Accepted Manuscript

Securing Cyber Physical System in Nuclear Power Plants Using LSA and Computational Geometric Approach

Hemangi. Laxman. Gawand, A.K. Bhattacharjee, Kallol Roy

PII: S1738-5733(16)30288-1

DOI: 10.1016/j.net.2016.10.009

Reference: NET 281

To appear in: *Nuclear Engineering and Technology*

Received Date: 25 June 2016

Revised Date: 29 September 2016

Accepted Date: 17 October 2016

Please cite this article as: H.L. Gawand, A.K. Bhattacharjee, K. Roy, Securing Cyber Physical System in Nuclear Power Plants Using LSA and Computational Geometric Approach, *Nuclear Engineering and Technology* (2016), doi: 10.1016/j.net.2016.10.009.

Securing Cyber Physical System in Nuclear Power Plants Using LSA and Computational Geometric Approach

Hemangi. Laxman. Gawand *, A. K. Bhattacharjee **, Kallol Roy ***

**Homi Bhabha National Institute, BARC, India, (hemangi.gawand@gmail.com),*

*** Reactor Control Division, BARC, India, (anup@barc.gov.in),*

****BHAVINI, India, (kallol.roykallol@gmail.com)*

Abstract:

In industrial plants such as Nuclear Power Plants, system operations are performed by embedded controllers orchestrated by Supervisory Control and Data Acquisition Software (SCADA). A targeted attack (also termed a control aware attack) on the controller/SCADA software can lead a control system to operate in an unsafe mode or sometimes to complete shutdown of the plant. Such malware attacks can result in tremendous cost to the organization for recovery, cleanup, and maintenance activity. SCADA systems in operational mode generate huge log files. These files are useful in analysis of the plant behavior and diagnostics during an ongoing attack. However, they are bulky and difficult for manual inspection. Data mining techniques such as Least Square Approximation (LSA) and computational methods can be used in the analysis of logs and to take proactive actions when required.

This paper explores methodologies and algorithms so as to develop an effective monitoring scheme against control aware cyber attacks. It also explains soft computation techniques such as the computational geometric method and LSA that can be effective in monitor design. This paper provides insights into diagnostic x`monitoring for its effectiveness by attack simulations on a four tank model and using computation techniques to diagnosis it. Cyber Security of I&C systems used in NPPs are of paramount importance and hence could be a possible target of such applications.

Keywords: Cyber physical systems (CPS), Convexity, Computational Geometry, Least Square Approximation (LSA), DataStream analysis, Nuclear Power Plant (NPP), real-time control system, Sequential Probability Ratio test (SPRT), Cumulative Sum (CUSUM), and Security.

1. Introduction

Cyber physical systems (CPS) are a diverse group of systems used to physically manipulate and monitor critical infrastructures such as industrial systems, power and water systems, security systems, etc. A NPP's Instrumentation and Control Systems (I&C) deploy a number of control systems that orchestrate safe and viable control of the neutronics, its control process, and electrical subsystems, realizing the overall plant control system.

There have been an increasing number of attacks from malware on industrial control systems such as Stuxnet in 2010. The biggest threat to CPS is from the targeted attacks where the attackers have deep knowledge of the targeted controller and various processes controlled by it.

Network based anomaly detection techniques are not enough to detect attacks on control systems as the access may be through a genuine access point but with the intent to change the behavior of the control loop. The latest information security tools alone are not sufficient for securing control systems. Securing the control system from possible targeted attacks on its computational elements requires a thorough diagnosis of its behavior against accepted normal behavior. Such diagnostics can be performed by a