Qualitative Assessment of Significance of Intrusion Detection in Cyber Resilience

BY :

SAURABH ARORA

DHARAMENDRA KUMAR

Background

- Cyber Resilience: **ability of a system to anticipate, continue to operate correctly in the face of, and recover from cyber infections**

- Resilience response mechanism:

  a) *Intrusion detection*

  b) *Host reset*

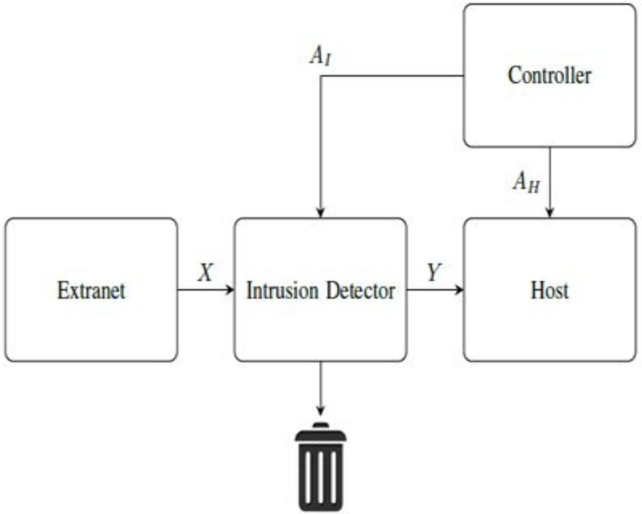
System Input, Controller, and Detection Output

Controller designates actions for two separate components of resilience system:

1. Host capable of resetting itself
2. IDS capable of inspecting and dropping messages

Terminologies:

1. x = message's infection capacity, {benign, malicious}
2. y = output of IDS, {benign, null, malicious}
3. a_i = action for IDS component
4. a_h = action for HOST component
5. λ **= probability of malicious input message**



Intrusion Detection and Response System

TARGET of Project

- Implementing IDS-host system MDP using graph-defined domains in BURLAP java code library
- Implementing three designs using MDP:
  - system without message interception (inspection and filtering) and host reset
  - system with message interception (classification) but without host reset
  - system with both capabilities
- Establishing the significance of interception of malicious messages by using expected utilities (optimal state value)
- Graphical demonstration

IDS State, IDS Action

State as per paper

$$b \in B = \{\text{idle}, \text{busy}\}$$

Action

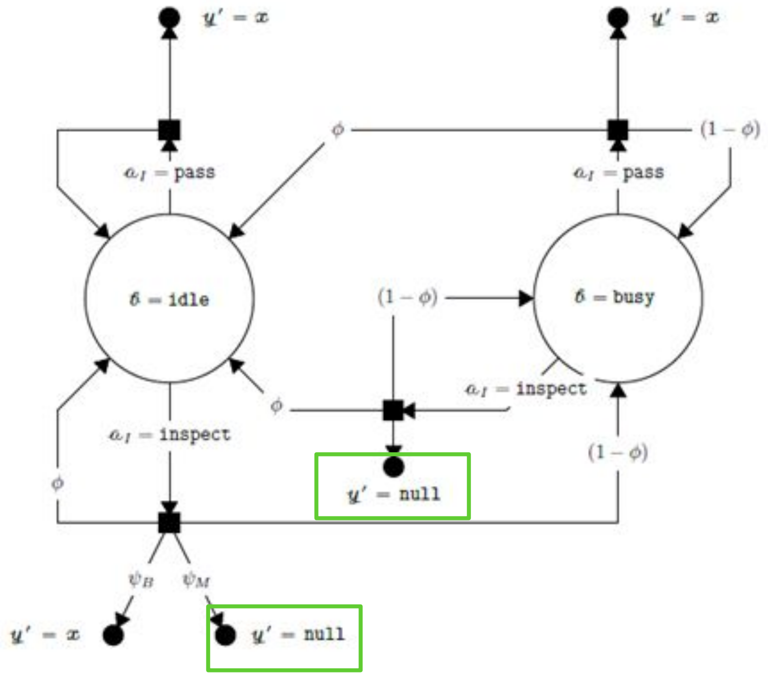
$$a_i \in A_I = \{\text{inspect}, \text{pass}\}$$

state in code implementation:

$$s_i = (x, b, y) \in X \times B \times Y$$

<u>inspect action</u> identifies and **intercepts malicious** messages before they reach the host system

(x1=**malicious**, b1, y1) **-- inspect** → (x2, b2, y2=**null**)



Intrusion detector state transition diagram (ϕ, ψ parameters decide transition probabilities)

Host state, Host action

State $(w, h) \in W \times H$

where W = {full, reset}, H = {clean, infected}.

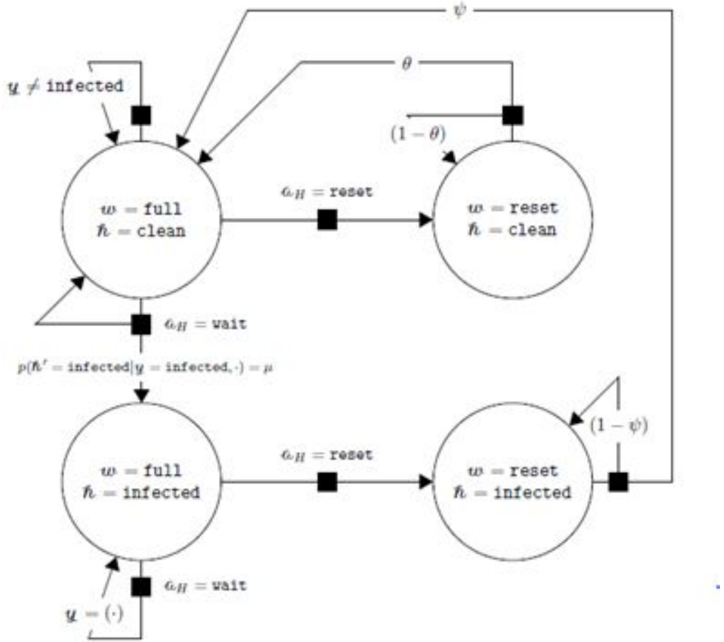
full = the host is capable of fully processing incomin messages, reset = the host is repaired if it was previously infected

State in code implementation:

$$s_h = (y, w, h) \in Y \times W \times H$$

Action $a_h \in A_H$={wait, reset}

μ **= probability of resisting a malicious message**



Host state transition diagram (θ, ψ, μ parameters decide transition probabilities)

Product of Two Component Spaces, Action-Sets, and Transitions

state of IDS-host combined system is the state where output y is same in both IDS state $s_i = (x, b, y) \in X \times B \times Y$ and host state $s_h = (y, w, h) \in Y \times W \times H$

s = (y, x, w, h, b) $\in S = Y \times X \times W \times H \times B$

action of combined system is a = $(a_i, a_h) \in A_I \times A_H$

transition probability of IDS-host system is :

$$P(s'|s, a) = P(y'|x, b, a_i)P(x')P(w', h'|w, h, y, a_h)P(b'|b, a_i)$$

Reward Structure

- Reward is based only on the state of host.
- It is parameterised for preferring
  - the state in which IDS intercepted malicious message before it reaches the host.
  - the state in which host resets itself after infection

W	H	Y	R
full	clean	benign	1.0
full	clean	null	$1.0 + \alpha\rho_+$
full	clean	malicious	$1.0 + \alpha\rho_-$
full	infected	benign, null, malicious	ρ
reset	clean, infected	benign, null, malicious	2ρ

Implementation of Product MDP Using BURLAP

- Motivation for using BURLAP is the availability of pre-made domains (data structure storing information about an MDP) for the systems representable using state transition graphs. IDS-host system is one of them.
- Individual domains are designed to IDS and host subsystems, with their respective states, actions, and transitions.
  - Specifications of IDS: 12 States, 2 Actions, 108 transitions;
  - Specifications of host: 12 States, 2 Actions, 21 transitions
- The domain for product MDP
  - product of states from IDS domain and host domain. The reward structure extends from host domain to IDS domains by implementation of the product of states.
  - transitions as the product of transitions of IDS domain and transitions of host domain.
- Specification for IDS-host MDP: 48 States, 4 Actions, 756 transitions

Designs for IDS-host system

- Baseline Sigma0 represents a system with no ability to either intercept malicious message (inspect) or reset if host becomes infected.
- Sigma 2 is the system with reset capable host but without inspection
- Sigma3 is the system with both the capabilities

	A_H	
A_I	{wait}	{wait, reset}
{pass}	Σ_0	Σ_2
{pass, inspect}		Σ_3

Significance of interception of malicious messages

λ **= probability of malicious input message**

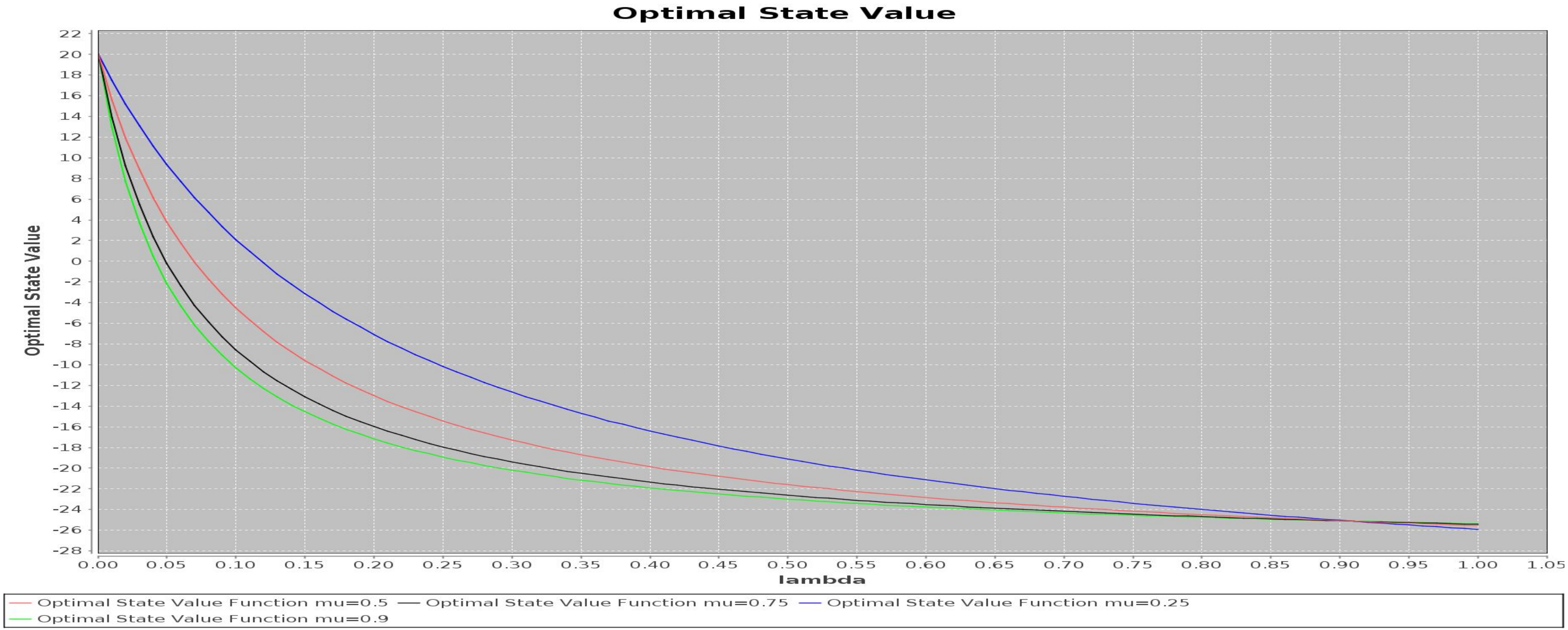
μ **= probability of resisting a malicious message**

Unit of Qualitative Comparison:

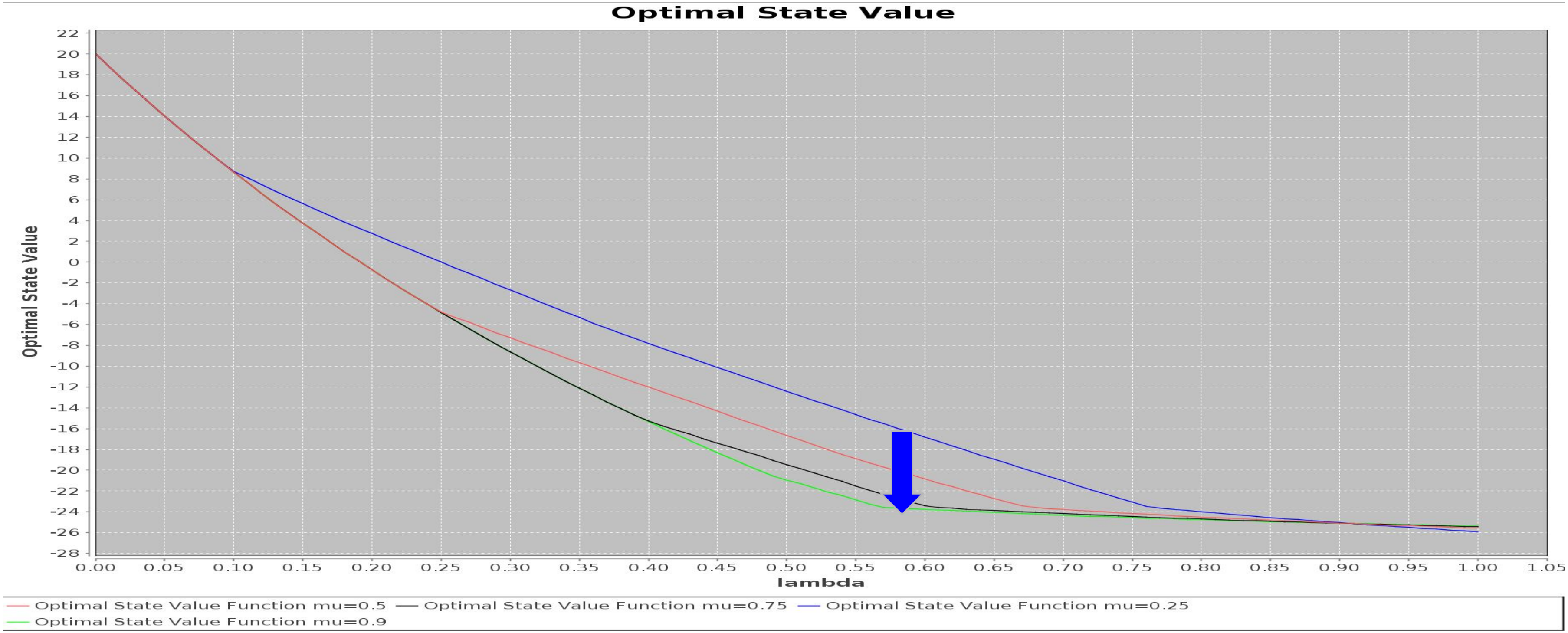
Variation in the expected utility (optimal state value) with the change in above two parameters demonstrates the degree of resilience against infection

	A_H	
A_I	{wait}	{wait, reset}
{pass}	Σ_0	Σ_2
{pass, inspect}		Σ_3

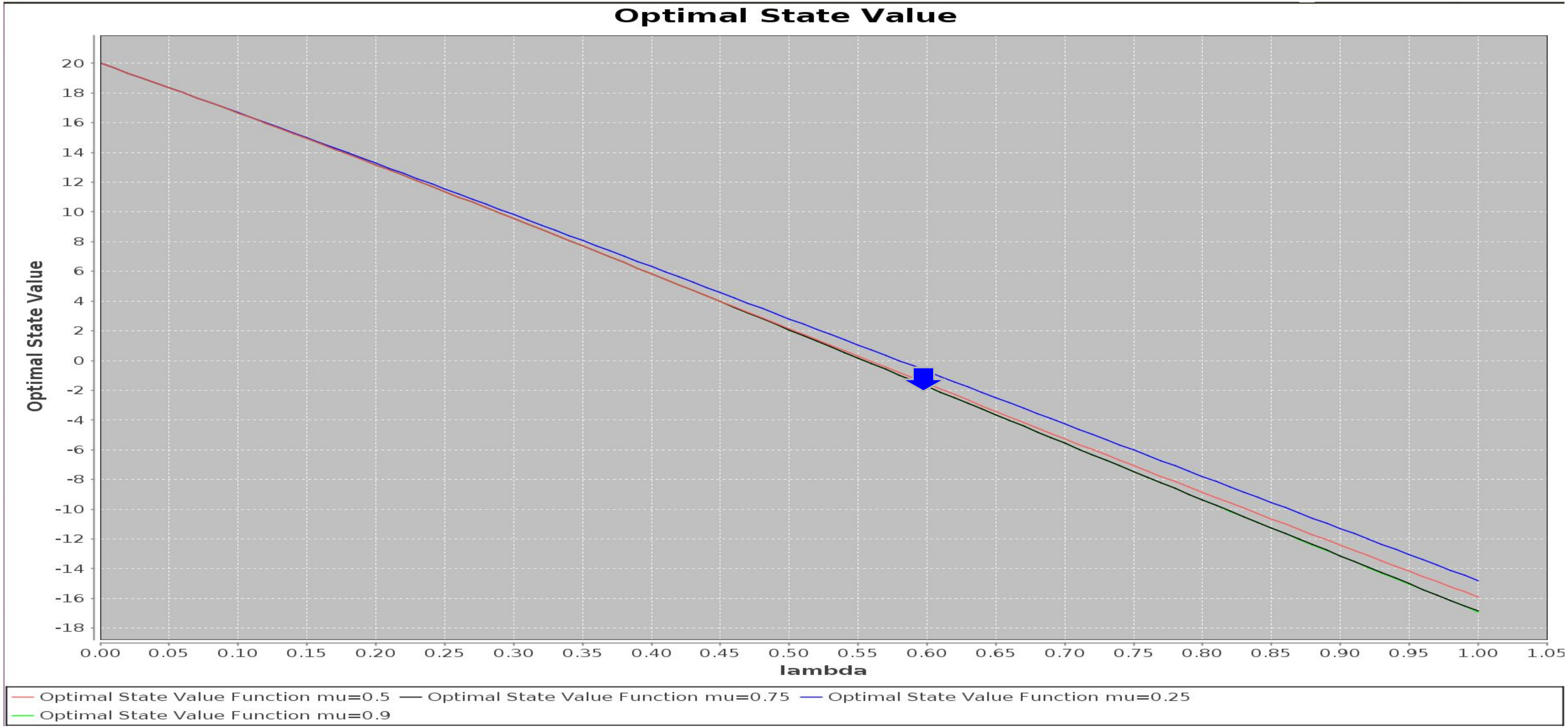
Extent of Utility Drop with Increase in Infection Sensitivity of host: System w/o Inspect and w/o Reset



Extent of Utility Drop with Increase in Infection Sensitivity of host: System with Reset but w/o Inspect



Extent of Utility Drop with Increase in Infection Sensitivity of host: System with Inspect and with Reset



Attempted Extension: Implementation of IDS as ML Classifier

- KDD'99 Data set - http://kdd.ics.uci.edu/databases/kddcup99/task.html
- Training data -
  - two classes {benign-message, malicious-message}
  - 4 GB of compressed binary TCP dump data from seven weeks of network traffic
- Random Forest classifier achieved 99.2 accuracy for predicting a message
- Probabilities of False Positive and False negative are computed.
- Bottleneck - Tuning the dataset to match the values of these probabilities in research paper.

Thank You