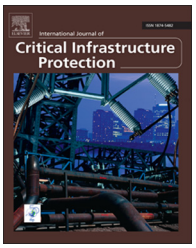
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory

*Xiaoxue Liu**, *Jiexin Zhang*, *Peidong Zhu*

School of Computers, National University of Defense Technology, Changsha, Hunan 410073, China

ARTICLE INFO

Article history:
Received 27 June 2016
Received in revised form
20 September 2016
Accepted 6 November 2016
Available online 1 December 2016

Keywords:
Cyber-Physical Systems
Cyber-Physical Attacks
Systematic Quantitative Modeling Approach
Dependency Model
Attack Model
Probabilistic Colored Petri Nets
Mixed-Strategy Attack-Defense Game Model

ABSTRACT

Cyber-physical attacks are posing great threats to the safety and security of cyber-physical systems. Modeling cyber-physical attacks reasonably and efficiently is the basis for defending cyber-physical systems effectively, which requires the development of quantitative analysis and modeling approaches for expressing threat propagation in cyber-physical systems. This paper extends the colored Petri net model by defining a probabilistic colored Petri net model that comprises basic models, rules, logical operators and transitions that describe threat propagation between nodes. Basic cyber-physical attack models based on probabilistic colored Petri nets are presented. Furthermore, a systematic modeling approach is presented for constructing a quantitative cyber-physical attack model for a cyber-physical system. The weights of the cyber-physical attack model connections are computed using a mixed-strategy attack-defense game model for each node and solving the Nash equilibrium. Additionally, a hierarchical method of division and integration is proposed to efficiently model complex, large-scale cyber-physical systems. Finally, the systematic cyber-physical attack modeling approach is applied to a case study involving a thermal power plant.

1. Introduction

Cyber-physical systems (CPSs) are becoming increasingly pervasive across the critical infrastructure. Examples of cyber-physical systems include smart homes, unmanned vehicles, industrial control systems and critical infrastructure networks. Critical infrastructure networks such as the smart grid, smart transportation systems and smart cities are complex, large-scale and distributed cyber-physical systems. Cyber-physical systems are attracting attention because they have become targets of attacks and face many security challenges.

Considerable research has been focused on the security of cyber-physical systems. Formal modeling and analysis tools have been applied to formalize the safety and security requirements of cyber-physical systems [2,19,23]. An aspect-oriented model that regards attacks as aspects of a system has been introduced to assess the security of cyber-physical systems [26]. System behavior under various malicious attacks has been modeled through mathematical tools and strategies have been proposed to improve intrusion detection in cyber-physical systems [11,14,22]. Systematic analyses of cyber-physical systems attacks have shown that they can result in various cyber-physical interactions [29], which can be clarified by distinguishing between the physical and cyber domains.

In cyber-physical systems, the physical domain covers various types of physical devices while the cyber domain primarily comprises computer, communications and control

*Corresponding author.
E-mail address: xiaoxue.liu@nudt.edu.cn (X. Liu).

http://dx.doi.org/10.1016/j.ijcip.2016.11.002
1874-5482/

systems. The two domains interact and integrate with each other—devices in the cyber domain analyze data from the physical domain in order to monitor and control physical devices whose states and behavior in the physical domain can affect the cyber domain. In addition, physical devices communicate and cooperate with each other via information and communications systems in the cyber domain. The interactions between the cyber and physical domains enable the cross-domain propagation of threats that are critical to cyber-physical attacks against cyber-physical systems.

1.1. *Cyber-physical attacks*

Cyber-physical interactions in cyber-physical systems make cross-domain attacks, specifically, cyber-physical attacks, possible. Attackers may use cyber attack techniques (involving viruses, worms and denial of service, etc.) in the cyber domain to cause damage in the physical domain or use physical attack means in the physical domain to cause disruptions in the cyber domain. In addition, these attack means can be applied comprehensively to achieve collaborative cyber-physical attacks. The objectives of cyber-physical attacks are usually achieved via threat propagation within and/or between the cyber and physical domains.

Cyber-physical attacks have been threatening the safety and security of cyber-physical systems and security problems in several cyber-physical systems have been shown to be caused by cyber-physical attacks. In 2003, the SQL Slammer worm infected a monitoring and control system at the Davis-Besse nuclear power plant in the United States, which caused the plant to be closed for maintenance [27]. In 2008, design flaws in control system software forced the shutdown of the Hatch nuclear power plant [9]. By far, the most famous cyber-physical attacks were launched by Stuxnet in 2010; these are regarded as the first professionally designed cross-domain attacks against a critical infrastructure asset [1]. Other examples include cyber-physical attacks that target electronic control systems in modern automobiles [8] and others that use cyber-physical systems as launching points to infect their controlling computers [29]. These and other cyber-physical attacks demonstrate that attack objectives are achieved through threat propagation within and/or between the cyber and physical domains, especially cross-domain propagation from the cyber domain to the physical domain.

Cyber-physical attacks significantly differ from traditional cyber attacks. Cyber-physical attacks usually attempt to compromise the safety of a cyber-physical system or the physical integrity of devices [30] while traditional cyber attacks threaten cyber security goals such as the confidentiality, integrity and availability of data and systems. With regard to attack means, cyber-physical attacks employ cyber and physical means to achieve cross-domain compromises while traditional cyber attacks only apply cyber techniques.

1.2. *Motivation*

Cyber-physical attacks have many new aspects that cannot be captured by existing cyber attack models. In order to adequately defend cyber-physical systems, it is important to develop sophisticated techniques for modeling cyber-physical attacks efficiently and with high fidelity.

Several researchers have formulated and analyzed interdependencies and vulnerabilities underlying cyber-physical systems [6,10,13,18,20,24,25]. Ouyang [17] has reviewed current approaches for modeling, simulating and analyzing cyber-physical system dependencies and has classified them into broad categories based on agents, network theory, system dynamics, etc.

Petri nets have been applied to model and reason about cyber-physical system security. Chen et al. [3] have employed Petri nets to express attacker behavior and state transitions in coordinated cyber-physical attacks against smart grids. Mitchell and Chen [15] have specified an analytical model based on stochastic Petri nets for capturing the dynamics between adversarial behavior and defensive postures in cyber-physical systems under three types of failures. Yampolskiy et al. [30] have presented a taxonomy of attacks on cyber-physical systems; their four attack categories are cyber to cyber (C-C), cyber to physical (C-P), physical to physical (P-P) and physical to cyber (P-C) attacks. Leveraging this taxonomy, Yampolskiy et al. [31] have devised a cyber-physical attack description language based on BNF and UML class diagrams to express conventional cyber attacks as well cross-domain attacks on cyber-physical systems.

While these approaches model cyber-physical attacks qualitatively through context descriptions, they do not support the quantitative modeling of cyber-physical attacks. In particular, researchers have not as yet presented systematic quantitative approaches for depicting the propagation of cyber-physical threats within and between the cyber and physical domains, which are critical to modeling, reasoning about and defending against cyber-physical attacks.

1.3. *Contributions*

This paper, which extends current work on the analysis and modeling of cyber-physical attacks, has three main contributions. The first is the extension of the colored Petri net model to the probabilistic colored Petri net model, which comprises basic models, rules, logical operators and, especially, transitions that capture threat propagation between entities in the cyber and physical domains. The probabilistic colored Petri net model is used to specify basic cyber-physical attack models, including the cyber-domain originated-attack model, physical-domain-originated attack model and collaborative cyber-physical attack models that engage the AND and OR logical operators.

The second contribution is a systematic modeling approach for constructing a quantitative cyber-physical attack model (CPAM) for a cyber-physical system. The approach comprises three main steps. A cyber-physical dependency model (CPDM) is first constructed for the cyber-physical system of interest using weighted directed graph theory to express all the assets and their dependencies. Next, the cyber-physical dependency model is converted to a cyber-physical attack model based on probabilistic colored Petri nets. Finally, an attack-defense game model is constructed for each node in the model based on mixed-strategy game theory by considering threat propagation to a node as an