# APPROXIMATE AUTOREGRESSIVE MODELING FOR NETWORK ATTACK DETECTION

Harshit Nayyar(UNB, Fredericton), Ali A. Ghorbani (UNB, Fredericton)

## 1. Introduction : Prisoners' Dilemma (PD)

Network attacks are becoming increasingly frequent. Attacks such as Denial of Service, Distributed Denial of Service and Worms cause network downtime and lead to significant losses. Timely detection and mitigation of these attacks is an active area of research. Network attacks cause changes in statistical properties of network signals. We detect such changes to identify an intrusion in an online real-time manner.

## 2. Objectives

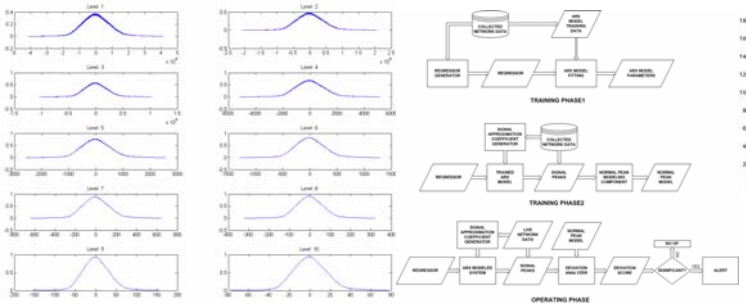
Our research focuses on automating the process of network signal anomaly detection. We define an anomaly as an unexpected occurrence. This definition by its very nature contains an aspect of expectation. Therefore, our first objective is to create a model of this expected behaviour. Next we need to identify the limits of normal deviations from expected behaviour. Finally, we should flag violations of these limits as anomalies.

## 3. Motivation

Most network signals follow predictable trends of high values during the day, low at night, increasing in the morning and decreasing in the evening. Network administrators gain experience from the signals of their networks and learn to identify abnormal conditions. We propose a solution to automate this process. Our methodology involves techniques such as system identification and wavelet processing.

## 4. Methodology

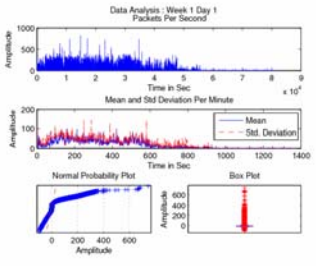
Network signals are non-stationary and have a high variance. This variance causes a decrease in correlation of network signals over multiple days. We use wavelet approximations to extract a high level summary from the network signal.



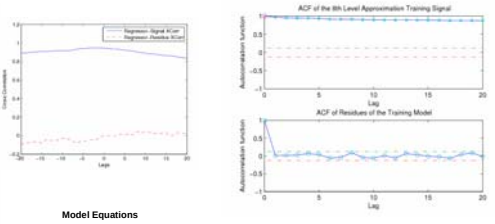

In Training Phase1, the *expected* network behaviour is modeled using an **ARX** (**A**uto**R**egressive with e**X**ternal input) model. In Phase2, the normal peak limits are created. Finally during operations, the signal is monitored for anomalous deviations from created models

## 6. Results

**Exploratory Data Analysis**




**ARX Model Training**



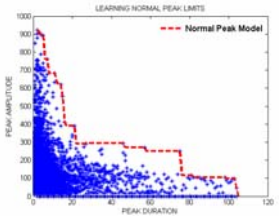

**Model Equations**

$$A(q)Y(t) = B(q)U(t) + e,$$

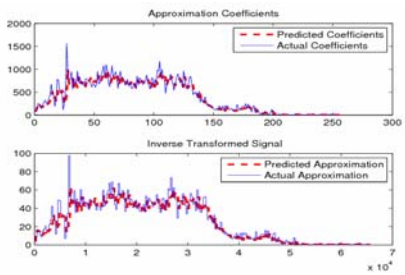
$$A(q) = 1 - 0.5473q^{-1} - 0.03136q^{-2} - 0.0863q^{-3} - 0.1015q^{-4}$$

$$B(q) = 0.1605 + 0.188q^{-1} - 0.1868q^{-2} + 0.1934q^{-3}$$

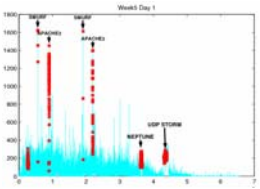
**Peak Model Training**




**Approximate Prediction**




**Output showing Anomalies Detected**




**Summary of Attacks Detected**

| Attack Name | Time in Documentation | Visual Inspection Time | Total Attack Duration | Latency (n=3) | Latency (n=1.75) | Latency (n=1.5) | Latency (n=1.25) | Latency (n=1) | Latency (n=0.75) | Latency (n=0.50) | Latency (n=0.25) | Latency (n=0.1) | Attack Type |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| WD01_SATAN | 12:02:13 | 12:02:21 | 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Hi Scan |
| WD04_SATAN | 9:33:17 | 9:33:32 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Hi Scan |
| WD04_NEPTUNE | 11:04:16 | 11:04:15 | 203 | 93 | 93 | 89 | 89 | 89 | 89 | 89 | 89 | 89 | DoS |
| WD05_NEPTUNE | 11:20:15 | 11:20:13 | 203 | 104 | 104 | 104 | 104 | 78 | 78 | 78 | 78 | 42 | DoS |
| WD01_SMURF | 21:34:16 | 21:34:06 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | DoS |
| WD03_SMURF | 18:29:25 | 18:29:13 | 1 | ND | ND | ND | ND | ND | ND | 1 | 1 | 1 | DoS |
| WD45_SMURF | 8:45:18 | 8:45:16 | 2 | ND | ND | ND | 0 | 0 | 0 | 0 | 0 | 0 | DoS |
| WD01_SMURF | 9:33:00 | 9:34:11 | 120 | ND | ND | ND | ND | ND | ND | 0 | 0 | 0 | DoS |
| WD01_APACHE2 | 10:29:22 | 10:29:20 | 1057 | ND | 28 | 22 | 19 | 16 | 13 | 11 | 4 | 1 | DoS |
| WD01_SMURF | 13:18:12 | 13:18:08 | 1 | ND | ND | ND | ND | ND | ND | 0 | 0 | 0 | DoS |
| WD01_APACHE2 | 14:05:43 | 14:05:39 | 604 | ND | ND | 26 | 26 | 26 | 26 | 26 | 6 | 4 | DoS |
| WD01_NEPTUNE | 18:04:43 | 18:04:00 | 411 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 90 | 56 | DoS |
| WD01_UDPSTORM | 20:00:27 | 20:00:30 | 900 | 102 | 102 | 102 | 102 | 102 | 102 | 102 | 86 | 73 | DoS |
| WD02_NEPTUNE | 11:38:04 | 11:31:38 | 821 | 68 | 50 | 18 | 15 | 11 | 7 | 0 | 0 | 0 | DoS |
| WD03_APACHE2 | 17:13:17 | 17:13:06 | 519 | ND | ND | ND | 15 | 11 | 7 | 7 | 7 | 1 | DoS |
| WD04_SATAN | 14:58:00 | 14:58:23 | 132 | 3 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | Hi Scan |
| **Average# of False Positives per day** | | | | <1 (0.57) | <1(0.64) | 1 | <2(1.21) | <2(1.64) | <3(2.28) | <3(2.64) | <5(4.20) | <6(5.71) | |

## 7. Conclusions

Networks signals display a high variance, which suppresses periodic and predictable behavior. This behavior can be unraveled using wavelet approximation coefficients and modeled using Auto Regressive Modeling. After prediction of predictable behavior, only high frequency transients which we call 'peaks' remain. An intrusion causes violation of either amplitude of a normal peak or frequency of a normal peak. This fact can be used to detect anomalies in network signals caused by network attacks. This methodology of network signal anomaly detection shows promising results.

network security laboratory

UNIVERSITY OF NEW BRUNSWICK

UNB