Statistical Traffic Anomaly Detection: A Large Deviations Approach

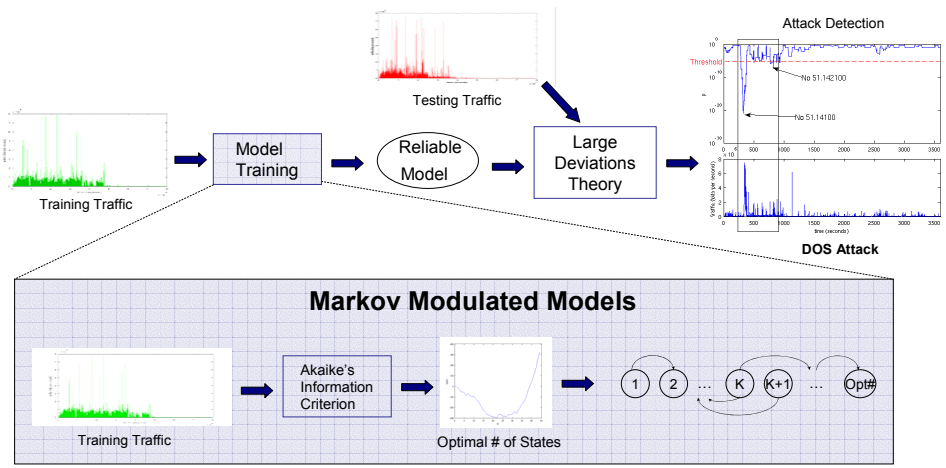
Georgios Smaragdakis, Maria Konte, Ioannis Ch. Paschalidis – Boston University

Abstract

We introduce a traffic anomaly detection mechanism based on Large Deviations asymptotic results. We monitor the aggregated traffic at a border router of a local network during busy hours, where no anomalies have been observed. We model this traffic with disjoint Markov modulated processes estimating the optimal number of states using the Akaike's Information Criterion and we assume that this model is reliable for representing the traffic activity for this time interval of the day. Using the model as reference we rapidly identify anomalies in traces corresponding to the same time-of-day interval. To that end, we develop Large Deviations results to assign to each traffic sample a probability of being "consistent" with the reference model. Our simulation results show that (even short-lived) anomalies are identified within a small number of observations. We have developed software to validate our technique by analyzing real traffic traces with time-stamped attacks.

Advantages:
1. ***General,*** as it detects all types of anomalies
2. ***Prompt,*** as it can detect on line the anomalies within a small number of observations.
3. Our threshold is ***Independent*** of traffic volume moments.

Method Overview



Anomaly Detection Algorithm

1) From an anomaly-free trace obtain a d-MMP with transition probability vector $\boldsymbol{p}$.
2) For each time t let $Y_t = (Y_{t-n}, Y_{t-n+1}, ..., Y_t)$ the trace of current traffic activity of n consecutive traffic measurements (in bits/sec). Compute its empirical measure and let $\mathcal{E}_{n,2}^{Y_t} = \boldsymbol{q}_{t,n}$ be the result (n is the size of a sliding window).

3) Then, $\rho_{t,n} = e^{-nI_1(\mathcal{E}_{n,2}^{Y_t})}$ approximates the probability that the trace Y_t is drawn from the d-MMP with transition probability vector $\boldsymbol{p}$. If $\rho_{t,n}$ is consistently low for some observed time interval (e.g., for 10 seconds), we conclude that the observed trace does not "appear coming" from the reliable model which indicates an anomaly.

Theoretical Background

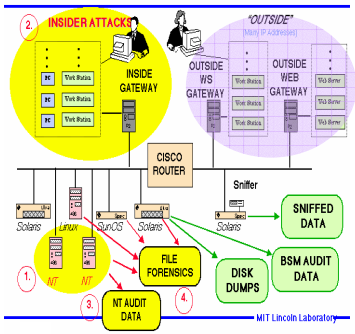
Assume that the d-MMP has an irreducible underlying Markov chain with M states 1,2,…,M. Let denote a sequence $Y_1, Y_2, ..., Y_n$ of states that the Markov chain visits and consider the empirical measures $\mathcal{E}_{n,2}^{Y_t}(y) = \frac{1}{n}\sum_{k=1}^{n} 1_y(Y_{k-1}Y_k)$ where 1_y is the indicator function for the subset

A large deviations result for $\mathcal{E}_{n,2}^{Y_t}$ is established in the next theorem:

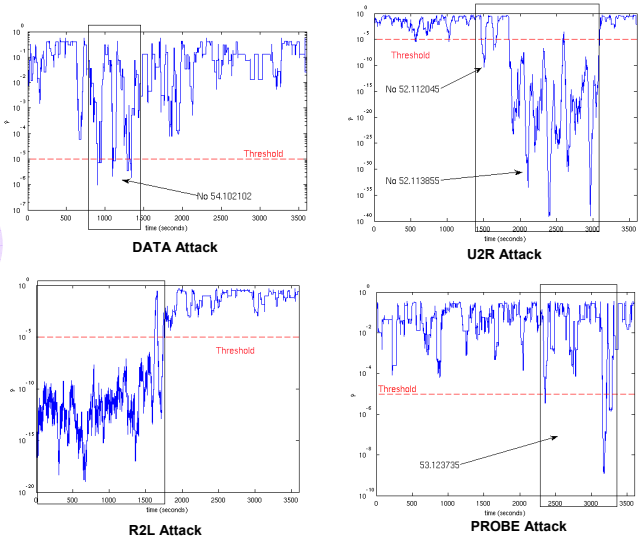
Theorem
For every $\boldsymbol{q} \in \boldsymbol{M}_1(\boldsymbol{A}_p^2)$ let $I_1(\boldsymbol{q}) = \begin{cases} \sum_{i=1}^{M} \boldsymbol{q}_1(\boldsymbol{i}) \boldsymbol{H}(\boldsymbol{q}_f(\cdot \mid \boldsymbol{i}) \mid \boldsymbol{p}(\boldsymbol{i},\cdot)), \text{ if } \boldsymbol{q} \text{ is shift invariant} \\ \infty, \text{ otherwise} \end{cases}$

where $\boldsymbol{H}(\boldsymbol{q}_f(\cdot \mid \boldsymbol{i}) \mid \boldsymbol{p}(\boldsymbol{i},\cdot))$ is the *relative entropy.* More intuitively, Theorem states that for a long trace Y (i.e, large n) it's empirical measure is "close to" **q** with probability that behaves as $\boldsymbol{P}[\mathcal{E}_{n,2}^{Y_t} \approx \boldsymbol{q}] \sim e^{-nI_1(q)}, y \in A^2 = \{1....,M\} \times \{1....,M\}$

Experimental Setting



Experimental Results



Performance Evaluation

Attack Category	Success Rate
Data	100%
DoS	89.50%
PROBE	84.60%
R2L	76.50%
U2R	88%
Overall	**88%**

Day	Attacks	Attacks Identified	False Alarms
Monday	17	16	3
Tuesday	21	17	1
Wednesday	13	8	1
Thursday	13	13	4
Friday	19	19	2
Overall	**83**	**73**	**11***

* These false alarms may correspond to other types of traffic anomalies that are not described in the DARPA evaluation of attacks.