



**Calhoun: The NPS Institutional Archive**  
**DSpace Repository**

---

Faculty and Researchers

Faculty and Researchers' Publications

---

2019-12

# Cyber System Assurance through Improved Network Anomaly Modeling and Detection

Bollmann, Chad A.

Monterey, California: Naval Postgraduate School

---

<http://hdl.handle.net/10945/69942>

---

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

*Downloaded from NPS Archive: Calhoun*



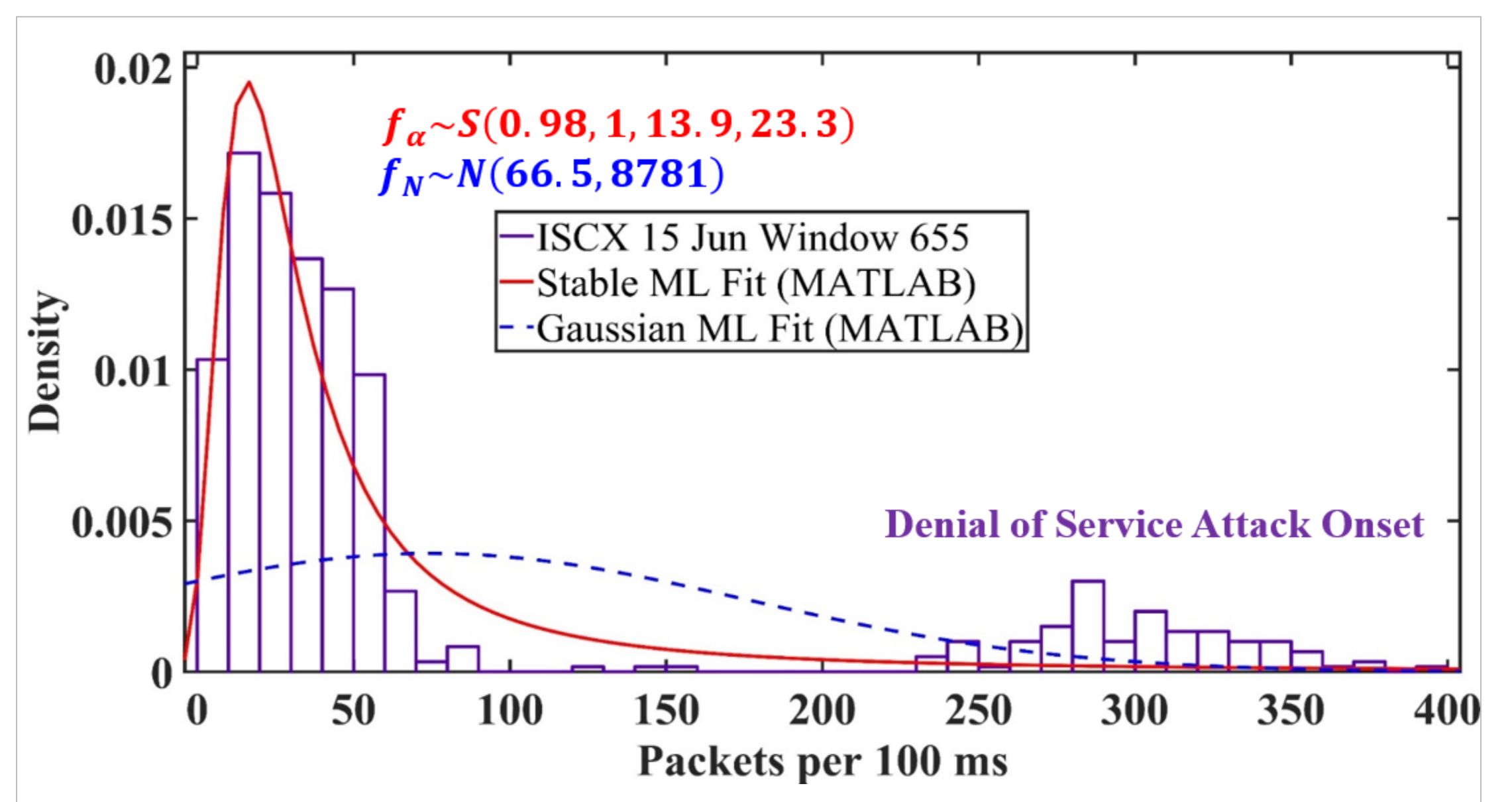
Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

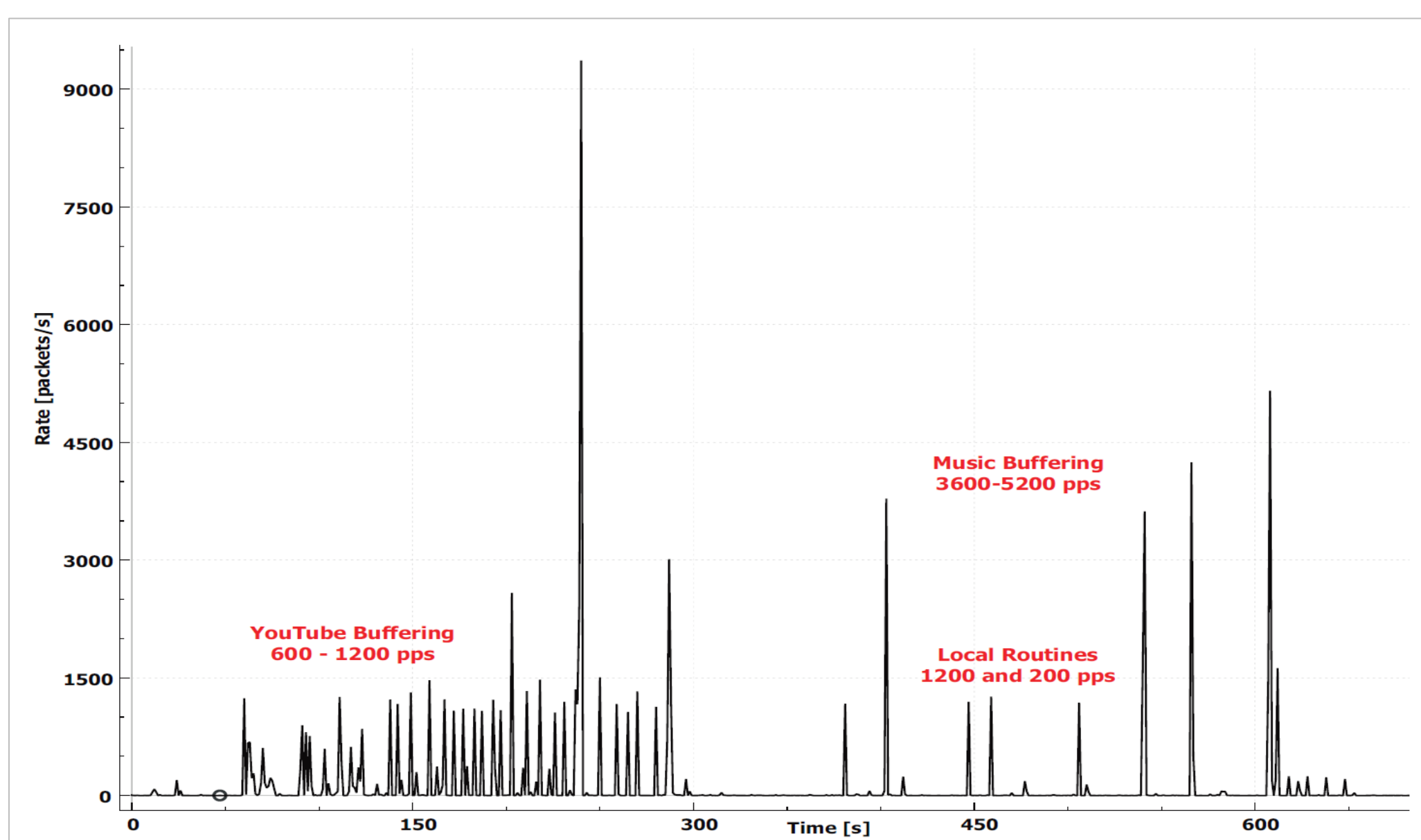
<http://www.nps.edu/library>

## Background

- Computer network traffic has traditionally been modeled with Gaussian distributions but is known to have non-Gaussian characteristics
- Little is known regarding the origins of scaling, heavy tails, and self-similarity frequently observed in the network core
- If traffic is known to be heavy-tailed, alternative distributions would improve accuracy of traffic models and anomaly detection systems



Improved fit of stable (solid line) over Gaussian (dashed) distribution to traffic data at onset of cyber attack.



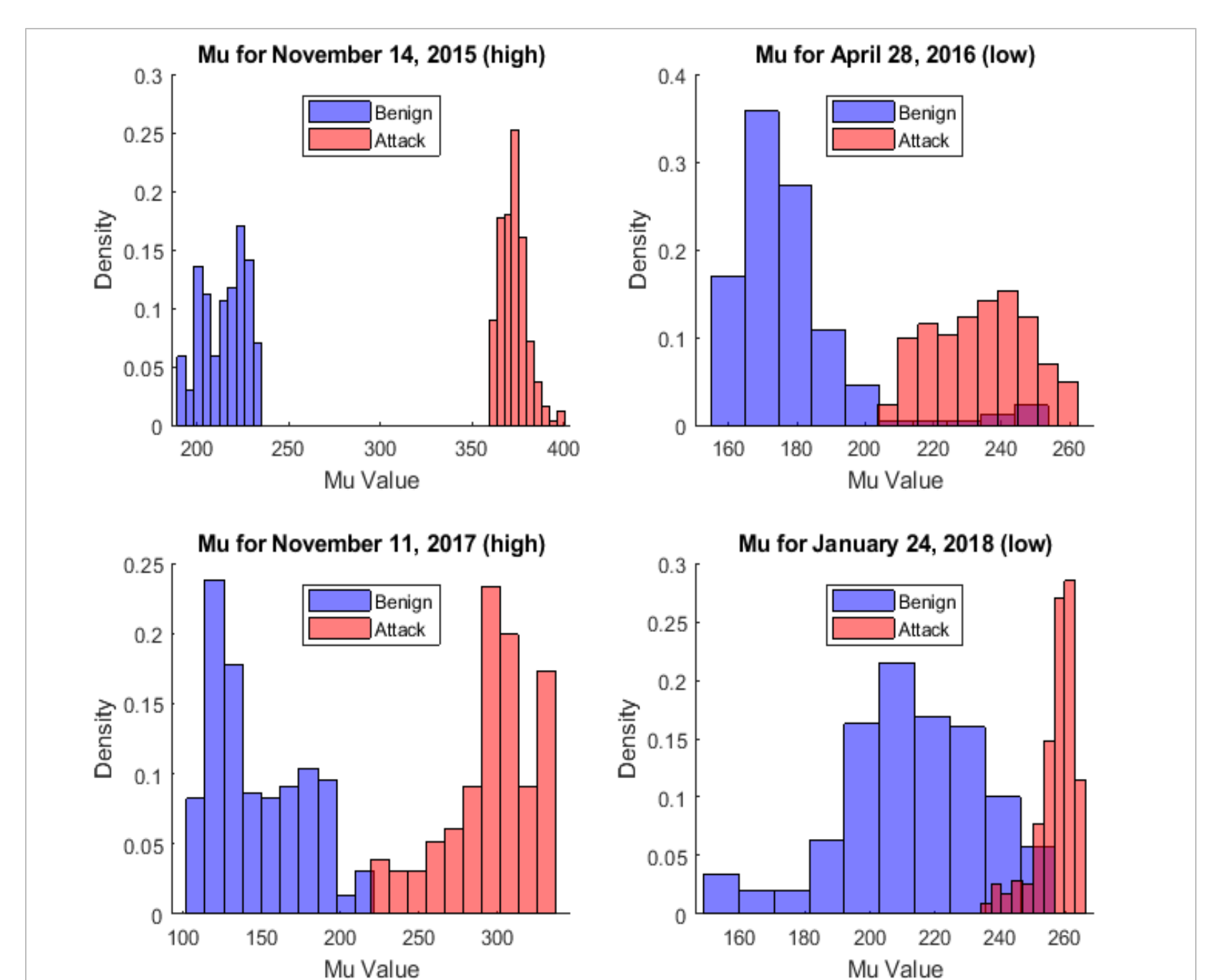
Device network traffic as a series of impulses, captured from 12 minutes of compute

## Methodology

- Use mathematical theory to explain observed heavy tails and self-similarity
- Identify and groom real-world data sets containing normal and attack network traffic
- Develop and employ alternative anomaly detectors using heavy-tailed (alpha-stable) tests
- Evaluate and optimize performance of alpha-stable detectors against denial-of-service attacks

## Results

- Categorizing device traffic as impulses permits applying the Generalized Central Limit Theorem or Renewal Theory that predict alpha-stable or Gaussian aggregations.
- Alpha-stable traffic can explain the self-similarity, scaling, and long-range dependence common in the literature.
- Alpha-stable anomaly detectors provide up to a 10% improvement over Gaussian tests at low false alarm rates ( $\leq 1\%$ ).
- Alpha-stable statistics vary significantly between attack and benign traffic, implying potential for ensemble detectors.



Stable parameter  $\mu$  (location) varies greatly between attack and benign traffic for 4 different data sets.

## Future Work

- Identify and optimize ensemble detectors (combinations of parametric tests) to fully harness the accuracy improvements provided by alpha-stable distributions.
- Improve the accuracy of the developed alpha-stable aggregation models to improve network resiliency and simulation.



**Researcher:** Assistant Professor Chad Bollmann  
Graduate School of Engineering and Applied Sciences  
**Topic Sponsor:** OPNAV N81IO, Information Warfare Branch

**NRP Project ID:**  
NPS-19-N039-A