Future Generation Computer Systems 67 (2017) 57–71

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A method for evaluating the consequence propagation of security attacks in cyber–physical systems

Hamed Orojloo, Mohammad Abdollahi Azgomi *

Trustworthy Computing Laboratory, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran

HIGHLIGHTS

- A method for evaluating the consequence propagation of security attacks in cyber–physical systems is proposed.
- The method evaluates the direct and indirect impacts of attacks on control parameters of CPSs including sensor measurements and controller signals.
- The first output is ranking the important assets of the system based on their sensitivity to the carried out attacks.
- The next output is prioritizing the attacks based on their impacts on the behavior of the system.

ARTICLE INFO

Article history:
Received 5 March 2016
Received in revised form
31 May 2016
Accepted 19 July 2016
Available online 30 August 2016

Keywords:
Cyber–physical systems (CPSs)
Security evaluation
Physical dynamics
Consequence propagation

ABSTRACT

Estimating the possible impacts of security attacks on physical processes can help to rank the critical assets based on their sensitivity to performed attacks and predict their attractiveness from the attacker's point of view. To address this challenge, this paper proposes a new method for assessing the direct and indirect impacts of attacks on cyber–physical systems (CPSs). The proposed method studies the dynamic behavior of systems in normal situation and under security attacks and evaluates the consequence propagation of attacks. The inputs to the model are control parameters including sensor readings and controller signals. The output of the model is evaluating the consequence propagation of attacks, ranking the important assets of systems based on their sensitivity to conducted attacks, and prioritizing the attacks based on their impacts on the behavior of system. The validation phase of the proposed method is performed by modeling and evaluating the consequence propagation of attacks against a boiling water power plant (BWPP).

1. Introduction

The risk of disruptive interventions against critical infrastructures from various groups of adversaries has become increasingly high in recent years. Because attacks against critical infrastructure (CI) may have catastrophic impacts on the physical world and human lives [1], the security of critical infrastructure has become an active research area in recent years. Smart grids, water plants, chemical plants, oil and natural gas distribution systems and transportation systems are examples of critical infrastructures, which many people depend on [2].

Integrating computing and communication systems with physical world has led to the emergence of cyber–physical systems (CPSs). CPSs are computer-controlled systems monitoring and controlling physical processes [2]. These systems use a number of controllers such as programmable logic controllers (PLCs), communication equipment, sensors and actuators to manage and monitor some entities in the physical world [2].

As mentioned in [3], the modernization of critical infrastructures and emergence of CPSs are crucial to improve efficiency and flexibility, but, on the other hand, this integration and progress have subjected them to cyber threats. The security failures in CPSs can impact human lives and safety in general, and cause damage to industrial products and facilities [1]. According to the report released by the industrial control systems computer emergency readiness team (ICS-CERT) [4], the number of incidents related to the security breaches involving CPSs in 2012 was more than five times their 2010 level [5]. Thus, addressing the security of these systems has become an important topic in recent years.

One of the most important issues in addressing the security of CPSs is to study how the physical process is being controlled using control principles. The next important challenge is to

* Correspondence to: School of Computer Engineering, Iran University of Science and Technology, Hengam St., Resalat Sq., Tehran, 16846-13114, Iran. Fax: +98 21 73021480.

E-mail addresses: orojloo@iust.ac.ir (H. Orojloo), azgomi@iust.ac.ir (M.A. Azgomi).

http://dx.doi.org/10.1016/j.future.2016.07.016
0167-739X/

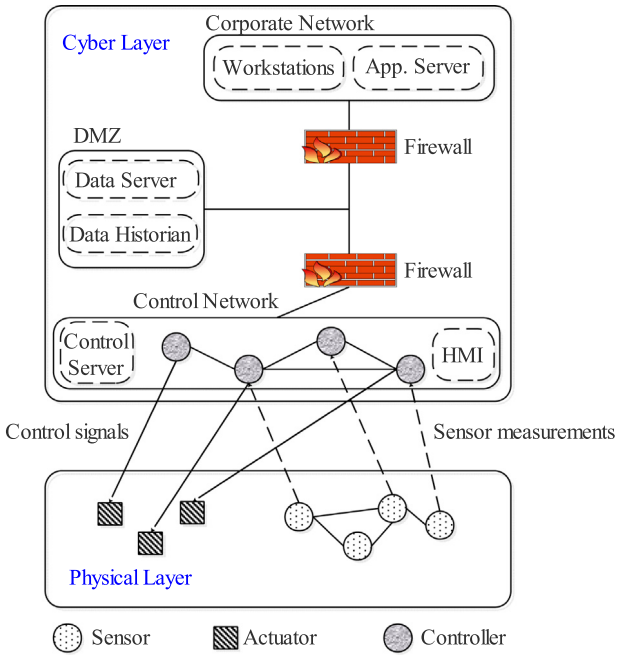

Fig. 1. The architecture of cyber–physical systems.

acquire sufficient understanding of the security requirements of the process under control. What puts the security of CPSs apart from the security of cyber systems is the concern for physical consequences of attacks [1]. It is desirable to determine the most vulnerable control parameters of these systems and analyze the sensitivity of their control loops.

To achieve this goal, in this paper we propose a new method that captures the dynamic behavior of CPSs with / without attacks and models the impact propagation of attacks. Finally, using the decision-making trial and evaluation laboratory (DEMATEL) [6,7] method, the proposed method ranks the critical assets of CPSs based on their sensitivity to disturbances and measures the direct and indirect consequences of attacks against them.

The DEMATEL method has been used for solving several groups of interdependent problems [8,9]. This method has been used in various contexts in recent years. For instance, it is applied to identify key success factors of hospital service quality [10], and to evaluate the causal relations among the criteria in auto spare parts industry [11].

DEMATEL is a comprehensive method used for building and analyzing a structural model involving causal relationships between complex factors [6,7]. This feature of the DEMATEL method is employed in this paper to evaluate and rank the impacts of intentional disturbances against the behavior of physical processes.

It is noteworthy that although we use the DEMATEL method for sensitivity analysis of control loops, the input data of the model are the control parameter values representing the dynamic behavior of the underlying physical process. In fact, in contrast to the traditional DEMATEL method, where the values of the parameters are assigned by system experts, in the proposed method, the impact evaluation of control parameters is performed according to the system dynamics.

In this paper, by considering sensor measurements and control signals as the primary target of disturbances, we study how an attack against system parameters can affect the values of other parameters. The normal behavior of the system without any disruptions and the abnormal behavior of the system under attacks are compared. The system parameters are divided into two classes of cause and effect parameters, which can be same as or different from each other. Finally, new metrics are proposed, which can be used for quantifying the importance level of each parameter in the underlying physical process. By using the resulting quantitative values, we can prioritize the sensor readings and control signals based on their sensitivity to conducted attacks. Besides, we can rank the performed attacks based on their direct and indirect consequences on physical dynamics of the system.

The rest of this paper is organized as follows. In Section 2, some related works are reviewed. In Section 3, we discuss about the architecture of CPSs and some important security issues of them. In Section 4, we present the formal and informal definitions of the proposed modeling and evaluating approach. In Section 5, an illustrative example is given. In Section 6, the proposed method is compared with other methods, and finally in Section 7, some concluding remarks are mentioned.

2. An overview of cyber–physical systems

In this section, we discuss about the overall architecture of CPSs and the security issues of them.

2.1. The architecture of cyber–physical systems

The current state of CPSs can be described by capturing the values of its important process variables. Two kinds of important process or state variables in CPSs include (1) measured variables representing the sensor measurements and (2) control variables representing the control signals [12]. The normal value of a certain process parameter is referred to as the set point. For example, the desired value of the pressure inside a tank in a chemical plant is called the set point of that process parameter [12].

In CPSs, the distance between the values of process variables and the corresponding set points is calculated by controllers. After calculating this offset, the controllers using a complex set of equations, elaborate a local actuation strategy, and calculate a new actuating or control variable. The resulting manipulated value is sent to the suitable actuator to keep the process closer to the determined set point [13]. The controllers also send the received measurements to main control servers and execute the issued commands from them.

In CPSs, the operators of the system must be aware of the current state of the controlled objects. Thus, a graphical user interface (GUI) called human–machine interface (HMI) represents the current state of the controlled object to the human operators. Fig. 1 depicts an overall representation of CPSs architecture.

The architecture of a CPS is often composed of two primary layers [3,14]:

(1) The cyber layer, that consists of corporate network, control network and a demilitarized zone (DMZ), and
(2) The physical layer, which consists of sensors, actuators and physical devices.

The corporate network containing workstations, employees and application server is in charge of business management and customer interaction.

The control network is composed of controllers like PLCs, control server and HMI. A DMZ is defined as a separate network segment that connects directly to firewalls [15,16]. Servers such as data server, data historian and web servers (for corporate–customer interactions) containing the data from the CPS that needs to be accessed from the corporate network are put on this separate segment for improved security [16].

The cyber layer often uses industrial protocols such as DNP3 [17], 61 850 [18] and Modbus [19] to communicate with the physical layer devices. A hugely popular approach for protecting the industrial control protocols are virtual private networks (VPNs) [16]. In order to protect these protocols from unauthorized