Game-Theoretic Perspectives and Algorithms for Cybersecurity

Christopher Kiekintveld
University of Texas at El Paso
TX, USA
cdkiekintveld@utep.edu

ABSTRACT

Information plays a key role in many games, and game theory includes reasoning about how agents should perceive signals, and how they should strategically decide what signals to send. This can involve complex tradeoffs about how revealing certain information will affect the beliefs and actions of other players. I will overview some basic approaches for modeling information in game theory, such as signaling games, and applications to games such as Poker. The second part of the talk will focus on our work applying game theoretic models and algorithms in cybersecurity. I will discuss how we apply game theory to optimize strategies for deception in cybersecurity, including honeypots, honey traffic, and other deceptive objects. I will also cover work that considers dynamic deception using sequential models that capture uncertainty. Finally, I will discuss some recent work in adversarial learning and connections between this area and game theory.

CCS Concepts/ACM Classifiers

•Theory of computation~Theory and algorithms for application domains~Algorithmic game theory and mechanism design~Algorithmic game theory•Security and privacy~Computing methodologies~Artificial

intelligence~Planning and scheduling~Planning under uncertainty

Author Keywords

Algorithmic game theory, computer security, uncertainty, cyber deception, information hiding, adversarial learning

BIOGRAPHY

Christopher Kiekintveld is an associate professor at the University of Texas at El Paso (UTEP). His research is in the area of intelligent systems, focusing on multi-agent systems and computational decision making. He is also interested in applications of artificial intelligence to security, trading agents, and other areas with the potential to benefit society. He received his Ph.D in 2008 from the University of Michigan for thesis work on strategic reasoning, including applications in designing a champion trading agent for the TAC SCM competition. He has worked on several deployed applications of game theory for security, including systems in use by the Federal Air Marshals Service and Transportation Security Administration. He has authored more than 80 papers in peer-reviewed conferences and journals (e.g., AAMAS, IJCAI, AAAI, JAIR, JAAMAS, ECRA). He has received several best paper awards, the David Rist Prize, and an NSF CAREER award.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

IH&MMSec '20, June 22–24, 2020, Denver, CO, USA

© 2020 Copyright is held by the owner/author(s).

ACM ISBN 978-1-4503-7050-9/20/06.

<https://doi.org/10.1145/3369412.3396883>