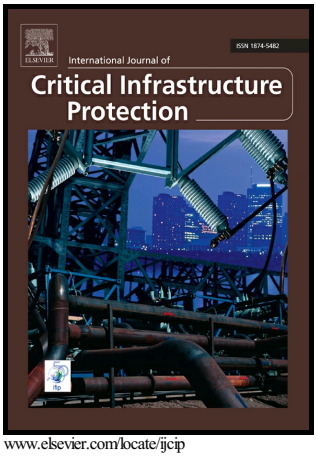

www.elsevier.com/locate/ijcip

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

Xiaoxue Liu, Jiexin Zhang, Peidong Zhu

PII: S1874-5482(16)30079-8
DOI: http://dx.doi.org/10.1016/j.ijcip.2016.11.002
Reference: IJCIP206

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

Received date: 27 June 2016
Revised date: 20 September 2016
Accepted date: 6 November 2016

Cite this article as: Xiaoxue Liu, Jiexin Zhang and Peidong Zhu, Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory, *International Journal of Critical Infrastructure Protection* http://dx.doi.org/10.1016/j.ijcip.2016.11.002

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

Xiaoxue Liu,[1] Jiexin Zhang, Peidong Zhu

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

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.

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

[1]Corresponding author: Xiaoxue Liu (xiaoxue.liu@nudt.edu.cn)