A Queuing Formulation of Intrusion Detection with Active and Passive Responses

Wei T. Yue, Metin Cakanyildirim, Young U. Ryu

Department of Information Systems and Operations Management

School of Management

The University of Texas at Dallas

Richardson, Texas 75083-0688, USA

Introduction

- Traditional IDS response tends to be passive – “passive response”
- Secondary investigation required because IDS is still imperfect
- Secondary investigation may not occur instantaneously
- These days, IDS can be set up to respond to events automatically – “active response”

Introduction

- Active response – dropping connection, reconfiguring networking devices (firewalls, routers), additional intelligence mining (honeypots)
- We only consider terminating connection

Introduction

- In the intrusion detection process, IDS configuration decision and the alarm investigation decision are related
- Alarm investigation resource would affect the delays in response in both active and passive response
- If multiple alarm types involved, which alarm to investigate is an issue

Research Goals

- Finding the corresponding configuration and investigation decision for the active and passive response approach
- Determine the “switching” policy on intrusion response

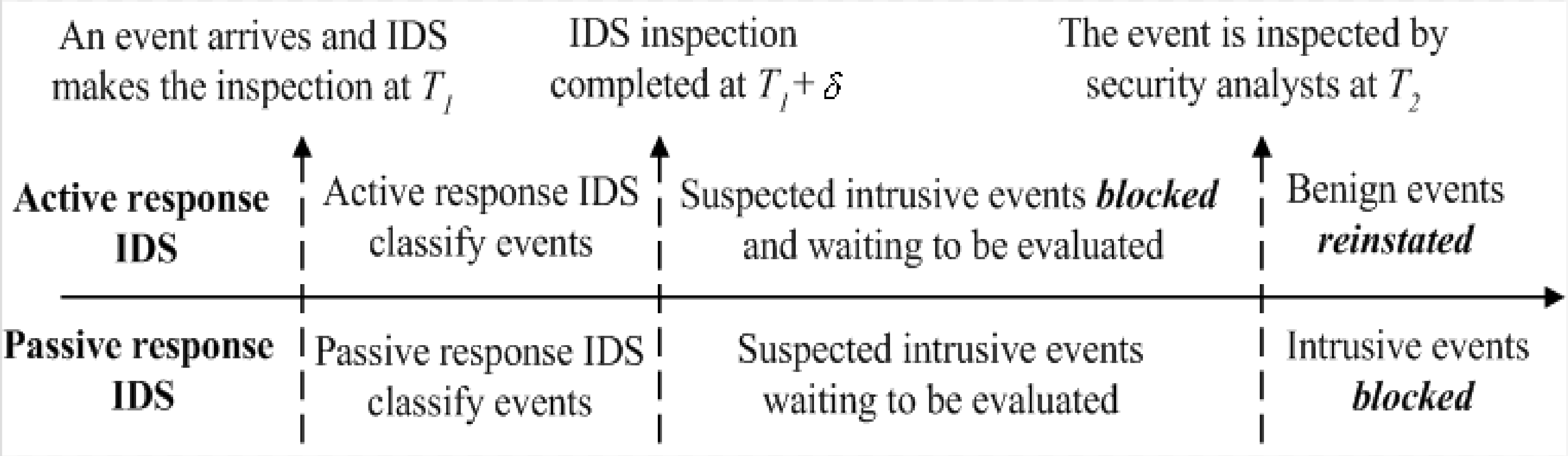
Problem Description

- Passive response
  - potential damage cost - resulting from alarmed events not investigated immediately
  - low false alarm costs since alarmed events are not disrupted

Problem Description

- Active response
  - It could prevent attack damage because the events are terminated immediately
  - higher false alarm costs contingent on the performance of the IDS

Problem Description



- Active response: false alarm cost is related to delay
- Passive response: damage cost is related to delay

Problem Description

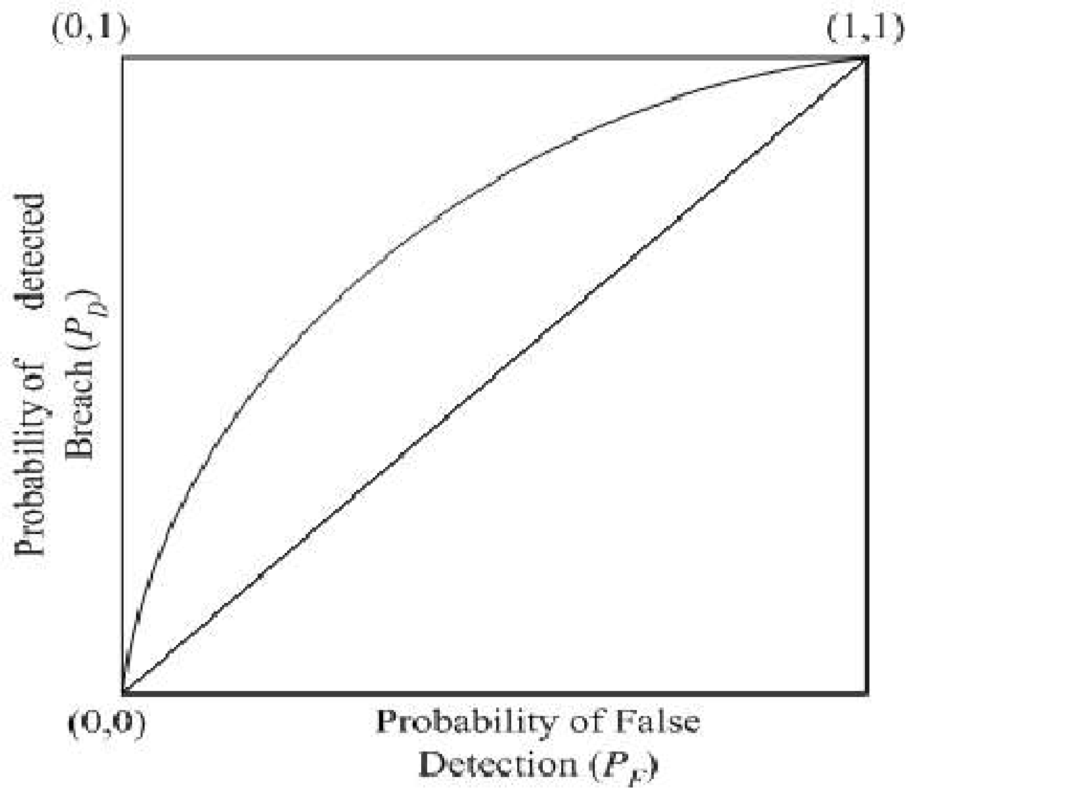
- Undetected, or non-alarmed intrusive events are assumed to be the same for the two response approach

- Given the parameter values, the decisions involved with the active and passive response approaches are different

IDS Quality: ROC curve

- A representation of IDS quality – detection rates ($\Omega(P_F)$) and false alarm rate (P_F)
- IDS quality can be determined experimentally – MIT Lincoln Lab (Lippman et al 2000a 200b), Columbia IDS group (Lee and Stolfo, 2000), etc

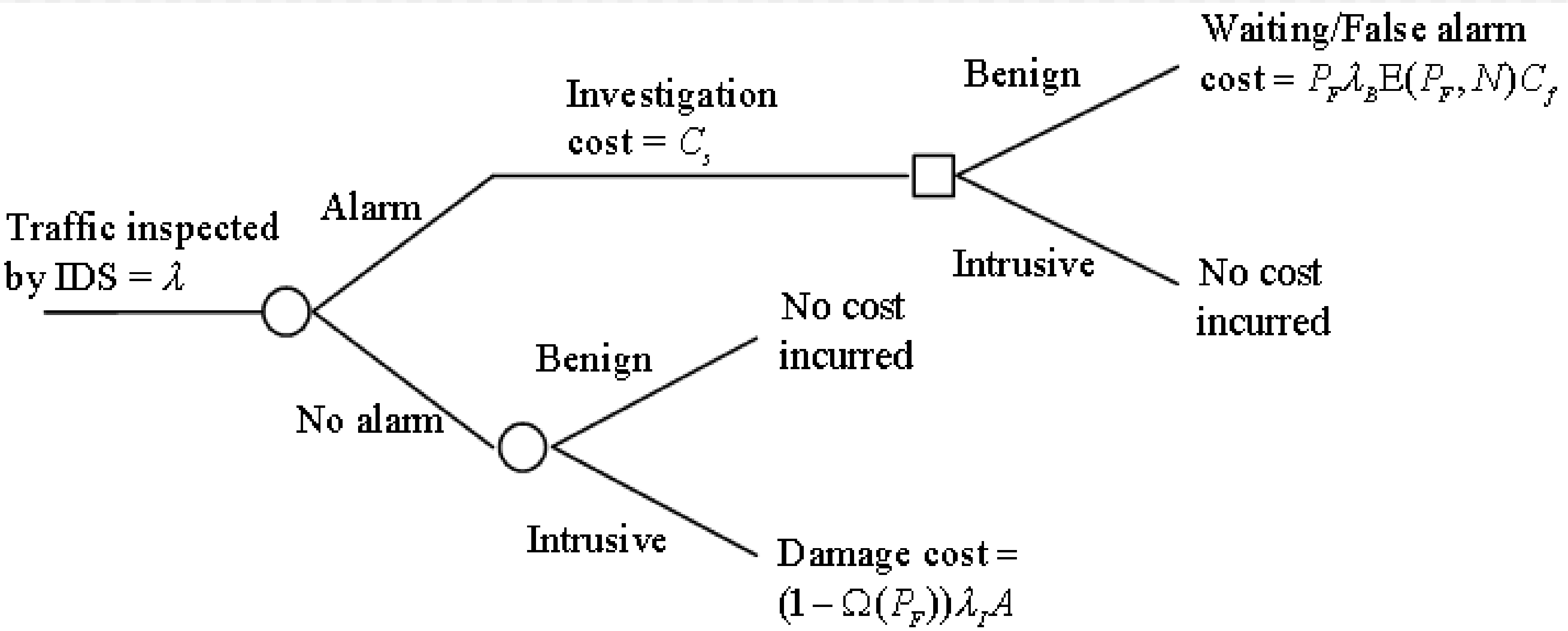
IDS Quality: ROC curve



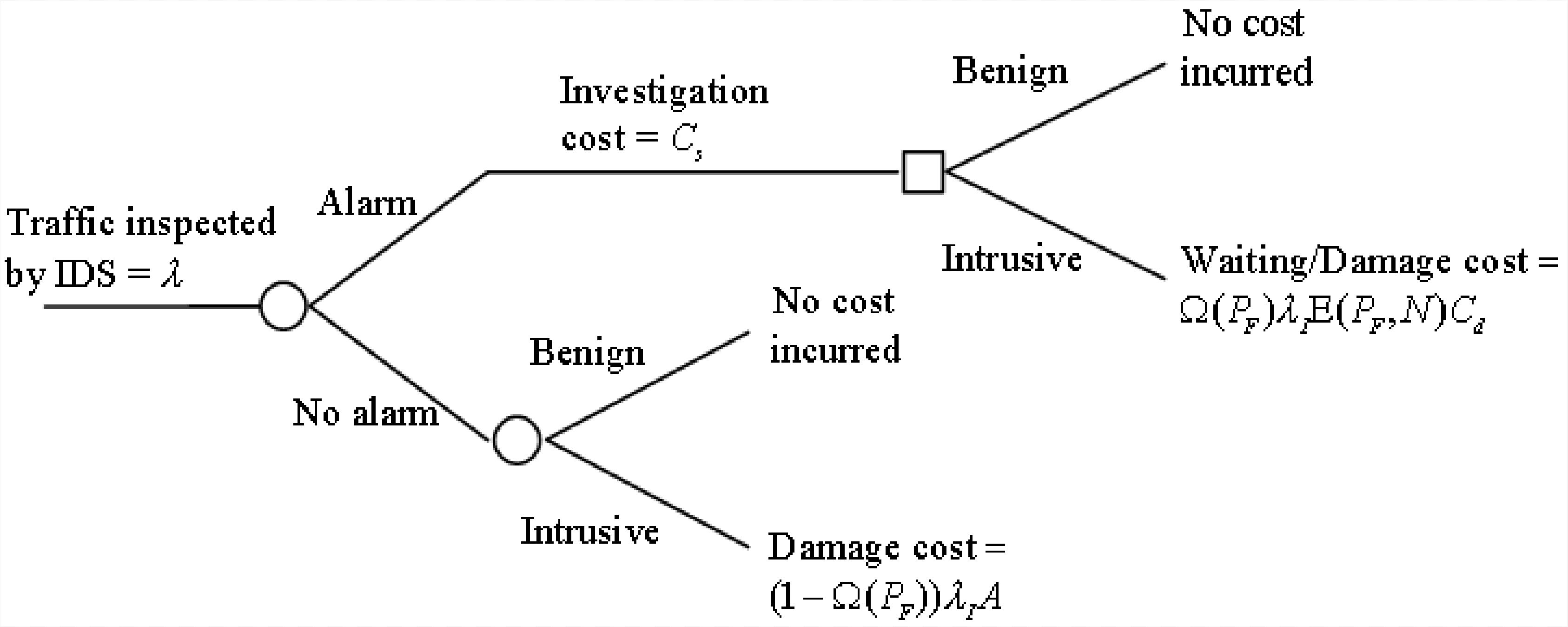
A Queuing Model of Intrusion Detection

- Benign and intrusive event arrivals – Independent Poisson process with rate λ_B and λ_I
- N – number of investigator
- μ - investigation rate
- $E(W(P_F, N)) = 1/\{N\mu - P_F\lambda_B - \Omega(P_F)\lambda_I\}$

A Queuing Model of Intrusion Detection: Active Response



A Queuing Model of Intrusion Detection: Passive Response



A Queuing Model of Intrusion Detection

Active Response

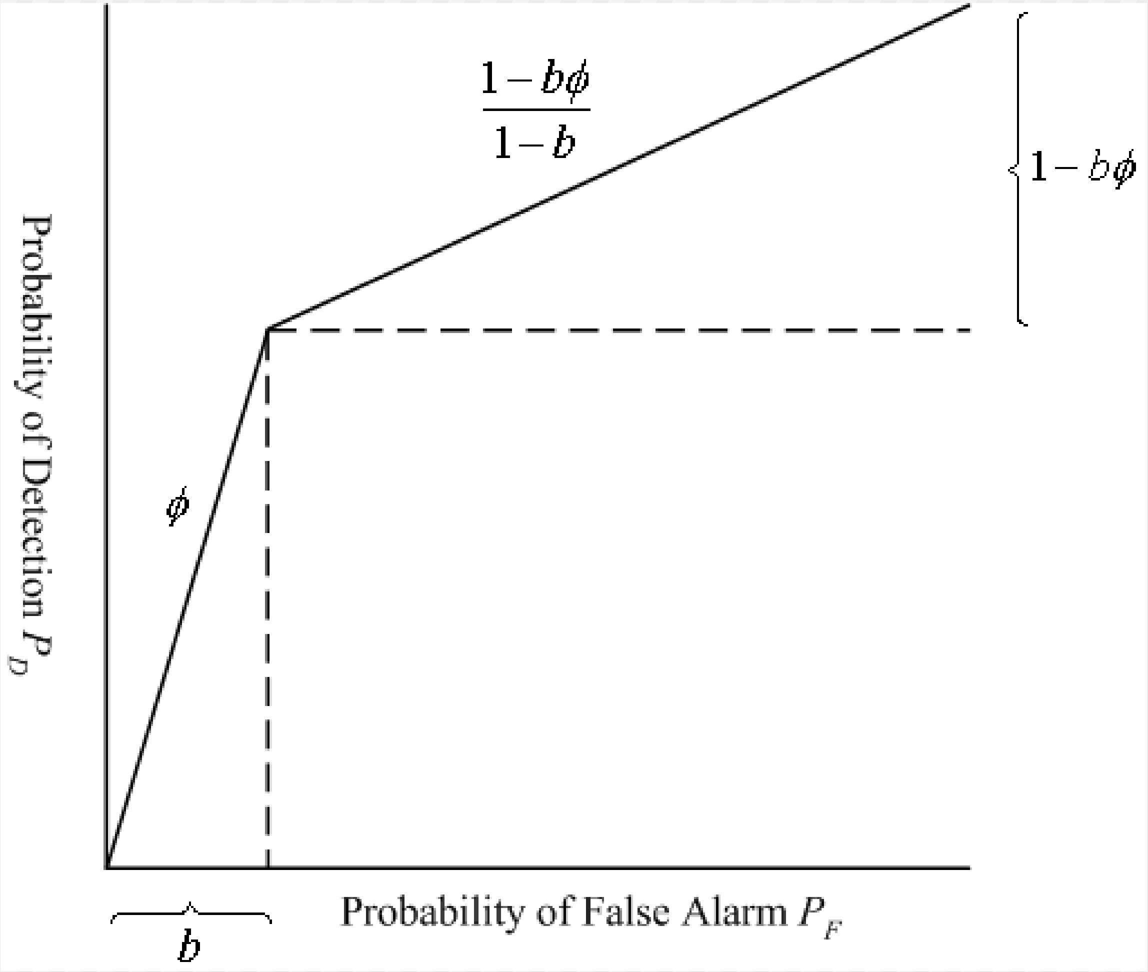
$$\min_{\substack{0 \le P_F \le 1 \\ N \ge 0}} P_F \lambda_B E(W(P_F, N)) C_f + (1 - \Omega(P_F)) \lambda_I A + N C_s$$

Passive Response

$$\min_{\substack{0 \le P_F \le 1 \\ N \ge 0}} \Omega(P_F) \lambda_I E(W(P_F, N)) C_d + (1 - \Omega(P_F)) \lambda_I A + N C_s$$

- We rewrite the N in terms of slack service rate S
  - $S = \mu N - P_F \lambda_B - \Omega(P_F) \lambda_I$

Linear Piecewise ROC



Optimal Configuration and Investigation

$$\Omega_P(P_F) = \begin{cases} \phi P_F & \text{if } P_F \leq b \\ b\phi + \frac{(1-b\phi)}{(1-b)}(P_F - b) & \text{if } P_F \geq b \end{cases}$$

$$S_A^*(P_F) = \left(\frac{\mu\lambda_B C_f}{C_s}\right)^{1/2} (P_{A,F})^{1/2}$$

$$S_P^*(P_F) = \left(\frac{\mu\lambda_I C_d}{C_s}\right)^{1/2} [\Omega(P_{P,F})]^{1/2}$$

Hybrid Response

Active (P_F, P_D)	Passive (P_F, P_D)	$TC_A > TC_P$ Conditions
$b, b\phi$	$b, b\phi$	$\lambda_B C_f \geq \phi \lambda_I C_d$ **I**
$b, b\phi$	1,1	$(1-b\phi)\lambda_I A\mu - C_s[\lambda - \lambda_B b - \lambda_I b\phi] \geq 2\sqrt{C_s\mu}\left[\sqrt{C_d\lambda_I} - \sqrt{C_f\lambda_B b}\,\right]$ **II**
1,1	$b, b\phi$	$(1-b\phi)\lambda_I A\mu - C_s[\lambda - \lambda_B b - \lambda_I b\phi] \leq 2\sqrt{C_s\mu}\left[\sqrt{C_f\lambda_B} - \sqrt{C_d\lambda_I b\phi}\,\right]$ **III**
1,1	1,1	$\lambda_B C_f \geq \lambda_I C_d$ **IV**

Hybrid Response

Active P_F, P_D	Passive P_F, P_D	$\lambda_B C_f \leq \lambda_I C_d$	$\lambda_I C_d \leq \lambda_B C_f \leq \phi \lambda_I C_d$	$\lambda_B C_f \geq \phi \lambda_I C_d$
$b, b\phi$	$b, b\phi$	Active **I**	Active **I**	Passive **I**
$b, b\phi$	1,1	Passive	Passive **II**	Passive
1,1	$b, b\phi$	Passive **III**	Passive **III**	Passive
1,1	1,1	Active **IV**	Passive **IV**	Passive **IV**

Conclusion

- Derive optimal intrusion detection decisions with linear piecewise function
- Extend the study with other types of ROC functions
- Include multiple types of alarm