Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 70 (2015) 238 – 244

Procedia Computer Science

4th International Conference on Eco-friendly Computing and Communication Systems

# Online Monitoring of a Cyber Physical System against Control Aware Cyber Attacks

Hemangi Laxman Gawand[a], A. K. Bhattacharjee[b], Kallol Roy[a.b]

[a]*Homi Bhabha National Institute, BARC, India, (hemangi.gawand@gmail.com),* [b] *Reactor Control Division, BARC, India, (anup@barc.gov.in),* [b2]*Research Reactor Maintenance Division, BARC, India, (kallolr@barc.gov.in)*

**Abstract**

In various industrial plants like power and chemical plants, the system operation is controlled by embedded controller(s). Any intentional malfunction of a critical controller can lead to shut down or failure of vital parts. It further leads the control plant into unsafe mode. Malware attacks can result in tremendous cost to the organization in terms of cleanup activity. Process related threats occur when the attacker gains control of the system and performs unintended actions. Industrial plants being a complex system need a wholesome approach for attack detection and prevention. In this paper we propose to use a geometric method to detect anomaly in a control system behavior which can possibly indicate a malware attack.
The paper focuses on analysis of the large data sets for anomaly detection by using computational geometric methods to observe and analyze trends in the controller's output.


Peer-review under responsibility of the Organizing Committee of ICECCS 2015

*Keywords:* Cyber physical systems (CPS), Convexity, Least Square Approximation (LSA), Data stream analysis, real-time control system, Sequential Probability Ratio test (SPRT), Cumulative Sum (CUSUM), Security.

## 1. Introduction

There have been an increasing number of malware attacks on the industrial control systems like Stuxnet in 2010 [1], Maroochy Shire Sewage attack in 2000[1], water filtering plant of Pennsylvania in 2006 and Davis-Besse power plant in Oak Harbor, Ohio in 2003[2]. Increasing vulnerabilities in the cyber physical system have made information security an immediate concern and need for detecting and controlling the spread of such malware. Information security methods like authentication and integrity are inadequate in securing these control systems. Attacks on control system can result in tremendous costs to an organization in rebuild and recovery activities.


Peer-review under responsibility of the Organizing Committee of ICECCS 2015
doi:10.1016/j.procs.2015.10.079

Cyber-Physical System (CPS) is integrations of computation with the physical processes. Control systems automate the tasks once performed by the humans by sensing the environmental conditions, executing the programmed logic and then actuating physical equipment to perform a desire task. Control systems are made up of sensors along with computational and communication capabilities. Data received by the actuator causes necessary action(s) on the physical system. Sensors measure the physical system states and transmit it to the distributed controllers. A control action is a reactive process and failure of any non-redundant sensor or actuator can cause irreparable damage to the system under control.

Statistical techniques like SPRT are useful in the malware detection as mentioned in [1, 2, and 4]. In a cyber-physical system like SCADA, data is collected in the form of bug reports and system status logs. These data can provide the vital historic information for understanding system behavior and its trends. However, these files are huge in size and difficult to inspect manually.

The paper focuses on using computational geometric techniques for understanding the controller profile to detect anomalous behavior. The paper is organized as follows: Section 2 provides a brief review of related work. Section 3 presents mathematical framework for vulnerability analysis. Section 4 explains computational geometry and its implications on control system using four tank model. Section 5 concludes with future scope.

## 2. Related Work

Alvaro et. al. in [1, 2, 12, and 14] have explained the need to secure CPS using the example of Stuxnet attack and have demonstrated various attacks on Tennessee-Eastman process control system model. They have used statistical techniques for attack models analysis. Various attacks like bias attack, geometric attack, stealth attacks are explained in [1]. M. Basseville's [3, 7] statistical techniques for fault detection were extended for analysis of false data injection attack (Yao Liu [16]) using four tank model by Hemangi et. al. [4,26]. Shyamasundar in [17] has described a big data approach for protecting and securing SCADA from malware attacks and analyzing data log files generated through SCADA system. Various methods exist for the analysis of data log such as sampling method [6], statistical method [3, 7, and 14] and continuous query of data stream [8, 9]. Izchak Sharfman [5] describes various search engines with different mirrors (filters) for data monitoring. Computational geometric approach has been used for analysis of large data stream by Fabio Pasqualetti et. al. [13, 14].

## 3. Mathematical Framework And Vulnerability Analysis For CPS

Cyber physical system plays the vital roles of controlling as well as monitoring critical physical processes. CPS is made of hierarchy of computer elements running a discretized control algorithm and is connected to sensors and control elements. Controller acts as the heart of a control system. Control system is represented in LTI model as given by Equation (1) and (2) [27].

$$x(k+1)= Ax(k) + Bu(k)+w_k \quad (1)$$

$$y(k)= Cx(k)+v_k \quad (2)$$

Where $x(k) \in R^n$, $y(k) \in R$, $A \in R^{nxn}$, $B \in R^{nxm}$ and $C \in R^{pxm}$.

An attack that causes the state matrix 'A' to change is termed as state attack and an output attack when measurement vector is targeted. Attacks on CPS are broadly classified as targeted and non- targeted. Targeted Attacks are further classified into:-

1. Input Data Attacks: Control Signal is targeted which results in a state change of the system.
2. Output Data Attacks: Measurement signal is targeted.
3. State Attacks: Attacker tries to manipulate any of the factors that affect the states of the system.