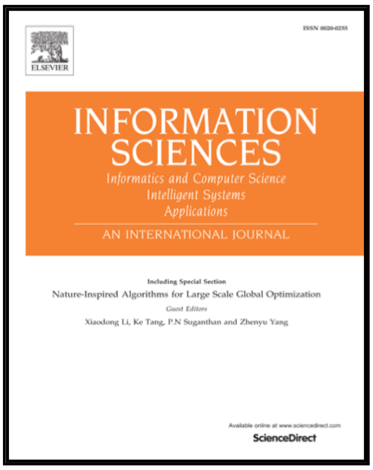

ISSN 0020-0255

ELSEVIER

INFORMATION SCIENCES

Informatics and Computer Science
Intelligent Systems
Applications

AN INTERNATIONAL JOURNAL

Including Special Section
Nature-Inspired Algorithms for Large Scale Global Optimization
Guest Editors
Xiaodong Li, Ke Tang, P.N Suganthan and Zhenyu Yang

Available online at www.sciencedirect.com
ScienceDirect

Game Theoretical Security Detection Strategy for Networked Systems

Hao Wu, Wei Wang, Changyun Wen, Zhengguo Li

PII: S0020-0255(18)30302-5
DOI: 10.1016/j.ins.2018.04.051
Reference: INS 13594

To appear in: *Information Sciences*

Received date: 11 December 2017
Revised date: 16 March 2018
Accepted date: 15 April 2018

Game Theoretical Security Detection Strategy for Networked Systems

Hao Wu, Wei Wang, Changyun Wen, and Zhengguo Li

H. Wu is with the Laboratory, CNCERT/CC, Beijing 100094, China. Email: whman@isc.org.cn, wuhao@cert.org.cn.

W. Wang is with the School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China. Corresponding author, email: w.wang@buaa.edu.cn.

C. Wen is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Nanyang Avenue, Singapore 639798.

Z. Li is with the Robotics Department, Institute for Infocomm Research, Singapore 138632.

Abstract

In this paper, a game theoretical analysis method is presented to provide the optimal security detection strategies for heterogeneous networked systems. A two-stage game model is firstly established, in which the attacker and defender are considered as two players. In the first stage, the two players make decisions on whether to execute the attack/monitoring actions or to keep silence for each network unit. In the second stage, two important strategic varibles, i.e. the attack intensity and detection threshold, are cautiously determined. The necessary and sufficient conditions to ensure the existence of the Nash equilibriums for the game with complete information are rigorously analyzed. The results reflect that with limited resources and capacities, the defender (attacker) tends to perform defense (attack) actions and further allocate more defense (less attack) resources to the units with larger assets. Besides, Bayesian and robust Nash equilibrium analysis is provided for the game with incomplete information. Finally, a sampling based Nash equilibrium verification and calculation approach is proposed for the game model with continuous kernels. Thus the convexity restrictions can be relaxed and the computational complexity is effectively reduced, with comparison to the existing recursive calculation methods. Numerical examples are given to validate our theoretical results.

Keywords: Networked systems, game theory, security detection, Nash equilibrium.

1. Introduction

Networked systems outperform traditional systems in many respects including achieving improved efficiency, cooperation and flexibility [34, 35, 17]. However, the involved network devices and communication links are often vulnerable to various cyber attacks, such as Denial of Service (DoS), computer viruses and bonnets. With the damaging effects of certain attack on a single unit expanded to the entire network, more severe system performance deterioration or even catastrophic events may be caused.

In the confrontation between an attacker and a defender, they can be regarded as two rational players who try to maximize their own payoffs by executing certain optimal strategies. This fact motivates us to investigate the security detection problem for networked systems based on game theoretical method in this paper. Note that available resources are always limited for both attacker and defender. Moreover, the networked systems are normally heterogeneous with respect to the security assets. Therefore, the two players should firstly determine which units deserve being allocated with attack and defense resources. Once the decisions are made, optimal attack intensity and detection threshold need be cautiously chosen in the second stage, as these two parameters are closely related to their security payoffs. In general, a higher threshold will result in a lower false alarm rate, whereas a higher missing alarm rate.