10.1117/2.1200707.0783

# A Markov game approach to cyber security

**Dan Shen, Genshe Chen, Jose B. Cruz, Jr., Leonard S. Haynes , Martin Kruger, and Erik Blasch**

*High-level data fusion based on Markov game models can refine predictive models and capture features relevant to cyber network awareness.*

Cyber attacks (CAs) have generally been one-dimensional, involving denial of service (DoS), computer viruses or worms, and unauthorized intrusion (hacking). Websites, mail servers, and client machines are the major targets. However, recent CAs have diversified to include multi-stage and multi-dimensional attacks with a variety of tools and technologies. Next-generation security will require network management and intrusion detection systems that combine short-term sensor information with long-term knowledge databases to provide decision support and cyberspace command and control.

Recent efforts to apply data fusion techniques to cyber situational awareness are promising[1,2], but assessing the potential impact of an attack and predicting intent, or high-level data fusion, continue to present substantive challenges. We propose a new approach to evaluate network defenses in which each possible attack pattern is generated by a data-mining module and estimated by a game-theoretic data fusion module.

Our cyberspace security system has two fully interlocking parts, as indicated in Figure 1. The *data fusion* module permits refinement of primitive awareness and assessment to identification of new attacks while the *dynamic/adaptive feature recognition* module generates estimates and learns about them. The Markov game method, a stochastic approach, is used to evaluate the prospects of each potential attack. Game theory captures the nature of cyber conflict: determining the attacker's strategies is closely allied to decisions on defense and vice versa.

Figure 1 also charts the data mining and fusion structure. For instance, detection of new attack patterns is linked to Level One results in *dynamic learning*, including deception reasoning, trend/variation identification, and multi-agent learning. Our approach to deception detection is heavily rooted in the application of pattern-recognition techniques to locate and diagnose anomalous conditions in the cyber environment. Dynamic learning and refinement can also enhance Level Two and Level Three data fusion.

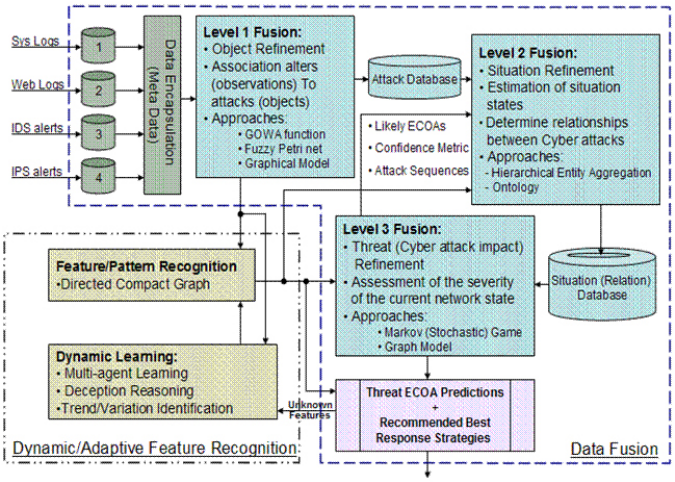


***Figure 1.*** *A data-mining/data-fusion approach for cyber situational awareness and impact assessment*

To address network security from a system control and decision perspective, we present a Markov game model in line with the standard definition.[3] Cyber attackers, defense-system users, and normal network users are *players* (decision makers). All possible states of involved network nodes constitute the *state space*. For example, the web-server is controlled by attackers, and to determine the optimal deployment of the intruder detection system, we include the defensive status for each network node in the state space. In addition, at every time step, each player chooses targets with associated actions based on local network information. Finally, the *transition rule* calculates a probability distribution over the state space for the next time step.

Our simulation of a network scenario with 269 computers, 10 routers, and 18 switches (see Figure 2) demonstrates that we can detect and defend two-stage cyber attacks in which a target computer (web server) is first infected or hacked and then used to

*Continued on next page*

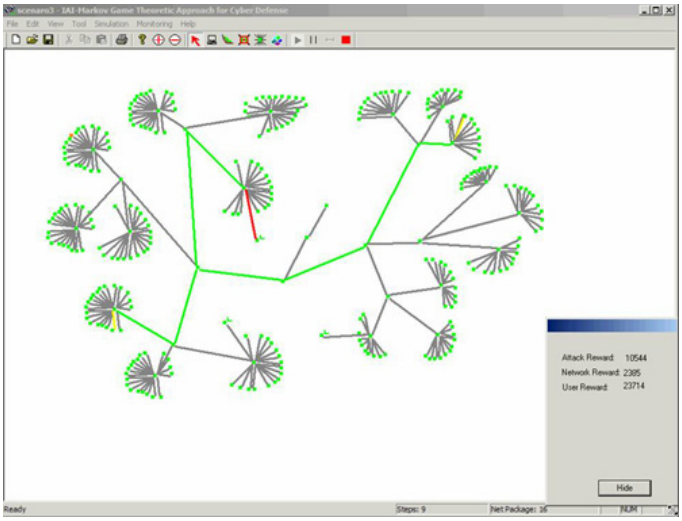


***Figure 2.*** *A complicated network defense scenario with 269 computers*

infect more important computers, such as file servers and email servers. This two-step attack scheme is based on two significant facts. First, a public web server is an easy target. Second, an infected internal computer, the web server in this case, is more efficient for attacking better protected computers, such as data and email servers, and operates with greater stealth than an external computer.

Our proposed game-theoretic data-mining approach can solve problems including cyber situational awareness and inferencing adversary intent in attack scenarios. Our next step will be to add adaptation schemes to the Markov structure, so each player can dynamically and intelligently adjust strategy based on observed system states.

## Author Information

**Dan Shen, Genshe Chen, and Leonard S. Haynes**
Intelligent Automation Inc.
Rockville, MD

Dan Shen received his MS and PhD degrees in electrical and computer engineering from Ohio State University in 2003 and 2006. He is currently a research scientist at Intelligent Automation Inc., where his interests include game theory and its applications, optimal control, and adaptive control.

Genshe Chen is a senior research scientist and program manager in Networks, Systems, and Control at Intelligent Automation Inc. He has served as technical lead/principal investigator for 15 projects, including maneuvering-target detection, as well as tracking, space situational awareness, asymmetric threat detection with prediction, cooperative control for teamed unmanned aerial vehicles, and differential pursuit-evasion game with multiple players.

Leonard S. Haynes received his PhD degree in electrical engineering and computer science from the University of Maryland in 1974. As president of Intelligent Automation Inc., which he founded more than 20 years ago, he has personally generated over 150 proposals that cover a range of innovative technologies.

**Jose B. Cruz, Jr.**
Electrical and Computer Engineering
Ohio State University
Columbus, OH

Jose B. Cruz, Jr. received his doctorate in electrical engineering from the University of Illinois, Urbana-Champaign, in 1959. He is currently distinguished professor of engineering and professor of electrical and computer engineering at Ohio State University. He was elected to the National Academy of Engineering in 1980.

**Martin Kruger**
Office of Naval Research
Arlington, VA

Martin Kruger manages the Intelligence, Surveillance and Reconnaissance Thrust Area for the Expeditionary Maneuver Warfare & Combating Terrorism Department of the Office of Naval Research. In that capacity, he is responsible for developing applicable technology. His research interests include sensing, data fusion & visualization, resource management, and information dissemination.

**Erik Blasch**
Air Force Research Laboratory/SNAA
Wright Patterson Air Force Base
Dayton, OH

Erik Blasch is an information fusion evaluation lead for the Air Force Research Laboratory's COMprehensive Performance Assessment of Sensor Exploitation (COMPASE) Center, and adjunct professor of electrical engineering at Wright State University and the Air Force Institute of Technology. He is active in SPIE and participates in regional activities, conference boards, journal reviews, and scholarship committees.

*Continued on next page*

**References**

1. J. Salerno, M. Hinman, and D. Boulware, **A Situation Awareness Model Applied To Multiple Domains**, **Proc. Defense and Security Conference**, Orlando, FL, March 2005.
2. G. Tadda, J. Salerno, D. Boulware, M. Hinman, and S. Gorton, *Realizing Situation Awareness within a Cyber Environment*, **Proc. SPIE 6242**, 2006.
3. L. S. Shapley, *Stochastic games*, **Proc. National Academy of Sciences of the United States of America 39**, pp. 1095–1100, 1953.