2018-04

Improved Detection of Cyber Anomalies

Bollmann, Chad; Tummala, Murali; McEachen, John

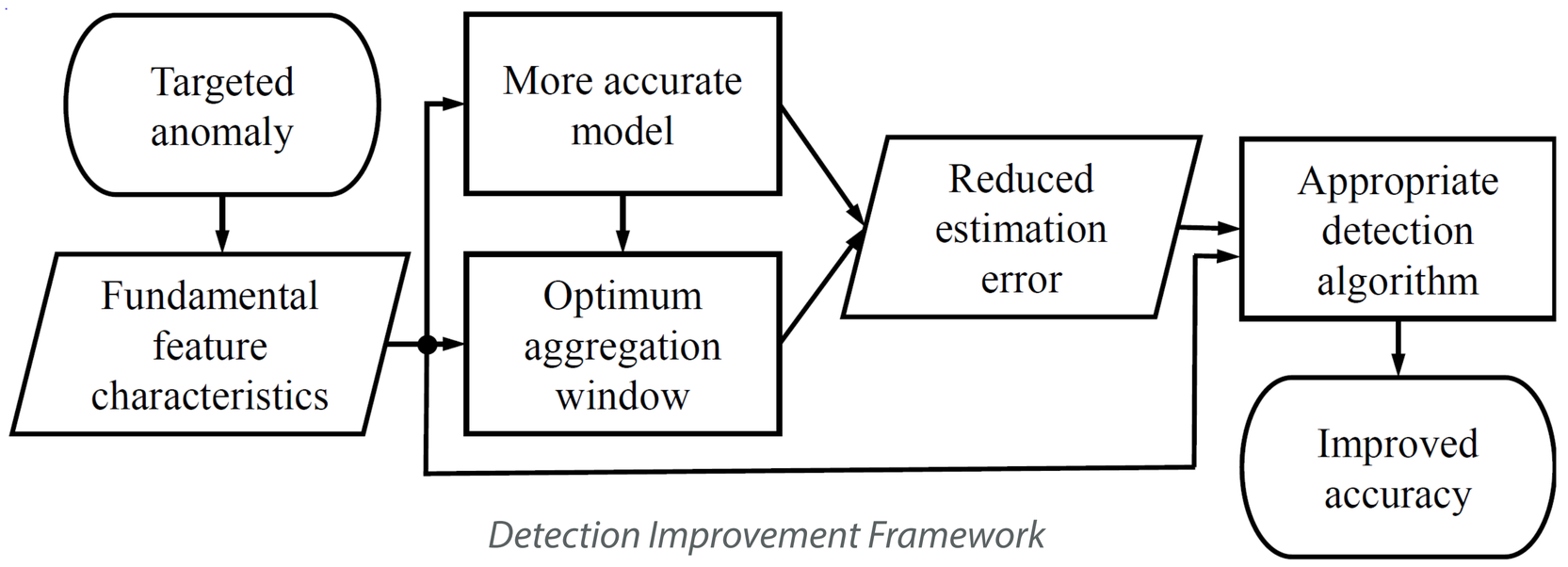
Monterey, California. Naval Postgraduate School

Improved Detection of Cyber Anomalies

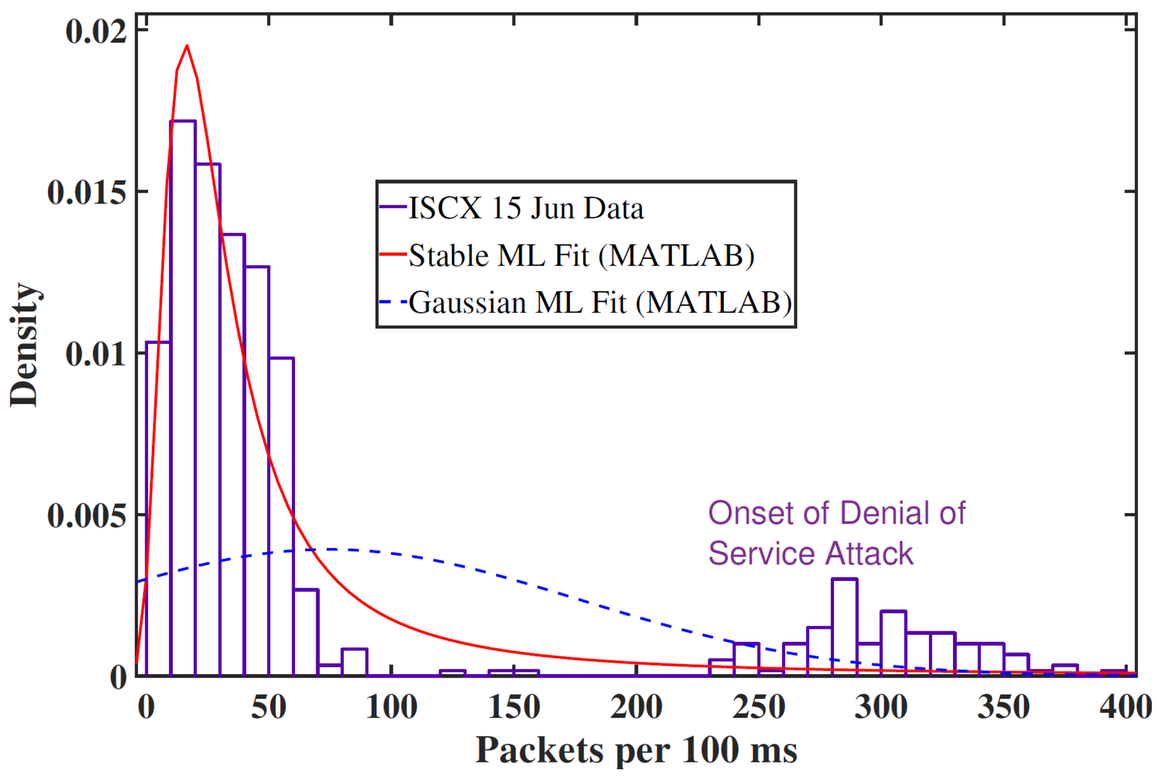
Naval Postgraduate School

Background

- α-Stable distributions provide better models for network traffic
  - Many traffic aspects are skewed and have heavy tails
- Our approach uses α-stable methods for more accurate detection of volumetric denial-of-service (DoS) attacks
  - Proof-of-concept operates in real time on backbone traffic at 1 Gbps



Detection Improvement Framework



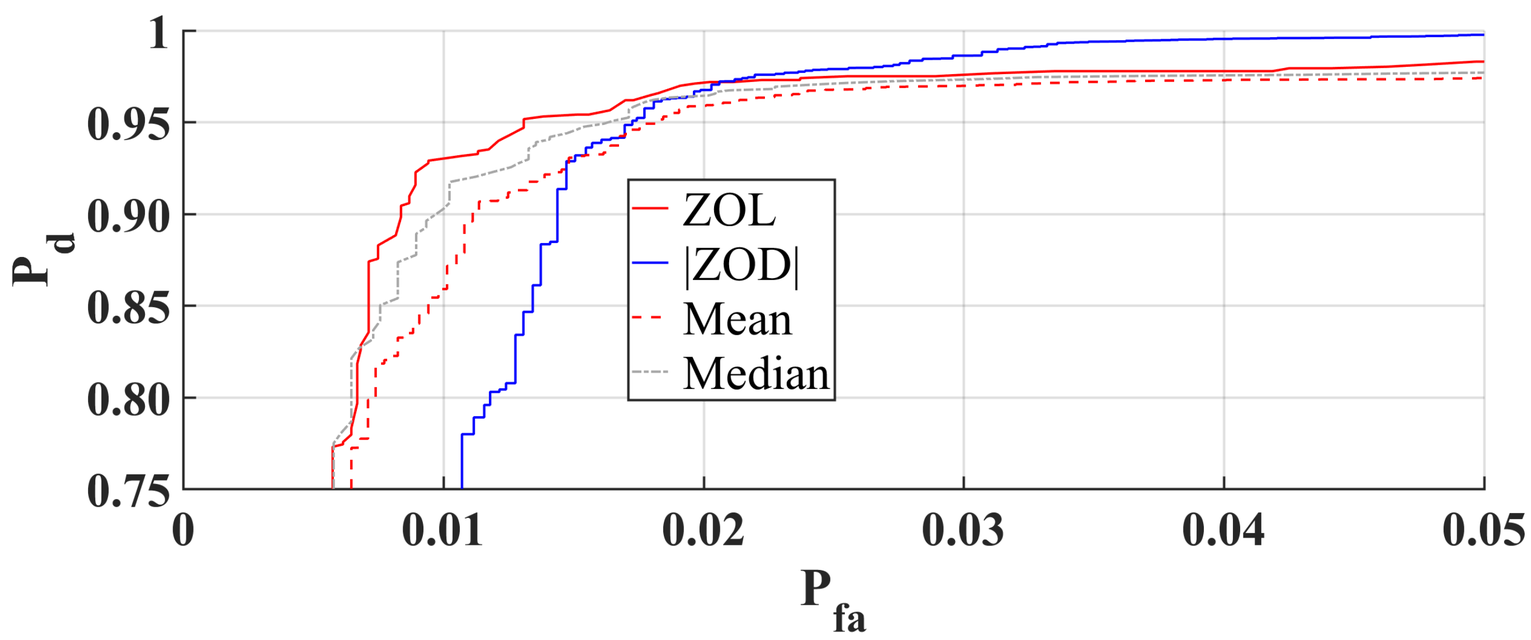
Comparison of Stable and Gaussian Models

α-Stable Traffic Models

- α-Stable models are more accurate under all conditions: attack (see left), benign, and transition
  - Peak accurately locates mode of traffic
  - Heavy tail accounts for outliers
- α-Stable models enable α-stable, maximum-likelihood approaches to detection and adaptive techniques

Detection with Stable Estimators

- Gaussian-equivalent estimators measure α-stable attributes
  - Location: ZOL
  - Dispersion: ZOD
- Detection performance assessed for low- (20%) and high-volume (100%) DoS attacks



Stable Detector ROC for Low Volume DoS Attack from MAWI Archive Data

Results

- Preliminary techniques improve accuracy by 3 – 8 % over Gaussian and peer methods
- α-stable estimators can be applied to any heavy-tailed time series in real-time

Proposed Future Work

- Investigate applicability to other networks and anomalies (e.g., changes in social networks)
- Refine and layer stable estimators for even greater real-time accuracy

Researcher: Asst. Professor Chad Bollmann, Professor Murali Tummala, and Prof. John McEachen
Graduate School of Engineering and Applied Sciences,
Electrical and Computer Engineering Department
Topic Sponsor: You?

Dissertation Title: Network Anomaly Detection with Stable Distributions