2019-12

Cyber System Assurance through Improved Network Anomaly Modeling and Detection

Bollmann, Chad A.

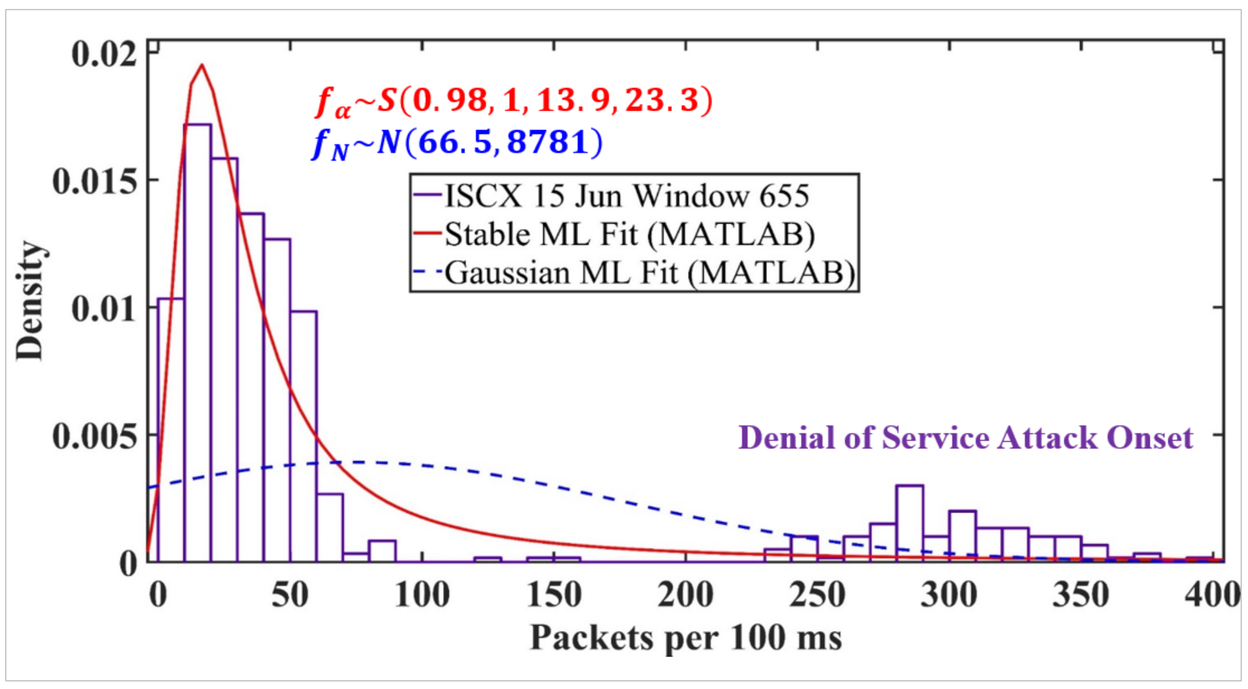
Monterey, California: Naval Postgraduate School

Cyber Assurance via Improved Network Modeling and Anomaly Detection

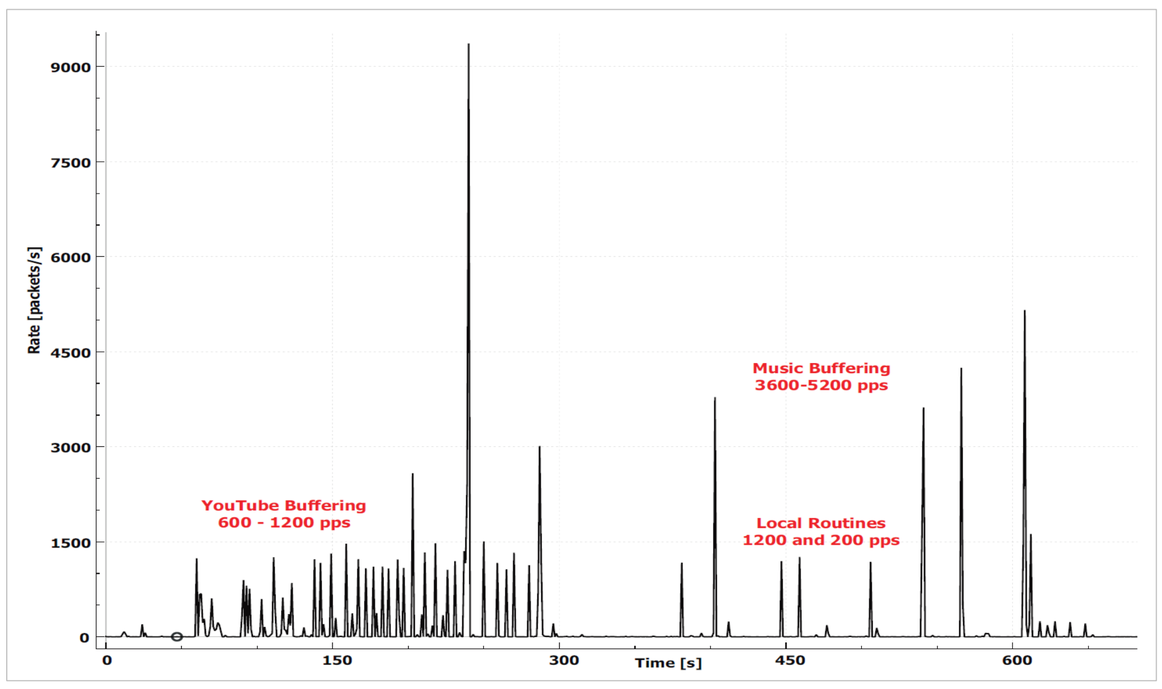
Naval Postgraduate School

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 onlset of cyber attack.



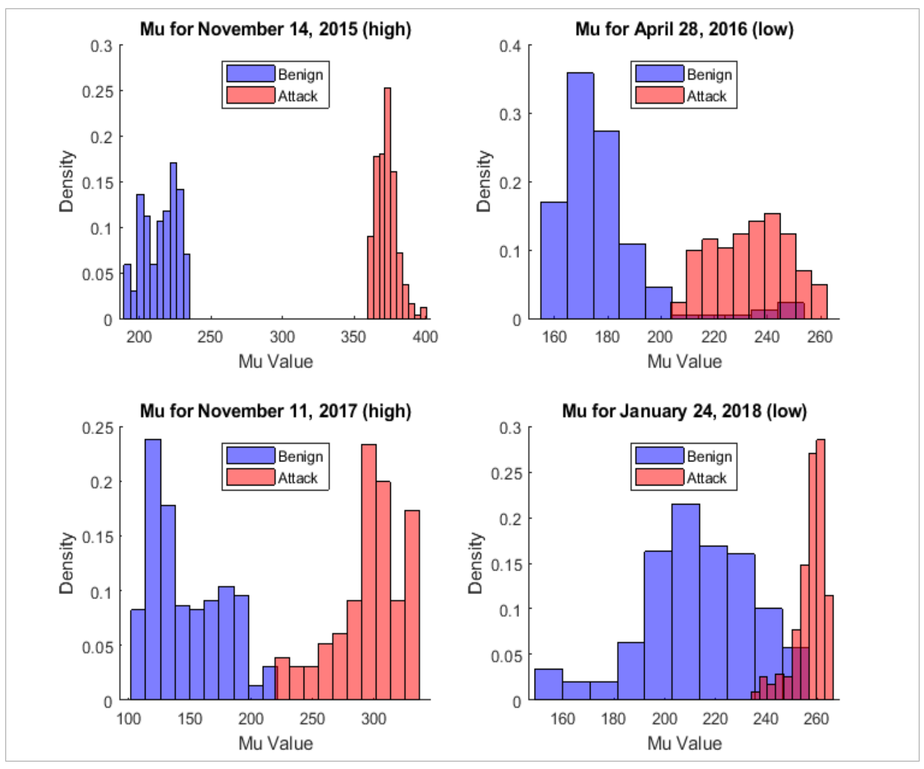
Device network traffic as a series of impulses, captured from 12 minutes of compute

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 (≤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