Network Anomaly Detection Using Adaptive Resonance Theory

Daniel Rossell, Christos G. Cassandras, Jing Wang, Ioannis Ch. Paschalidis

Motivation

- **Biology**
  - Adaptive Resonance Theory (ART) was originally developed to describe how the human eye recognizes and classifies different images (Carpenter & Grossberg, 1987)
  - This idea can be extended to network traffic flows to classify good and bad traffic

- **Network Security**
  - Help identify previously unknown network intrusion threats
  - Much faster than traditional packet inspection techniques
  - Ability to learn and adapt improves detection rates over time

Cluster Creation

- **Phase 1 – Process Input**
  - Process input based on Flow Size, Flow Duration and IP Distance
  - Compare each input sample to each existing cluster using the cluster’s prototype vector
  - Find the best match for the sample using the vigilance parameter
  - Each cluster adapts to the addition of new samples via the learning process

- **Phase 2 – Cluster Fluctuation**
  - Cluster prototype vectors change over time due to the learning process
  - Recheck each sample and compare to each existing cluster until an equilibrium is reached

Test Network Design

- **Topology**
  - Realistic network design based on current generation military networks
  - Hub and spoke topology with satellite transmission paths

- **Network Flow Simulation**
  - The network flow simulation tool FS was used to generate realistic network flow data
  - Anomalous flows were also created and added to the input stream for the ART algorithm to analyze

Anomaly Detection

- **Identify Desired Detection Characteristics**
  - Tradeoff between anomaly detection rate and false positive rate
  - Ideal threshold value around 0.15
  - Anomaly Identification is 100% for deviations >5%

- **Different Vigilance Parameter Values**
  - Graph showing the relationship between vigilance parameter and false positive rate

Results

- **Flow Size Anomaly**
  - Grouping of flows with a much larger than normal flow size

- **IP Based Anomaly**
  - Normal traffic from an unknown IP address

Key Concepts

- **Vigilance Parameter**
  - A value between 0 and 1 that determines how far away a sample point can be on a given dimension and still be considered a match for a given cluster. A higher value means smaller cluster size.

- **Threshold**
  - A value between 0 and 1 that determines how many anomalous clusters will be identified. A higher value flags more clusters as anomalies.