Computers in Industry 88 (2017) 44–57

Contents lists available at ScienceDirect

Computers in Industry

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

A game-theoretic approach to model and quantify the security of cyber-physical systems

Hamed Orojloo, Mohammad Abdollahi Azgomi*

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

ARTICLE INFO

Article history:
Received 18 November 2016
Received in revised form 23 February 2017
Accepted 30 March 2017
Available online xxx

Keywords:
Cyber-physical system (CPS)
Security modeling
Security evaluation
Game theory

ABSTRACT

The security of cyber-physical systems (CPSs) has become an active research area in recent years. The goal of attackers in these systems is often disrupting physical processes. However, breaking into a CPS is not the same as disrupting its physical process. To achieve the desired physical disruptions, an attacker needs to deep understanding about the failure conditions of the system, its control principles, and signal processing. For a better evaluation of the security of these systems, considering these issues is necessary. This paper presents a modeling approach to evaluate the security of CPSs. In the proposed model, the system moves discretely between different states, and in each state, the system evolves continuously according to a system of ordinary differential equations. The security modeling process of CPSs is divided into two phases of intrusion and disruption. In each phase, a game-theoretic paradigm with different parameters predicts the interactions between the attacker and the system. By solving the model, the security of CPSs is estimated in terms of metrics, such as mean-time-to-system shutdown and availability. Finally, the security of a chemical plant is investigated as an illustrative example.

1. Introduction

Cyber-physical systems (CPSs) are defined as computational and communication elements monitoring and controlling physical processes [1]. These systems can be found in critical infrastructures, such as smart grids, chemical and power plants, transportation systems, and natural gas distribution systems [2].

In these systems, a set of sensors measures some physical phenomena, such as temperature, pressure, and rotating speed from monitored and controlled objects. The measured information is transferred to the controllers through communication elements. Based on the received information from sensors, the controllers make correct decisions and apply them to actuators [1]. Fig. 1 depicts an overall architecture of CPSs.

CPSs facilitate the monitoring and controlling of physical entities. However, this modernization has exposed them to security threats [1]. We can refer to the maintenance of the availability of service and the protection of the stored and transmitted data as the primary concerns of the security enhancement activities in information technology (IT) systems. However, the protection of operations is the main goal of the security enhancement activities in CPSs [3]. The fact is that to achieve the desired disruptive results, an attacker needs to deep understanding about the failure conditions of the system, control principle and signal processing, which is not required when attacking IT systems [1].

Attacks on CPSs may have different consequences, such as equipment damage, including overstress of equipment and violation of safety limits, production damage (i.e., targeting product quality and production rate), and compliance violation, including safety hazards and environmental pollution [4]. Hence, the security of CPSs has strategic importance [4].

This paper proposes a modeling approach for evaluating the security of CPSs. The main contributions of this paper are as follows:

- Modeling the dynamic behavior of CPSs in normal situation and under security attacks.
- Investigating how different system-based and attacker-based parameters, such as the detection interval and probability, the attacker's knowledge level about the system, the time to physical disruption parameter, and the attacker's penalty as a result of detection of the attack may affect the security of CPSs.
- Using game theory to find out how the attacker and the system choose their strategies in different situations of

* Corresponding author at: School of Computer Engineering, Iran University of Science and Technology, Hengam St., Resalat Sq., Tehran, 16846-13114, Iran.
E-mail addresses: orojloo@iust.ac.ir (H. Orojloo), azgomi@iust.ac.ir (M.A. Azgomi).

http://dx.doi.org/10.1016/j.compind.2017.03.007
0166-3615/

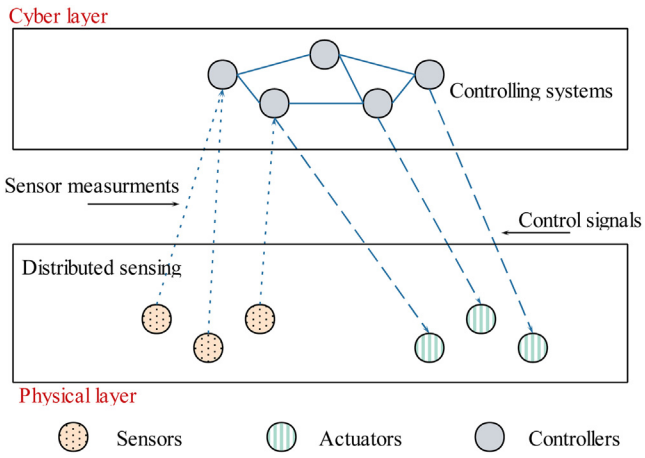

Fig. 1. An overall architecture of CPSs.

interdependence and estimating the attack and detection probabilities according to special parameters defensive and adversarial parameters. Indeed, the proposed game models consider the parameters that have not been previously considered.

- Evaluating the security of CPSs by using the proposed model based on metrics, such as mean-time-to-shutdown (MTTSD) and availability.

The proposed approach is applied to a chemical plant as an illustrative example and it is experimentally validated. The resulting quantitative analysis is useful for identifying significant control loops that require more accurate protection, and accordingly, for determining appropriate countermeasure strategies.

The rest of this paper is organized as follows. We start by discussing related work in Section 2. Section 3 presents the system model. In Section 4, the detailed description of the proposed method is provided. An illustrative example is presented in Section 5. And finally, in Section 6, the paper is concluded and an outlook to future work is given.

2. Related work

In this section, we provide an overview of related works in the context of the security of CPSs. Game theory has been employed for studying the security of computer networks and systems and also CPSs. We first review a number of game-theoretic approaches and then, we describe some other approaches. Moayedi et al. [5] have proposed a game-theoretic framework to evaluate the impacts of hackers diversity on security measures. Lv et al. [6] have proposed a stochastic game net model for security analysis of online digital goods business. Njilla et al. [7] have employed the game theory to model the security and trust relationship in cyberspace. Ma et al. [8] have provided game-theoretic approaches with different benefit functions, such as linear, negative exponential and S-shaped. Finally, they have determined the outcome of each game for each of the considered benefit functions.

Backhaus et al. [9] have proposed a game-theoretic model of human interactions in CPSs. The considered interactions are between a cyber adversary and an operator of an electrical grid supervisory control and data acquisition (SCADA) system. The outcome of the considered interactions and social welfare of these outcomes are estimated using the proposed model and subsequent analysis.

A dynamic game-theoretic method to model the interactions between the cyber level policy making and physical level robust control design is presented in [10]. The presented model captures the cascading failures in which one harmful event propagates failures in the system. Finally, a set of coupled optimality conditions is provided to characterize the pure strategy equilibrium of robust control design and cyber defense policy.

By considering correlated jammers as the rational decision makers, Zhu et al. [11] have provided a two-level receding-horizon dynamic Stackelberg game. They have proposed a receding-horizon Stackelberg control law for the operator, and assessed the resulting closed-loop stability and performance of the system under malicious behaviors.

Vigo et al. [12] have proposed a game-theoretic approach to model the behavior of attackers in control systems. They have assumed that sensor nodes communicate with an assessor and this communication channel may be threatened by jamming attacks. They have presented a decision making process between an adversary and sensors with energy limitation assumption. Finally, they have obtained the optimal strategies of the adversary and the system.

Almasizadeh et al. [13] have proposed an approach to model the attacker's actions and the system's reactions. They have modeled the attack process based on the temporal features of the attacker and the system actions. They have used the suitable time distributions to parameterize the proposed model. Finally, they have performed the security evaluation by computing the steady-state security and the mean-time-to-security-failure (MTTSF) measures.

Wei et al. [14] have discussed about the potential attacks against power grid and their impacts. They have captured the challenges and strategies for protecting smart grid and proposed a conceptual framework to protect power grid against attacks. Also, Wang et al. [15] have focused on the cyber security challenges in smart grids.

Ramos et al. [16] have used generalized stochastic Petri nets (GSPNs) to propose a methodology to model the operating sequences of protections in power systems. They have primarily focused on the modeling the uncertainty in the operation of protection devices using GSPN and measuring its impacts on the security evaluation.

Filippini et al. [17] have proposed a methodology of resilience analysis of systems of systems, with infrastructures as a special instance based on the functional relationships among its components. In order to identify the most critical and vulnerable components, the system has analyzed with respect to its structural and dynamic properties.

Huang et al. [18] have investigated the physical and economic consequences of attacks against control systems. To this end, several integrity and denial of service (DoS) attacks against the sensors and controllers have been examined. Also, Cárdenas et al. [19] have addressed the risk assessment, detection of attacks and determining suitable response strategies of process control systems. The proposed methods in these papers are applicable to evaluate the impacts of disturbances that bring the system to shutdown state.

Hu et al. [20] have discussed about the concept and strategies for building a robust and resilient CPS. They have defined the resiliency as a 3S-oriented design, that is, stability, security, and systematicness. They have also explained the CPS modeling issues.

In a recent paper [21], we have proposed a method for evaluating the consequence propagation of adversarial attacks in CPSs. The primary focus of this method was estimating the direct and indirect consequences of security attacks on the critical assets of CPSs. Furthermore, this method can be employed to evaluate and prioritize the system parameters according to their sensitivity to adversarial attacks.