Unclassified Unlimited Release

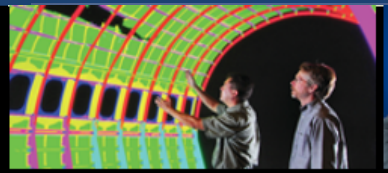
SAND2020-11255PE

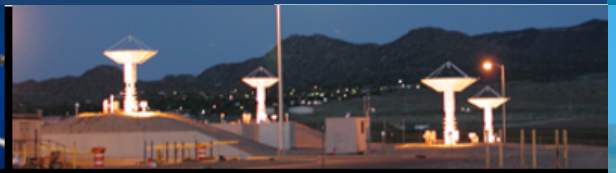
DEPARTMENT OF STATISTICS
PURDUE UNIVERSITY

Sandia National Laboratories

STARCS

Towards Cognitive Analytics for Resilient Satellite Systems (TCARSS)





Presenter: Robert G. Cole, Ph.D.

Organization: Sandia National Laboratories

Address: Albuquerque, New Mexico

Academic Alliance Partners: Profs. Arman Sabbaghi and William Cleveland, Dept. of Statistics, Purdue University

LDRD LABORATORY RESEARCH & DE

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.

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.

Robert G. Cole, SNL

Abstract:

Cyber security R&D at Sandia National Laboratories (SNL) has made extensive use over the years of emulation models of Internet Technologies (IT) and Operational Technologies (OT) to develop, test and train cyber detection and mitigation technologies [1]. Exemplar emulation systems at SNL include MiniMega [2], Firewheel [3] and SCEPTRE [4].

The TCARSS (Towards Cognitive Analytics for Resilient Satellite Systems) program is leveraging this experience for the development of a satellite environment emulation system. The main purposes of the TCARSS Emulation platform are a) develop a capability to generate large datasets for training, testing and validating cyber Machine Learning (ML) algorithms in a representative satellite environment and b) to provide a platform for testing the effectiveness of cyber protection and mitigation techniques in a satellite environment. We are developing this initial capability starting with the NASA developed open source simulation platform called NOS3 [5].

To achieve our main objectives, our major challenge areas are:

- **Adding realism into the operational behaviors of the emulated systems.**
- **Adding fidelity to the platform to better emulate cyber effects.**
- **Generating synthetic data to enrich sparse datasets collected off the emulation platform in order to build large datasets for ML training, testing and validation.**
- **Addressing platform use-ability issues by developing common data formats and access interfaces for all data collection using Elastic [7].**

Robert G. Cole, SNL

Project Overview

- *This project address the Cyber Threat*
- *Cyber resilience is most effective when the Attack is detected and a corrective response is taken*
- *Key challenges to attack detection and mitigation in satellite systems is limited sensing analytics for cyber threat and a sparsity of data to train sensing analytics*

R&D Goals & Milestones

- *Tool selection – 9/1/19*
- *System realism (operations) – 4/1/21*
- *System realism (HITL) – 9/1/20*
- *Attack Modeling – 6/1/21*
- *Generative methods – 5/1/21*
- *Demonstration – 9/1/21*

Risks – achieving the necessary level of realism in the emulated systems

Technical Approach

- *Leverage Emulytics(TM) capabilities and expertise to develop a satellite emulation platform and synthetic data generation techniques that can be used to create training and validation data sets for anomaly detection algorithms*

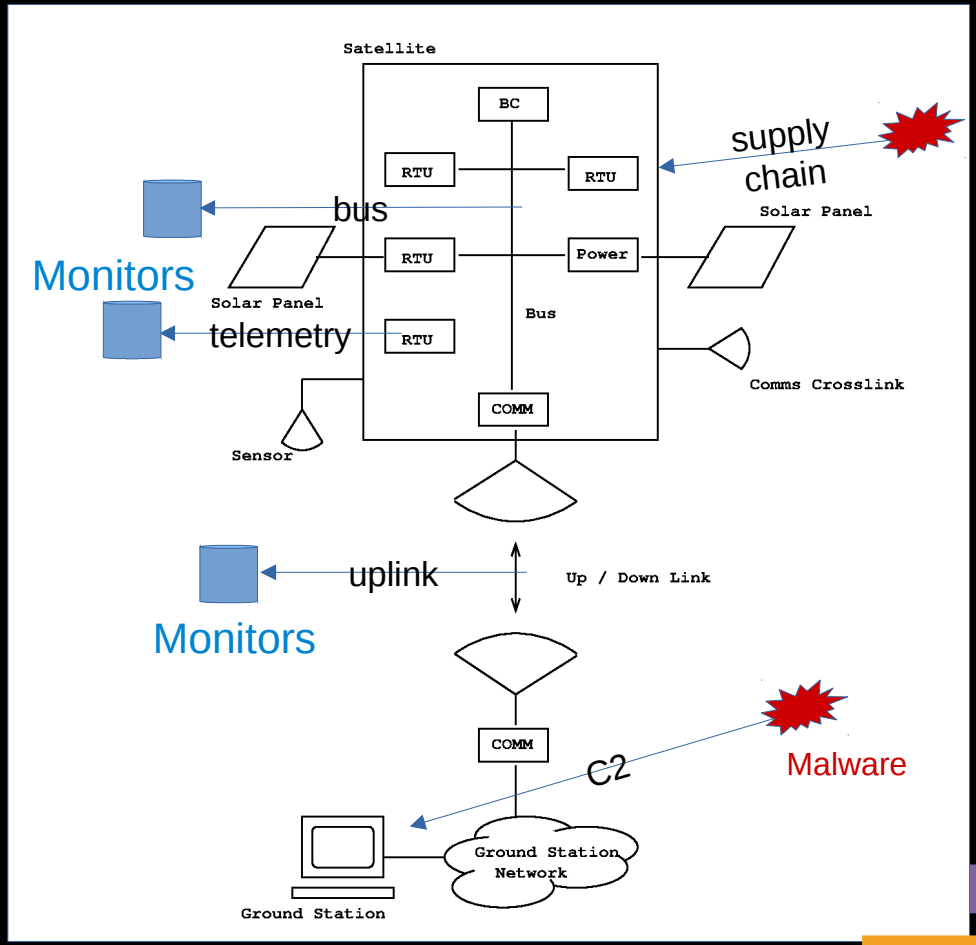
Significance of Results

- *Platform will enable data collection and testing environment for training and evaluation*
- *Expand synthetic data sets via generative methods*
- *Demonstrate improvement in performance of classifier trained on larger and larger synthetic data set*

TCARSS may provide the foundational capability and data for rigorous development, training and testing of cognitive analytics methods

Robert G. Cole, SNL

- **NOS3 enhancements** for improved d**ata collection and modeling realism**
  - telemetry and C2 Monitors (TCP traffic, host logs, serial bus)
  - additional mission payloads
  - navigational tracking
  - intermittent Communications (navigational tracking)
  - scripted C2 from GS to satellite
  - separation of GS and Satellite for packet capture
- **Building a rack-based HITL** capability
  - initially a branched development, to be merged later
- **Integration of all TCARSS data collection into ELK**
  - common repository of all data collection, integration into Python and R analysis packages, data visualization through Kibana
- **Multi-Thermal Imagining (MTI) data analysis**
  - extensive, multi-year logs from SNL satellite system
- **Generative methods and statistical analysis**
  - class of neural networks named Extreme Learning Machines
- **Documentation and training for SNL users**
  - user manuals to encourage use
  - encourage user contributions
- **Exemplar malware models,** using, e.g.,
  - bus interceptor and payload manipulation
  - serial bus attacks
- **Demonstration**
  - Testing the project hypothesis



Robert G. Cole, SNL

Accomplishments highlights

- *Built Partnering Relationships with NASA and Purdue University*
  - *With NASA to expand the capabilities of the emulation platform*
  - *With Purdue to investigate statistical and machine learning methods for synthetic data set generations*
- *Expanded the data collection capabilities of the emulation platform*
  - *Developed serial bus interceptor code for all mission payloads*
  - *Integration of traffic capture and log file information into Elasticsearch*
- *Adding HITL capabilities for improved cyber-attack response (i.e., two platform configurations, a) VM based and b) FlatSat based)*
- *Leveraging MTI data analysis to build realism into the Emulytic(TM) Platform*

Robert G. Cole, SNL

References:

1) *https://www.elastic.co/https://www.sandia.gov/emulytics/*
2) *https://www.sandia.gov/emulytics/_assets/documents/uur_minimega-fact-sheet.pdf*
3) *https://www.sandia.gov/emulytics/_assets/documents/uur_firewheel-fact-sheet.pdf*
4) *https://www.osti.gov/servlets/purl/1376989*
5) *https://github.com/nasa/nos3*
6) *https://www.sciencedirect.com/science/article/pii/S0925231206000385*
7) *https://www.elastic.co/*

Questions, comments ?

Thanks,

Robert G. Cole, Ph.D.
SNL
rcole@sandia.gov