12TH ICCRTS

"Adapting C2 to the 21st Century"

Game Theoretic Solutions to Cyber Attack and Network Defense Problems

Suggested Topics: Network and Networking (Track 2)
C2 Technologies and Systems (Track 8)
C2 Concepts, Theory, and Policy (Track 1)

Dan Shen
Intelligent Automation, Inc
15400 Calhoun Drive, Suite 400
Rockville, MD 20855
Tel: (301)294-5235
Email: dshen@i-a-i.com

Genshe Chen (Principal point of contact)
Intelligent Automation, Inc.
15400 Calhoun Drive, Suite 400
Rockville, MD 20855
Tel: 301 294 5218 (direct)
Fax: 301 294 5201
Email: gchen@i-a-i.com

Jose B. Cruz, Jr.,
The Ohio State University
205 Dresses Laboratory, 2015 Neil Ave
Columbus, OH 43202
Ph: (614)292-1588
Email: cruz.22@osu.edu

Martin Kruger
The Office of Naval Research
Email: Martin_Kruger@onr.navy.mil

Erik Blasch
AFRL/SNAA
Erik.Blasch@WPAFB.AF.MIL

ABSTRACT

Game Theoretic Solutions to Cyber Attack and Network Defense Problems

There are increasing needs for research in the area of cyber situational awareness. The protection and defense against cyber attacks to computer network is becoming inadequate as the hacker knowledge sophisticates and as the network and each computer system become more complex. Current methods for alert correlation to detect and identify network attacks rely on data mining approaches that use features or feature sets of network data to discover an attack. These approaches are useful for simple attacks but for complex or coordinated cyber intrusions, they have various issues such as false positive, limited scalability, limits on detecting new types of coordinated and sophisticated cyber attacks. Therefore, the cyberspace security requires next-generation network management and intrusion detection systems that combine both short-term sensor information and long-term knowledge databases to provide decision-support systems and cyberspace command and control.

In this paper, we propose a game theoretic high level information fusion based decision and control framework to detect and predict the multistage stealthy cyber attacks. The main focus of this paper is to address the cyber network security problem from a system control and decision perspective and revise the Markov game model[1] with the knowledge of the cyber attack domain.

Outline:

[1] D. Shen, G. Chen, J. B. Cruz, Jr., et al., “Game Theoretic Approach to Threat Intent Prediction," in Proceedings of CCRTS 2006: the Command and Control Research and Technology Symposium, San Diego, July, 2006.