



The Insecurity of Open Source Intrusion Detection Systems: A Case for Cryptographically-Inspired IDS Design

Syed Ali Khayam

Assistant Professor

Wireless & Secure Networks (WiSNet) Research Lab

School of EE&CS (SEECS)

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

Malware Trends ...

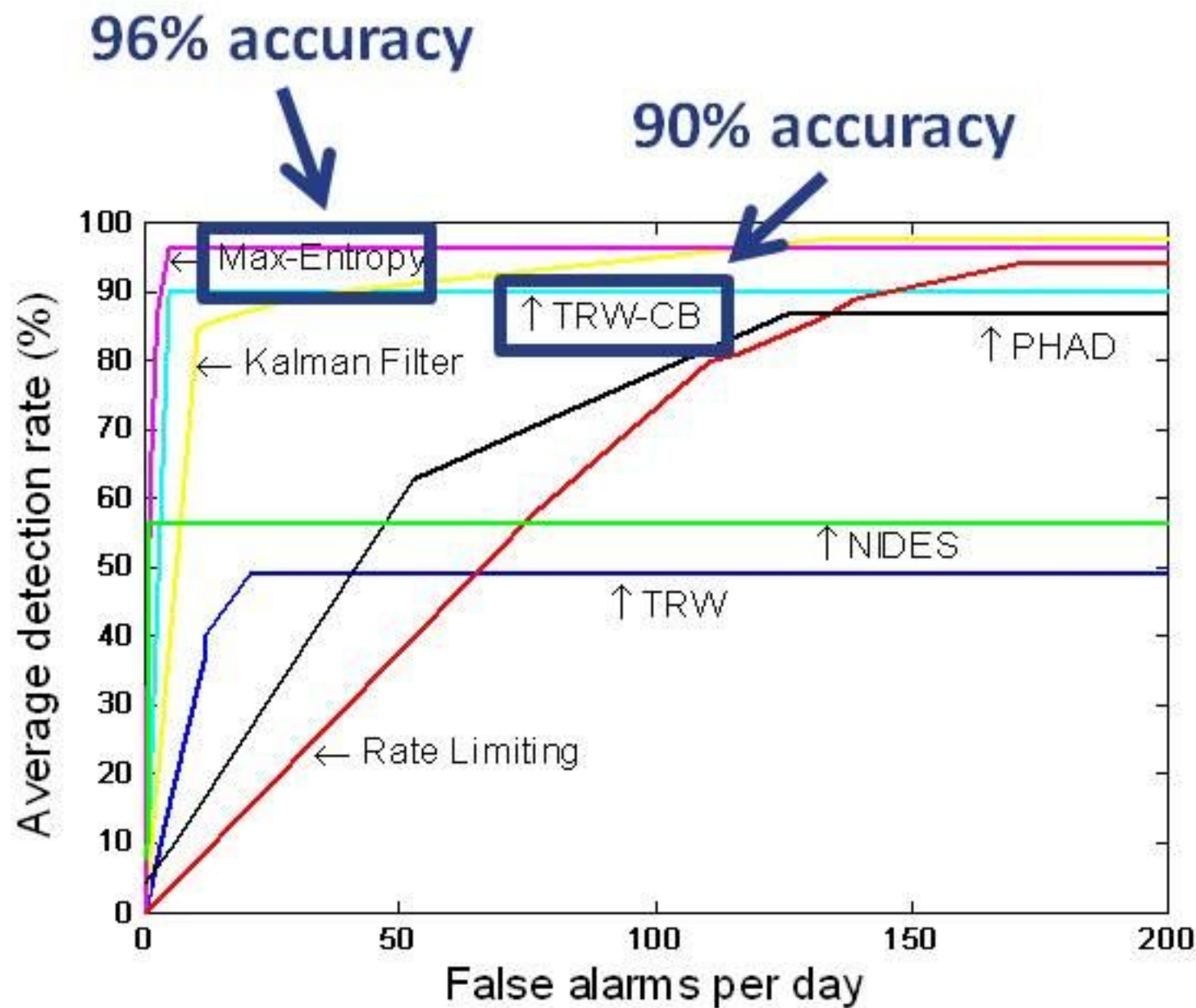
- Symantec reported a **468% increase** in previously-unseen attacks over a six month period in 2007
- Symantec reports 1,656,227 malicious code threats detected in 2008 which represents over **60 percent** of the approximately 2.6 million malicious code threats that Symantec has **ever** detected
- “We are projecting a **10-fold** increase in malware objects (in 2009 as was) detected in 2008”Ryan Naraine, the security evangelist for Kaspersky

Reference: Symantec Internet Security Threat Reports I–XI, Jan 2002–Jan 2008.

Symantec Global Internet Security Threat Report Trends for 2008, Volume XIV, 2009

Emerging Cyber Threats Report for 2009, Georgia Tech Information Security Center, October 15, 2008

Current State-of-the-Art in IDS

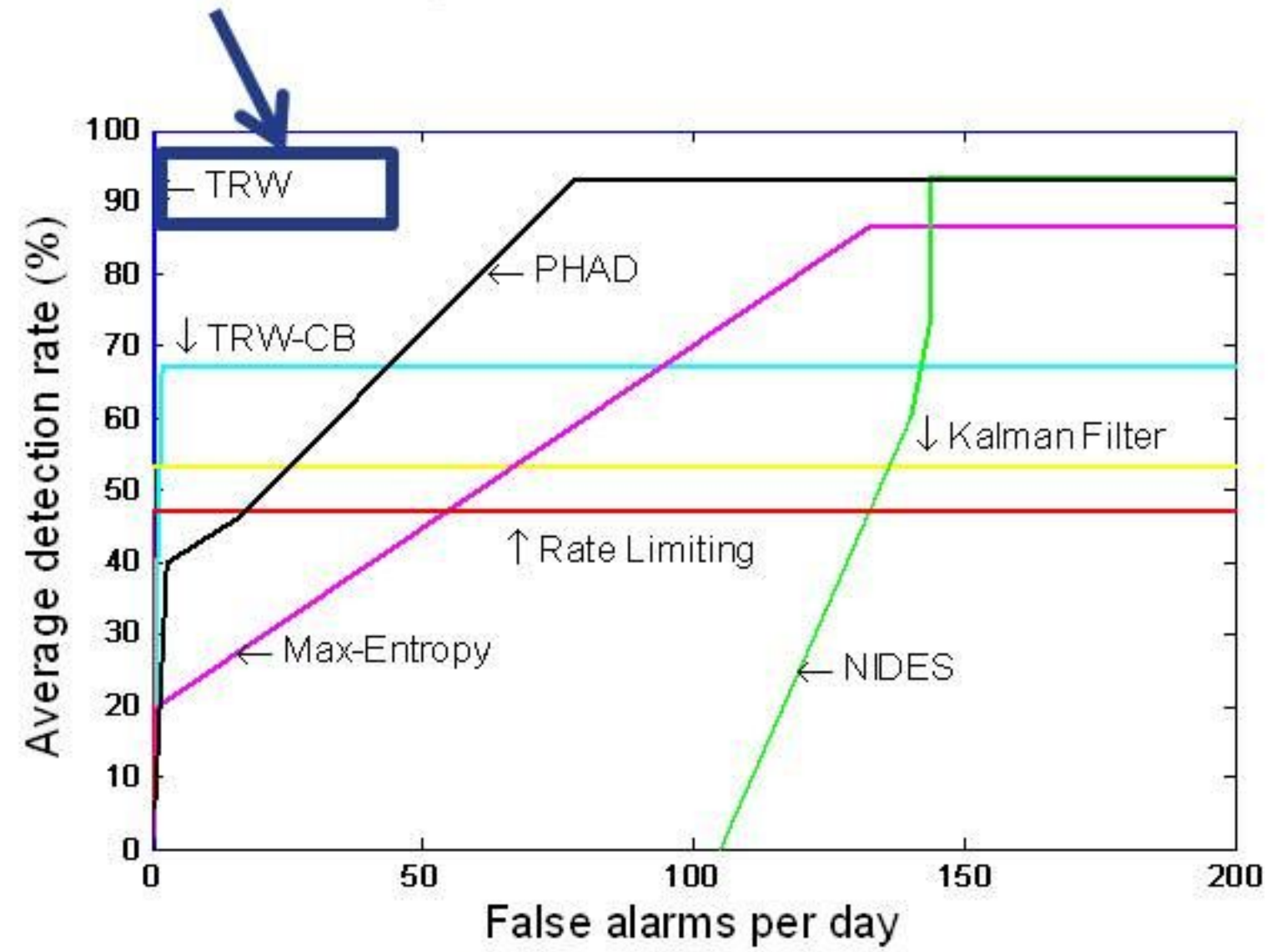


On Network Endpoints

Reference: Ayesha Binte Ashfaq, Maria Joseph Robert, Asma Mumtaz, Muhammad Qasim Ali, Ali Sajjad, and Syed Ali Khayam, "A Comparative Analysis of Anomaly Detectors under Portscan Attacks," Recent Advances in Intrusion Detection (RAID), September 2008.

Current State-of-the-Art in IDS

100% accuracy !



On Network Gateway

Reference: Ayesha Binte Ashfaq, Maria Joseph Robert, Asma Mumtaz, Muhammad Qasim Ali, Ali Sajjad, and Syed Ali Khayam, "A Comparative Analysis of Anomaly Detectors under Portscan Attacks," Recent Advances in Intrusion Detection (RAID), September 2008.

Why do IDSs still fail?

The malware detection techniques **rely on statistical testing** and therefore **can be fooled by test simulability**. In other words whenever the underlying detection methodology is **known**, it is possible to build an attack to evade the IDS.

- social engineering
- reverse engineering
- fingerprinting
- trial and error
- polymorphic blending attacks
- mimicry attacks
- portscans, etc.

Reference:

Eric Filiol, Frederic Raynal, "Malicious statistics," CanSecWest 2008.

Eric Filiol, "Malware of the Future," Journal in Computer Virology, 2007.



Breaking State-of-the-Art IDSs

Aim: Our main aim, as an attacker, is to estimate the **evasion margin** for the IDS. This evasion margin is the bound on the number of attack packets (t) that an attacker can send to a target entity (host/network) without detection !

Breaking Maximum Entropy IDS

~Configuration Parameters

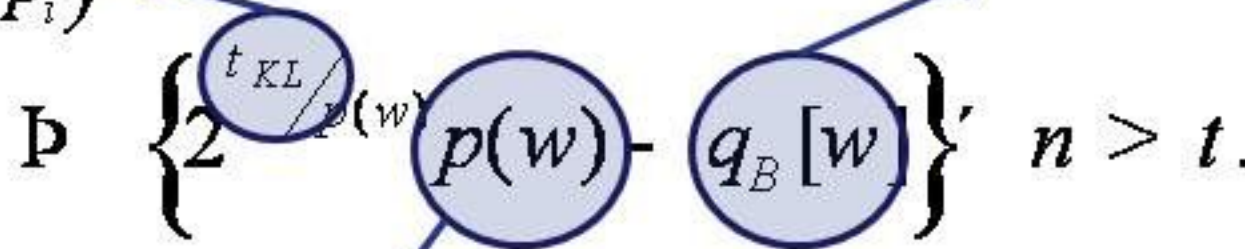
- Threshold: t_{KL}
- Baseline distribution: $p(w)$
- Real-time distribution: $q(w)$

~Detection Principle

$$D_{p||q}(w) = p(w) \log \left(\frac{p(w)}{q(w)} \right) > t_{KL}.$$

Markovian stochastic model

$$H_{\max} = \max_{i,j \in \{1,2,\dots,n\}} H(p_j | p_i)$$



- Real-time Observation
- Brute force

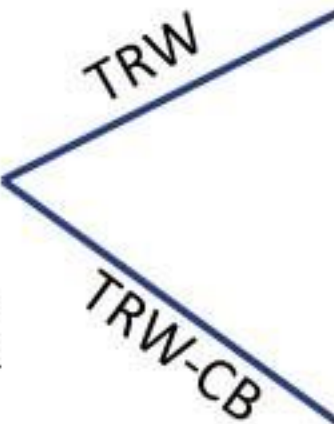
Breaking TRW-based IDSs

~Configuration Parameters

- Threshold: t_1
- A priori probabilities:

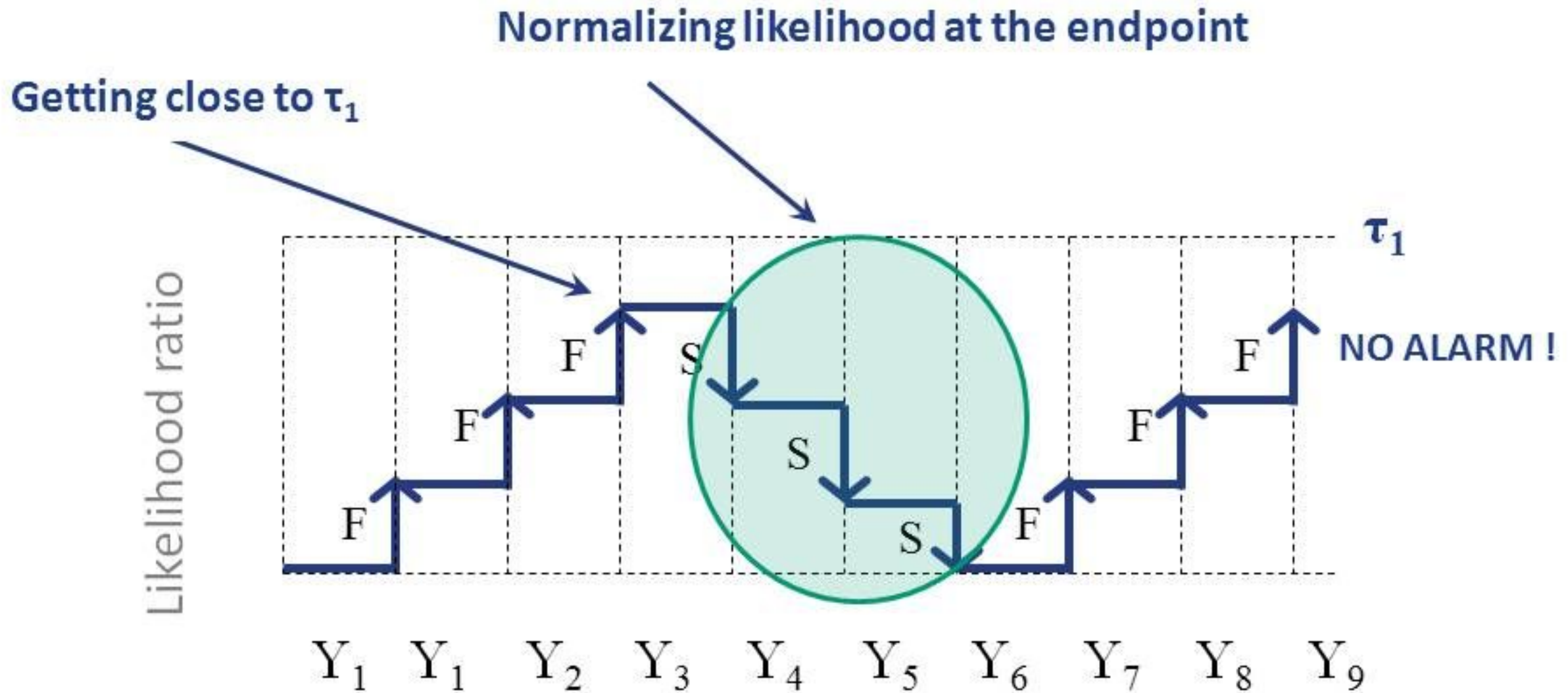
$$\begin{aligned} \Pr[Y_i = 0 / H_0] &= q_0 & \Pr[Y_i = 1 / H_0] &= 1 - q_0 \\ \Pr[Y_i = 0 / H_1] &= q & \Pr[Y_i = 1 / H_1] &= 1 - q \end{aligned} \quad " \quad q_0 > q .$$

~Detection Principle

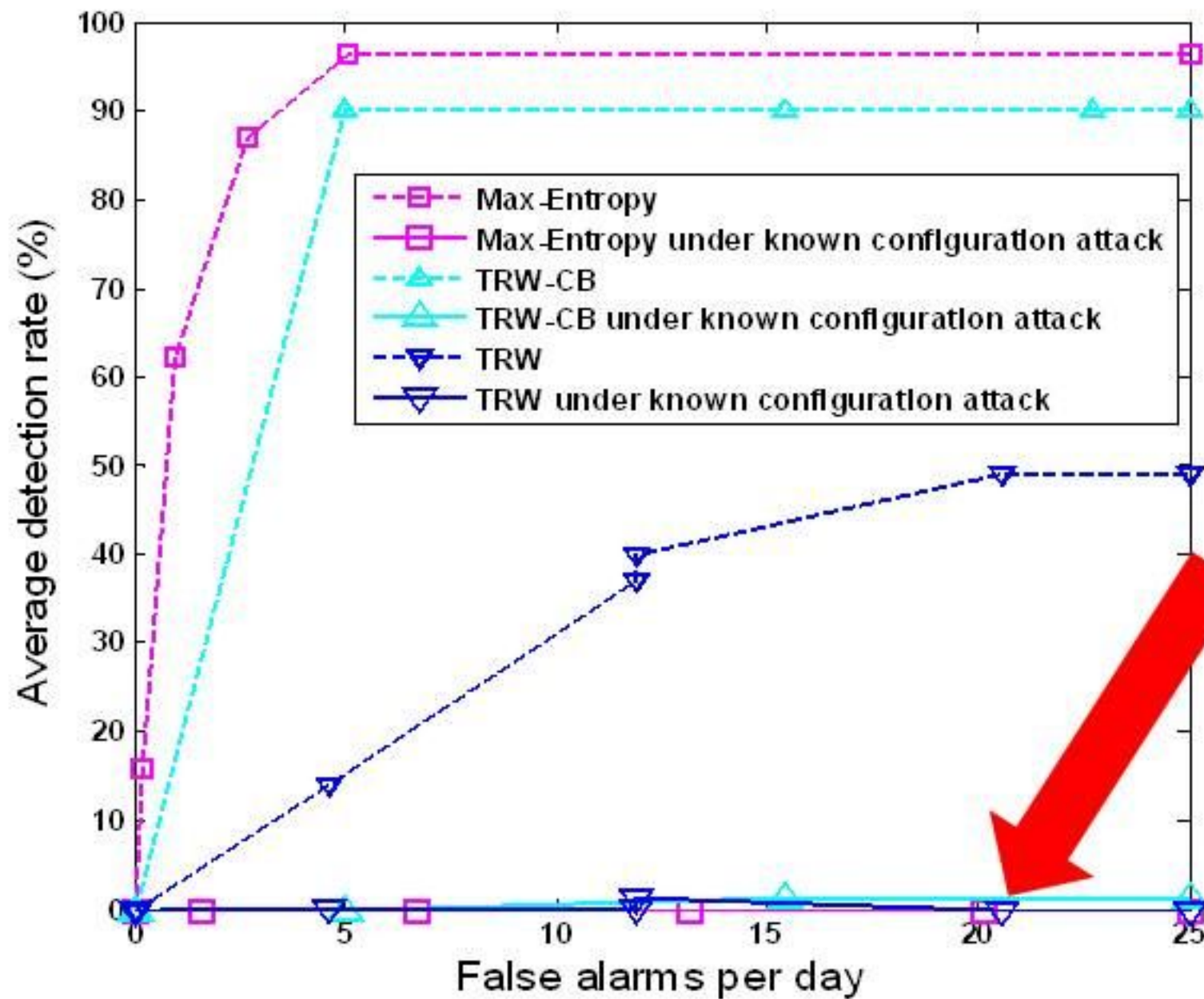
$$\Lambda(Y) \equiv \prod_{i=1}^n \frac{\Pr[Y_i | H_1]}{\Pr[Y_i | H_0]} < \eta_1$$


- Estimates if the local/remote host is a scanner
- Per host basis

Breaking TRW-based IDSs



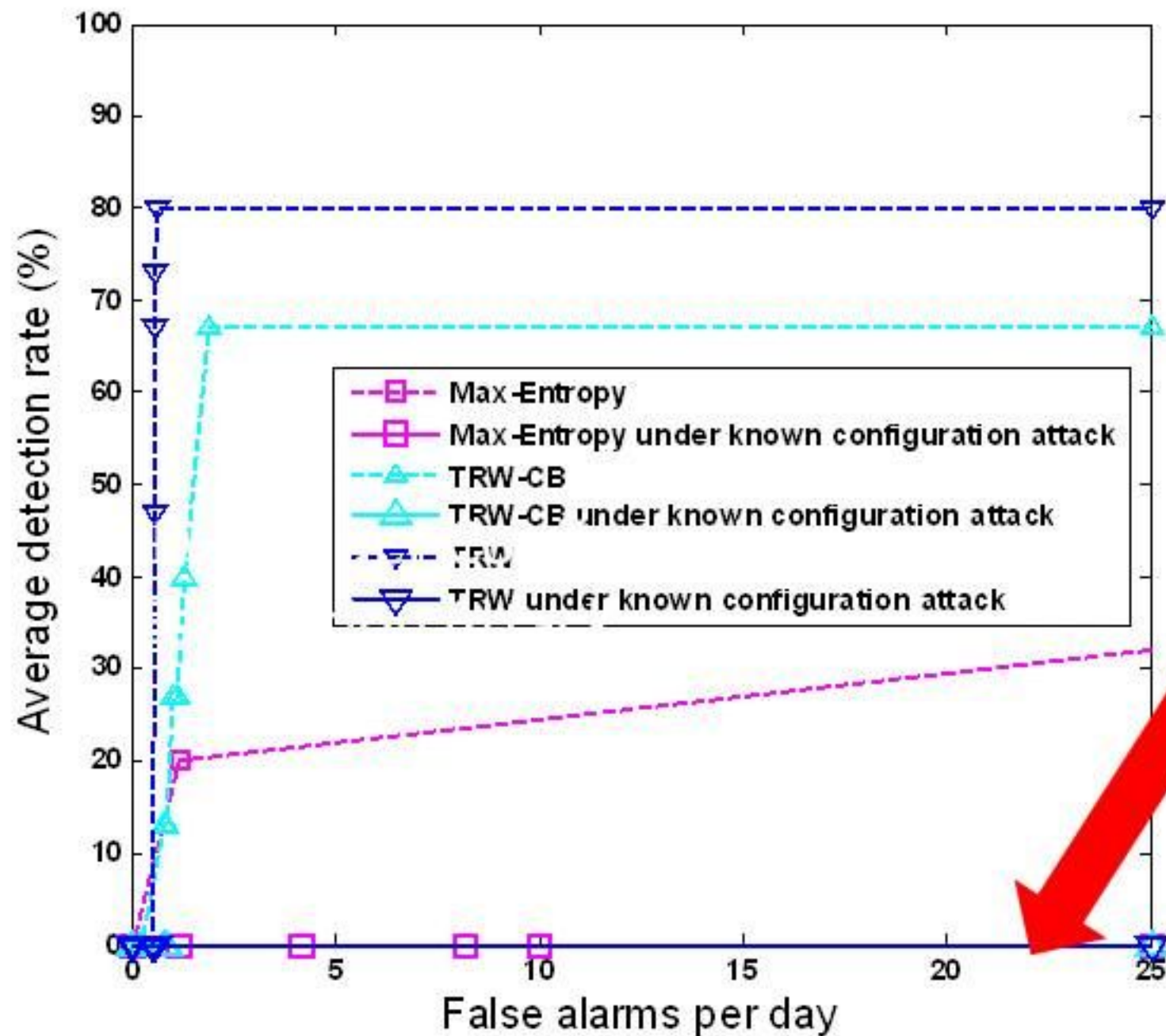
IDSs under Configuration Estimation Attack



IDSs completely Paralyzed !!!!!

On Network Endpoints

IDSs under Configuration Estimation Attack



IDSs completely Paralyzed !!!!!

On Network Gateway

Lessons Learnt

- Current State-of-the-Art IDSs provide acceptable accuracy dividends on specific deployment points
- Cannot scale to different points of network deployment
- Statistical IDSs provide highest accuracy
- Trivial to break statistical IDSs with stochastic analysis

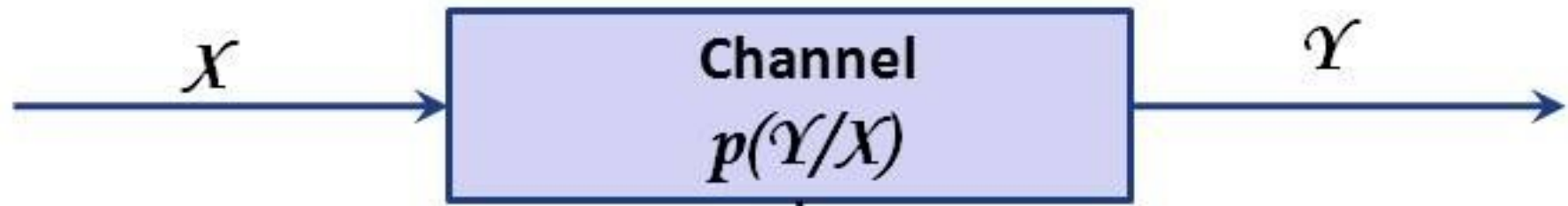


Cryptographically-Inspired Intrusion Detection

There is a need to revisit the IDS detection design philosophy in accordance with **Kerckhoff's principle** of cryptography

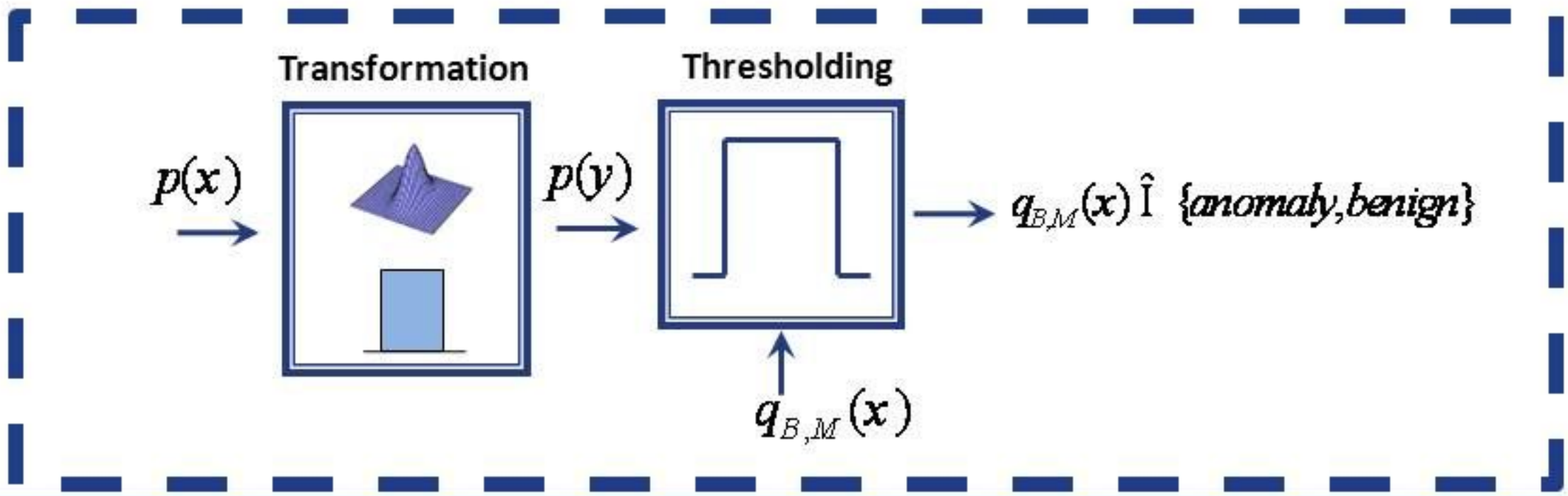
“The attacker has *full knowledge* of the workings of the system.”

Modeling IDS detection as an Information Channel Coding problem

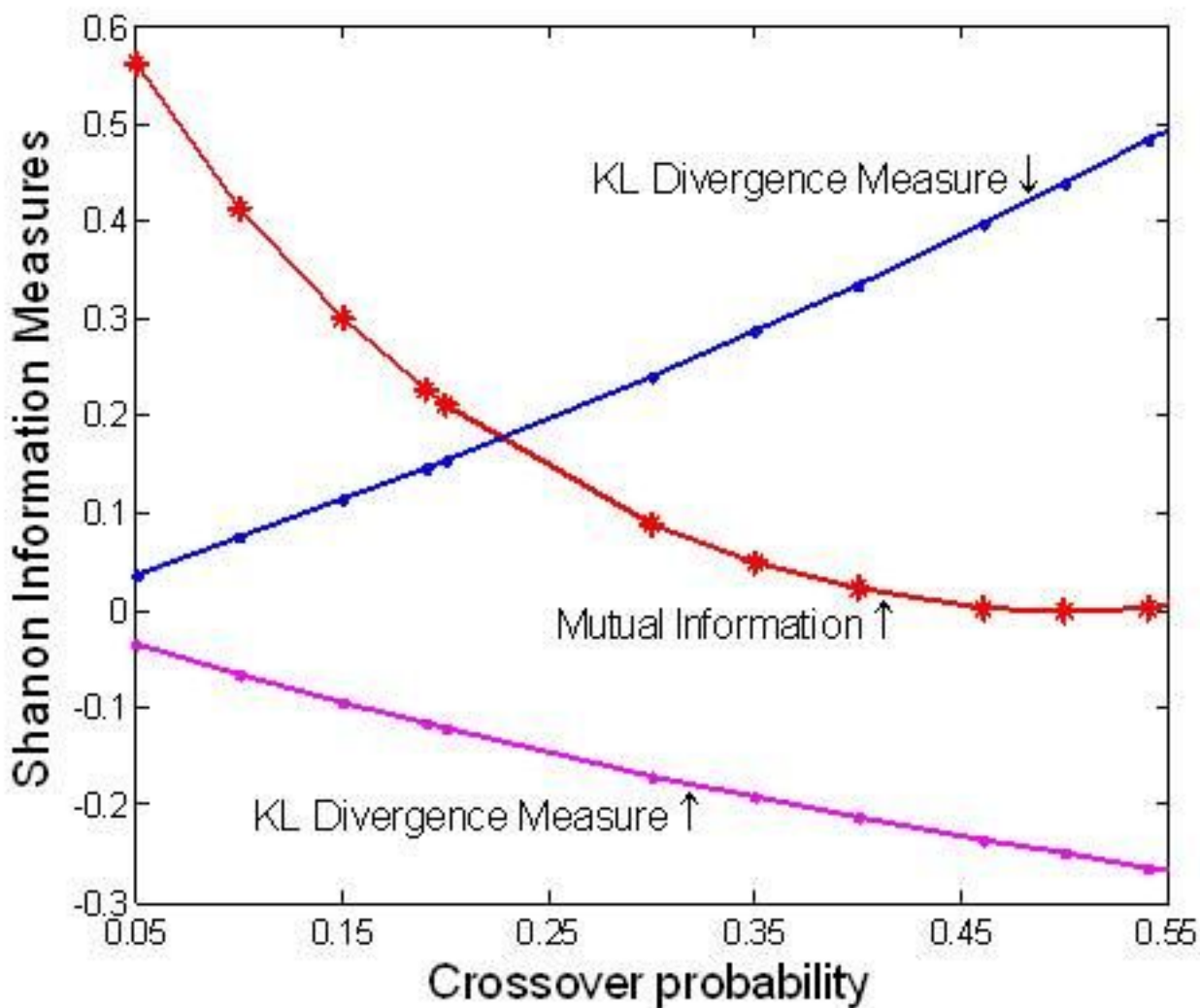


Channel Transition Matrix

$$p(\mathbf{y} / \mathbf{x}) = \begin{pmatrix} p(y_0 / x_0) & p(y_1 / x_0) & \dots & p(y_{|\mathcal{Y}|-1} / x_0) \\ p(y_0 / x_1) & p(y_1 / x_1) & \dots & p(y_{|\mathcal{Y}|-1} / x_1) \\ \vdots & \vdots & \ddots & \vdots \\ p(y_0 / x_{|\mathcal{X}|-1}) & p(y_1 / x_{|\mathcal{X}|-1}) & \dots & p(y_{|\mathcal{Y}|-1} / x_{|\mathcal{X}|-1}) \end{pmatrix}$$



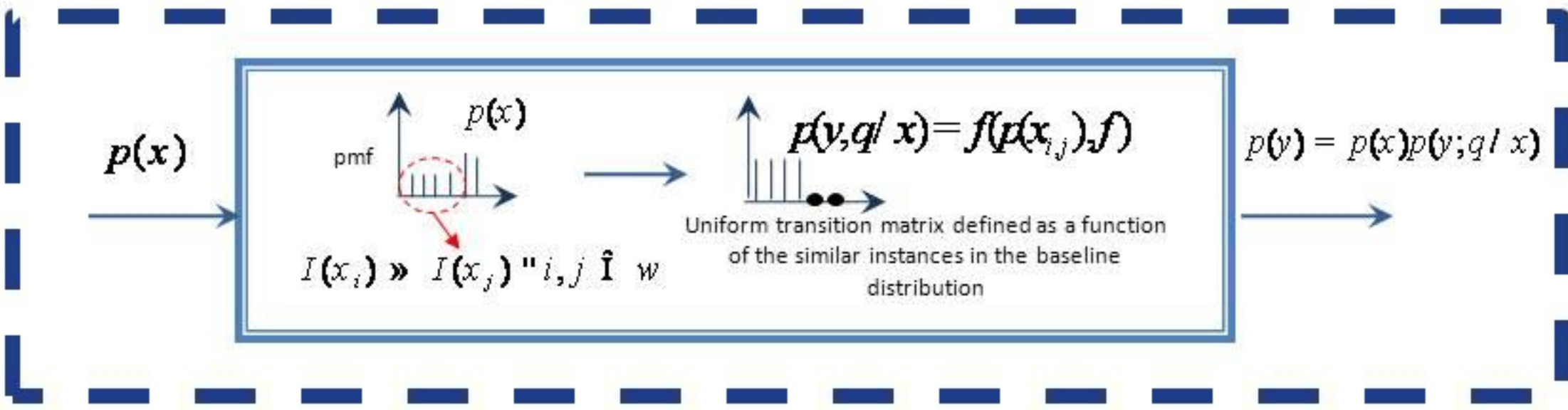
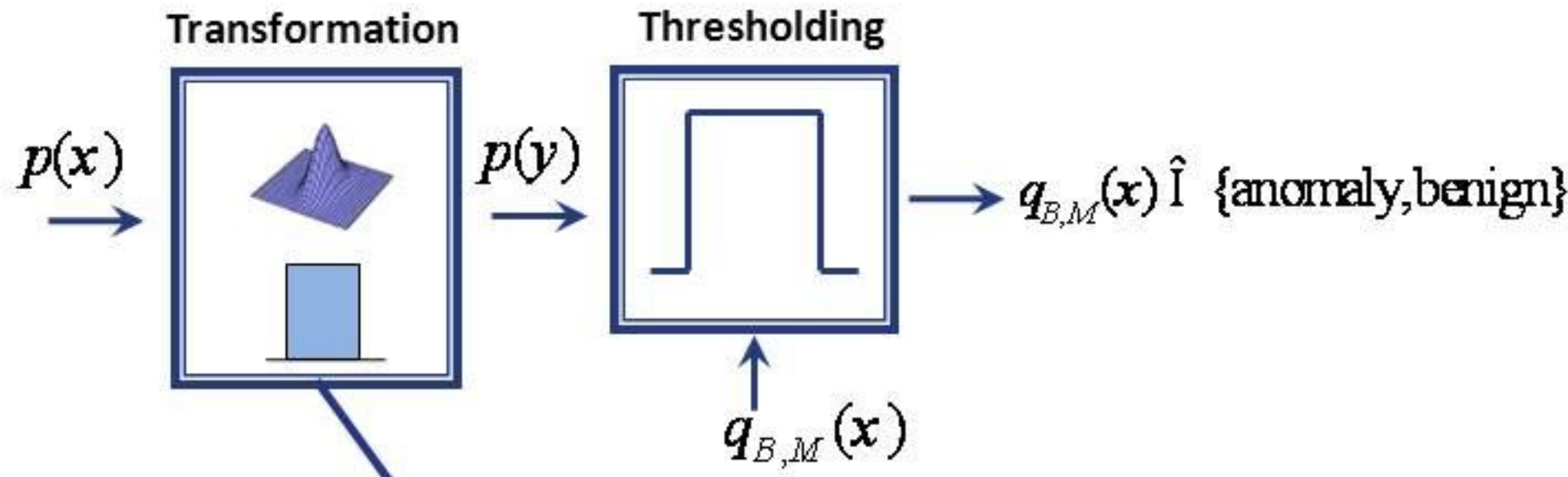
Modeling IDS detection as a Information Channel Coding problem



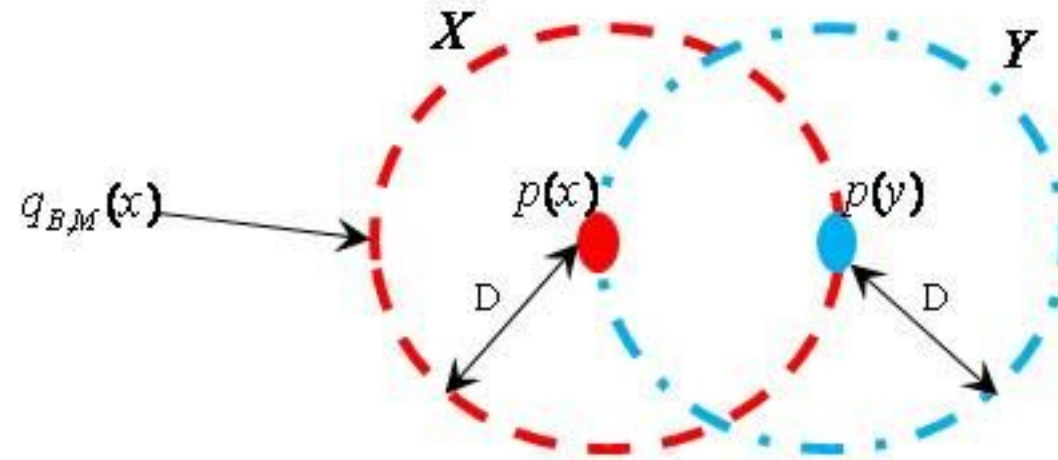
Minimizing the mutual information between input $p(x)$ and the output $p(y)$

$$\min_{p(y; q | x)} I(X; Y) = \min_{p(y; q | x)} \sum_{x \in X} \sum_{y \in Y} p(x, y) \log_2 \frac{p(y; q | x)}{p(y)} = \sum_{x, y \in W} p(x, y) \log_2 \frac{p(y; q | x)}{p(x) p(y; q | x)}$$

Modeling IDS detection as an Information Source Coding problem



Modeling IDS detection as an Information Source Coding problem



Intrusion detection on the non-overlapping boundary region between $p(x)$ & $p(y)$:

$$D(p(x) || q_{B,M}(x)) \gg D \text{ \& } D(p(y) || q_{B,M}(x)) \gg 2D.$$

Intrusion detection on the overlapping boundary region between $p(x)$ & $p(y)$:

$$D(p(x) || q_{B,M}(x)) \gg D \text{ \& } D(p(y) || q_{B,M}(x)) \ll D \text{ \& } 0.$$

Benign traffic window:

$$D(p(x) || q_B(x)) \ll D \text{ \& } D(p(y) || q_B(x)) \hat{=} \{(< 2D \zeta > D)\hat{=} \gg D\}.$$

Thank you!

- Contact Information:
 - Email: ali.khayam@seecs.nust.edu.pk
 - Web: <http://wisnet.seecs.nust.edu.pk>