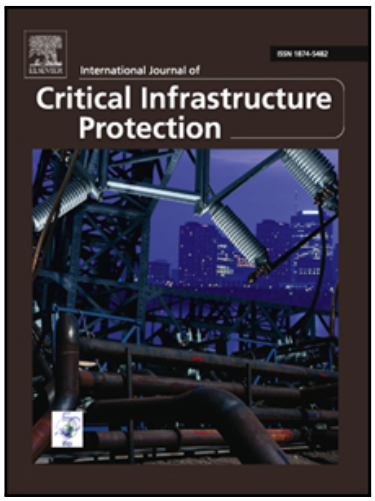

SIDS: State-based Intrusion Detection for Stage-based Cyber Physical Systems

Abdullah Khalili , Ashkan Sami , Amin Khozaei , Saber Pouresmaeeli

PII: S1874-5482(16)30044-0
DOI: 10.1016/j.ijcip.2018.06.003
Reference: IJCIP 256

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 9 April 2016
Revised date: 29 May 2017
Accepted date: 17 June 2018

Please cite this article as: Abdullah Khalili , Ashkan Sami , Amin Khozaei , Saber Pouresmaeeli , SIDS: State-based Intrusion Detection for Stage-based Cyber Physical Systems, *International Journal of Critical Infrastructure Protection* (2018), doi: 10.1016/j.ijcip.2018.06.003

SIDS: State-based Intrusion Detection for Stage-based Cyber Physical Systems

Abdullah Khalili[#,a], Ashkan Sami[*,b], Amin Khozaei[*,c], and Saber Pouresmaeeli[+,d]

Department of Electrical and Computer Engineering, University of Hormozgan, Bandar Abbas 3995; Iran

* Department of Computer Science and Engineering and IT, School of Electrical Engineering and Computer, Shiraz University, Shiraz 71348 - 51154; Iran

+ Department of Power and Control Engineering, School of Electrical Engineering and Computer, Shiraz University, Shiraz 71348 - 51154; Iran

[a] Email: khalili@hormozgan.ac.ir

[b] Email: sami@shirazu.ac.ir, Mobile: +989173142062, Fax and Tel: +987136133569 (Corresponding Author)

[c] Email: akhozaei@cse.shirazu.ac.ir

[d] Email: s.pouresmaeeli@gmail.com

Abstract

Attacks to Cyber Physical Systems (CPSs) are detected by Industrial Intrusion Detection Systems (IIDSs). Operation of stage-based CPSs (those that their underlying process is batch) consists of three parts: normal states, normal transitions between the normal states, and normal time-intervals for transitions. Unfortunately, state-of-the-art IIDSs directly address cyber-attacks that result in anomalous states whereas anomalous transitions or time-intervals can also indicate cyber-attacks. In this paper, a State-based IDS (SIDS) is proposed to detect all the three anomalies. For doing this, SIDS first automatically extracts the normal behavior of CPS. Then it monitors current CPS behavior and detects intrusions by directly looking at the data of field layer. A small-scale but real CPS (a mixer process) is provided to illustrate how SIDS works. In addition, experimental results on three cyber-attacks orchestrated on a simulated milk pasteurization process indicate that SIDS can successfully detect cyber-attacks to large I/O CPSs.

Keywords: Cyber Physical System (CPS), Industrial Control, Intrusion Detection System (IDS), Process Control, Security.

1. Introduction

Cyber Physical Systems (CPSs) control and monitor modern critical infrastructures such as oil and petrochemical industries, transportation systems, factories, and nuclear power plants. CPS consists of two main parts: physical and cyber part. Physical part is the underlying physical process controlled, engineered, and also monitored by the cyber part. In addition, cyber part makes the necessary communications between the different elements of CPS [1]. CPS is a general term used for many types of control systems such as Supervisory Control and Data