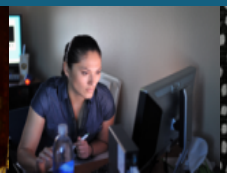
SAND2020-11279PE

Sandia National Laboratories

Moving Target Defense for Space Systems



Project Team: Chris Jenkins, Eric Vugrin, Indu Manickum, Nicholas Troutman, Jacob Hazelbaker, Matthew Napier

Project Manager: Drew Woodbury

STARCS Thrust Area: Threat-defended Hardware

October 15, 2020

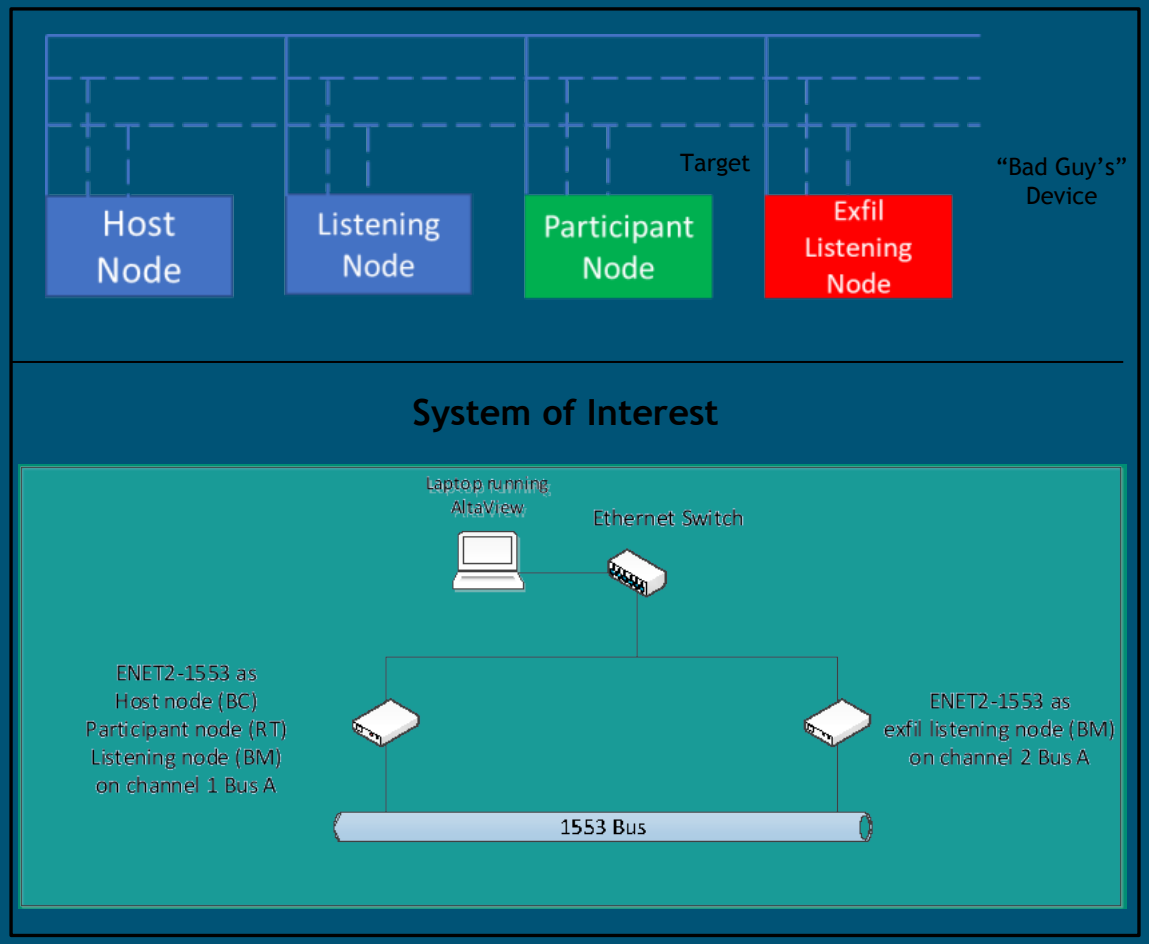
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

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

Project Overview

- Goal: improve cyber resilience of space systems to cyber-attacks
- Project outcome: proof-of-concept moving target defense hardware implementation and demonstration of efficacy against various attacks
- Key Idea: create an “orchestrated chaotic environment” that confuses attacker and enables platform to continue operations
- Technical Approach: dynamically & randomly change node addresses, confusing attacker
- Apply to MIL-STD-1553 protocol
- Experiments measure efficacy against various cyber attacks (exfil, data injection)
- Demonstrate and quantify benefit of MTD
- Demonstrate feasibility for ML trained model to make predictions in real-time

Resilience Expt.: Exfiltration Attack Scenario



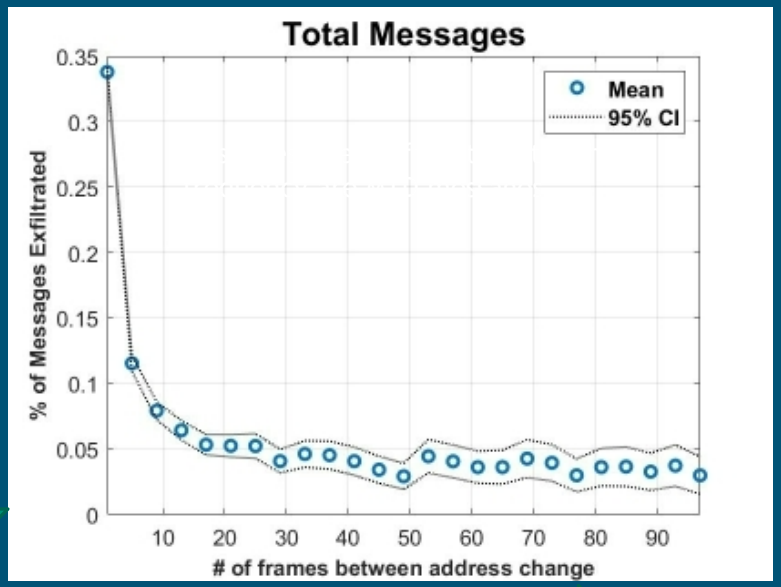
Set Up

- Attacker has corrupted an node to be an exfil listening node (red)
- Messages to/from target participant node (green) = messages of value to the attacker
- Exfil listening node monitors & exfils all messages to/from target
- With no MTD, exfil listening node will see and exfil 100% of messages to/from target

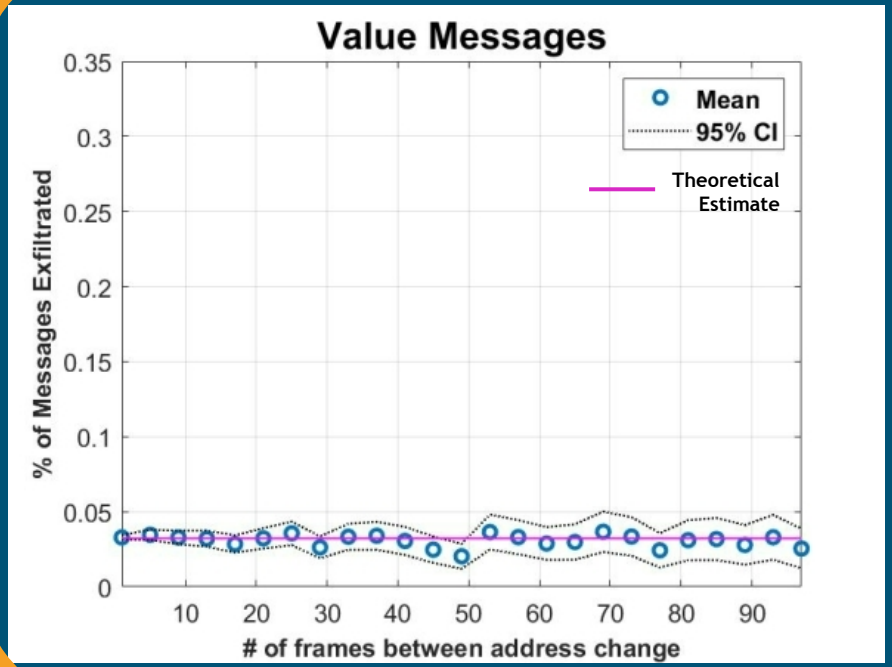
Question: does the implementation of MTD reduce the fraction of "messages of value" that are exfiltrated?

Exfil Experiment Results

Resilience Increases



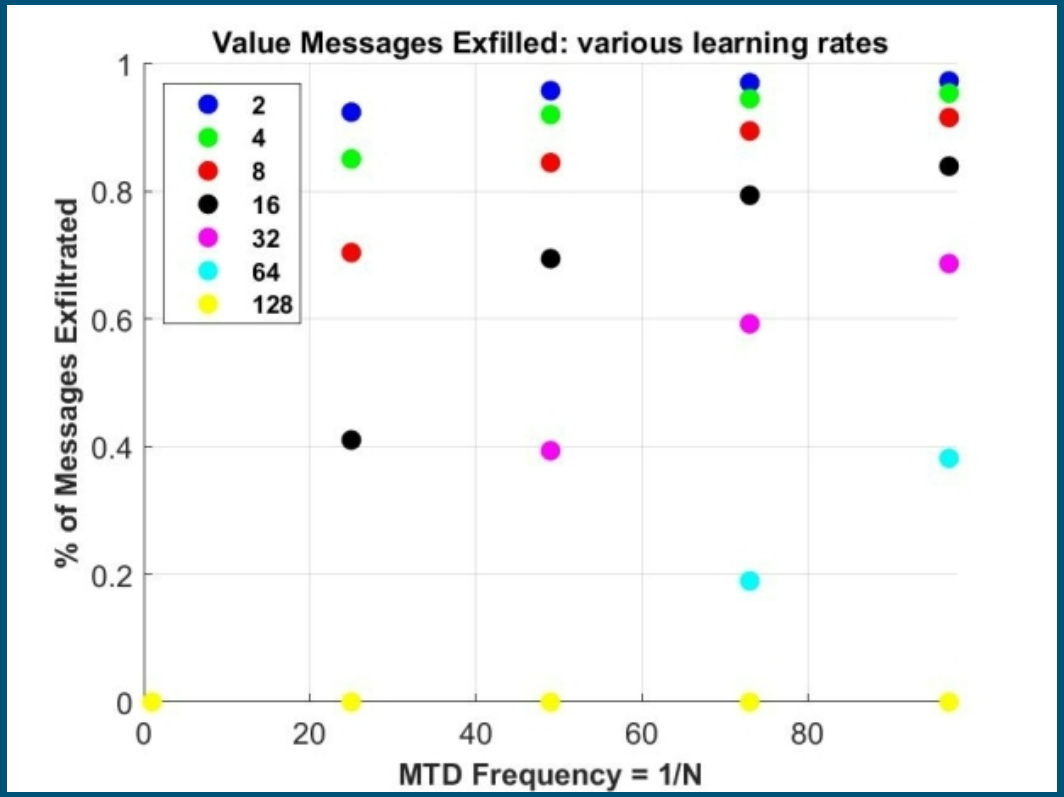
Frequency Decreases



In this scenario

- MTD reduces % of value messages exfiltrated by ~97%
- Experimental results match theoretical estimates
- We can quantify how well MTD increases resilience

Exfil Experiment Results: Learning Adversary



1000 Fibonacci Generations, 25 trials

Assume adversary learns new address after X frames

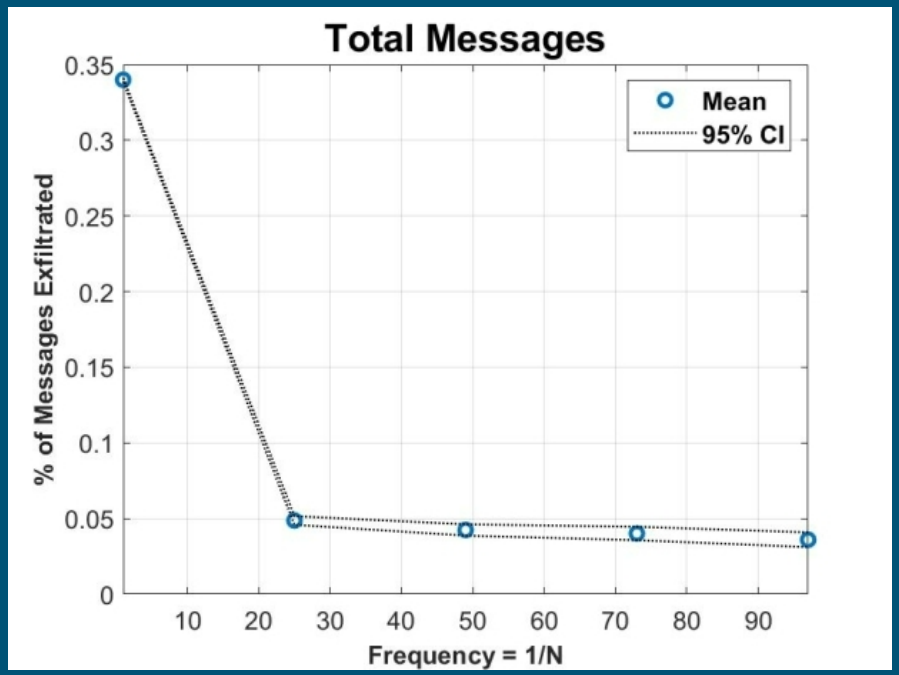
Example:

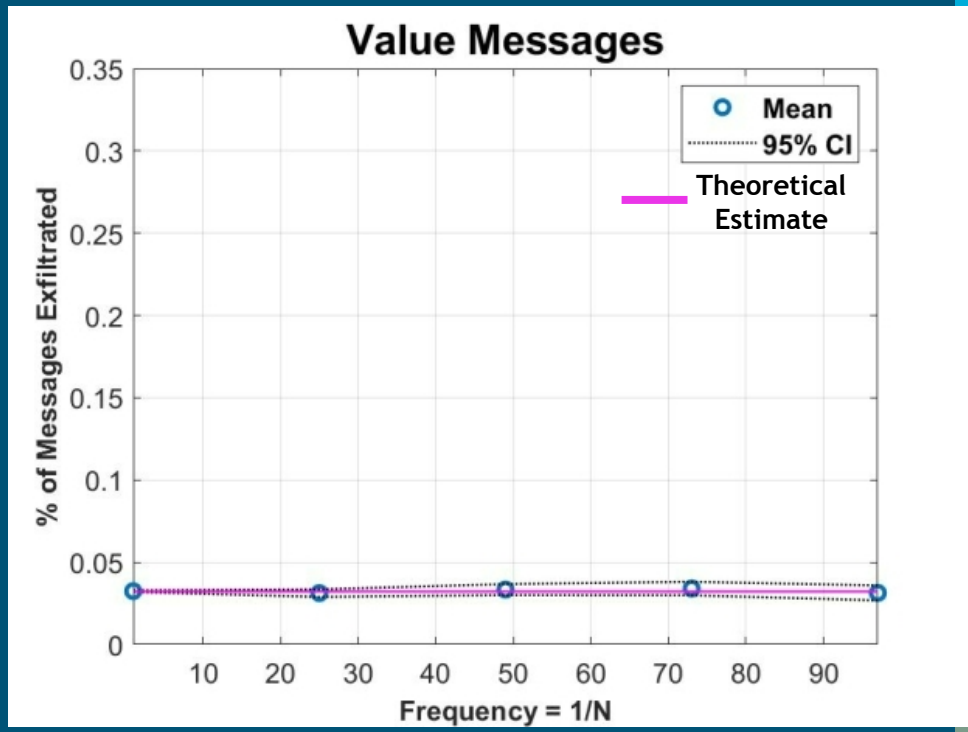
- Freq = 25, learned = 8 frames, exfil = 70%
- Freq = 25, learned = 16 frames, exfil = 40%
- Freq = 25, learned = 32, exfil = 0%

Takeaways:

- Against a learning adversary, MTD frequency needs to be faster than adversary learning rate to significantly mitigate exfil attacks
- These data can start informing design requirements

Exfil Experiment Results:
1000 Fibonacci Generations, 25 trials, Random Static Adversary



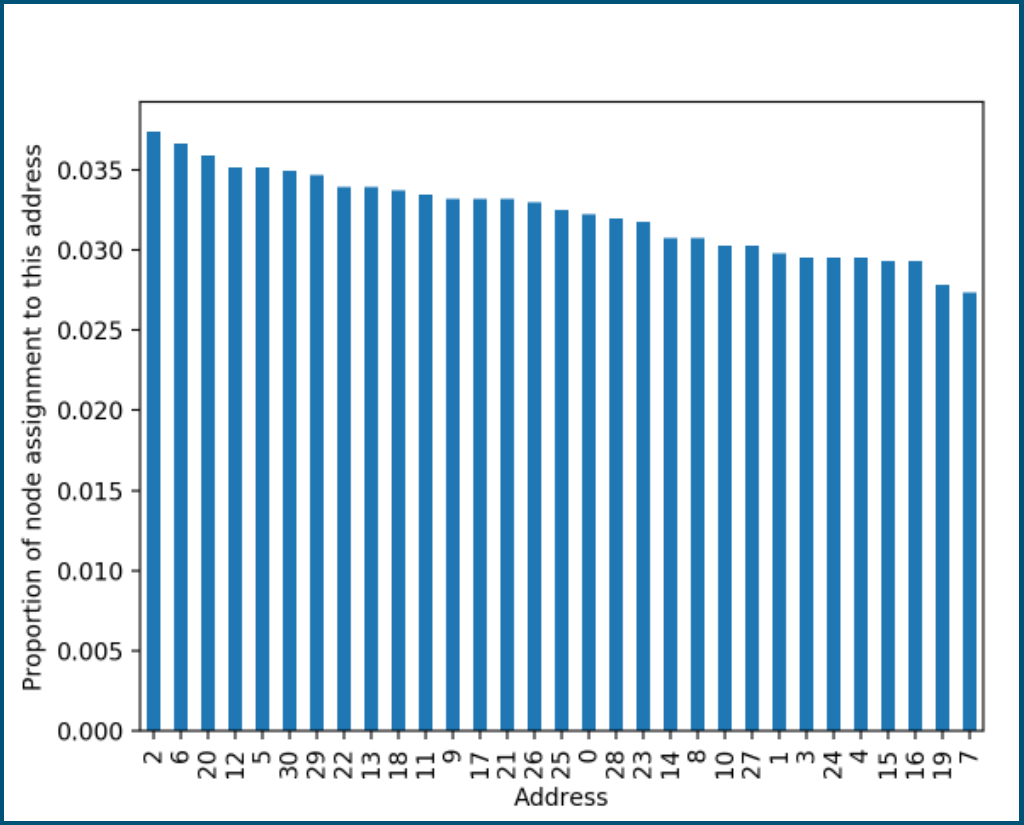


Randomness Evaluation of MTD Architecture

Metrics used:

- Entropy – Quantifies the ability of adversary to randomly guess the device's next address based on the frequency with which that particular address has previously been used.
- Lempel Ziv – Quantifies compressibility of address assignment sequence. This relates to how often patterns repeat in the sequence.

Input: time series of what address a node on the bus was assigned to at each frame



Preliminary findings

- Frequency of addresses is not perfectly uniform, leaving some area for improvement (entropy is 0.62 vs maximum score of 1 for perfectly uniform distribution)
- More frequent address updates increases Lempel-Ziv scores, indicating greater challenge to adversaries

Randomness Evaluation of MTD Architecture