

Towards Systematically Evaluating Flow-level Anomaly Detection Mechanisms

Daniela Brauckhoff

brauckhoff@tik.ee.ethz.ch



Motivation

- Anomaly Detection systems widely deployed in ISP networks to provide detection of large scale anomalies
- *Benchmark evaluation traces* for systematic evaluations are not available to neither research nor industry
- Three major problems prevent systematic evaluations:
 - Privacy issues prevent publication of traces
 - Fixed intensity of anomalies in traces
 - Anomalies in traces are not annotated („ground truth“ is missing)

Existing Approaches

- **Privacy** is addressed with anonymization
 - Anonymization trade-off is still unsolved [Slagell05a, Slagell05, Pang06]
- **Varying anomaly intensity** is addressed with anomaly injection
 - Interaction with normal traffic is disregarded [Soule05, Lakhina05, Rupp05]
- **Ground truth** is addressed with either manual labeling or labeling through reference systems
 - Both approaches subjective and error-prone

Our approach: Synthetic generation of benchmark traces

- Has potential to provide a variety of background traffic and anomaly scenarios
- Ground truth is known a priori given that anomalies are generated from model
- Main Challenges
 - Define normal and anomalous network behavior („*baselining*“)
 - Find *realistic models* for normal and anomalous flow traffic

Baselining

- Ground truth is key to building baseline model and anomaly models
- Step 1: Explicitely define what is anomalous/normal
 - Take prevalent behavior for normal
 - Characterize known anomalies (DDoS, portscan, etc.)
- Step 2: Identify anomalies according to definition
 - May require additional data

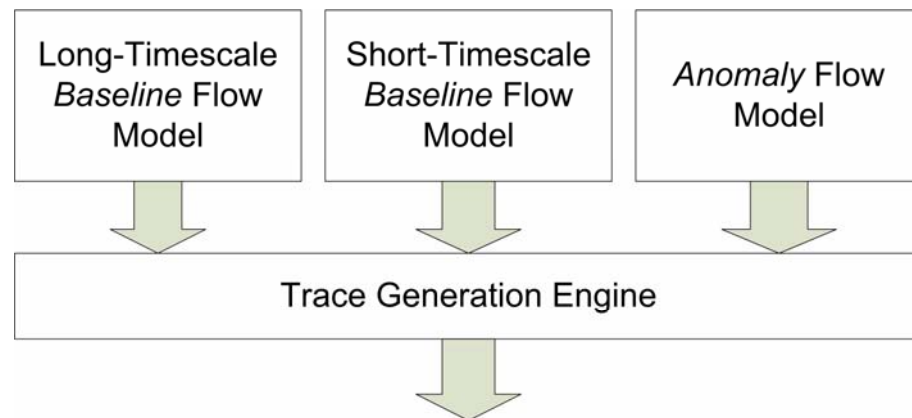
Realistic Reference Model

- Timescale of traffic
 - Long (training period) and short (typical aggregation interval of several minutes) timescale needs to be addressed by model
- Flow parameters
 - Address typical volume (packets, bytes) and spatial (IP addresses, ports) metrics
- Versatile anomaly models
 - Anomalies of varying intensities, account for interaction with normal traffic

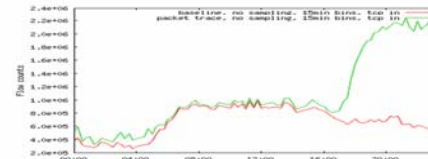
None of the existing models addresses all requirements
[Soule05, Barakat03, Fredj01, Sommers04]

Generating Synthetic Flow Traces

1. Traffic model for baseline/normal flow traffic (long and short timescale)
2. Traffic model for anomalous flow traffic
3. Trace generator generates traffic according to models



Synthetic Benchmark Flow Traces



Discussion

- We have identified three main problems with systematic evaluations
 - Privacy-concerns, variable anomaly intensities, ground truth
- We have shown that existing approaches fall short in addressing these problems
- We suggest to generate synthetic benchmark traces and have identified the main challenges
 - Baselineing to identify anomalies
 - Find realistic flow traffic models for normal/anomalous traffic
- Synthetic benchmark traces can be generated from a baseline model and anomaly flow models