection environments.

References

[1] Sandia National Laboratories, “minimega”, https://sandia.gov/emulytics/uur_minimega-fact-sheet.pdf/.

[2] Sandia National Laboratories, “Firewheel”, https://sandia.gov/emulytics/uur_firewheel-fact-sheet.pdf/.

[3] Sandia National Laboratories, “SCEPTRE”, https://osti.gov/servelets/purl/1376989/.

[4] Matt Grubb. “The NASA Operational Simulator for Small Satellites (NOS3)”, https://github.com/nasa/nos3/, 2021.

[5] Ball Aerospace, “COSMOS Ground Station Software”, https://cosmosc2.com/

[6] National Aeronautics and Space Administration, “NASA core Flight Software (cFS)”, https://github.com/nasa/cFS

[7] National Aeronautics and Space Administration, “The NASA 42 simulator”, https://sourceforge.net/projects/fortytwospacecraftsimulation/, 2021.

[8] QoSient, “Argus Packet Flow Collection”, https://openargus.org/.

[9] “MTI Satellite”, https://earth.esa.in/web/eoportal/satellite-missions/m/mti/.

[10] Guang-Bin Huang, Lei Chen, Chee Kheong Siew, et al. Universal approximation using incremental constructive feedforward networks with random hidden nodes. IEEE Trans. Neural Networks, 17(4):879–892, 2006.

[11] Yann LeCun and Corinna Cortes. MNIST handwritten digit database, 2010.

[12] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In International conference on machine learning, pages 214–223. PMLR, 2017.

Acknowledgments

We wish to acknowledge Matt Grubb, a developer of the NASA Open Source Operational Simulator for Small Satellite (NOS3) system, for his extreme patience with our questions, for sharing code with us and for his development of wonderful, remote training during our time of need. Thanks Matt.