Game Theory for Security: Lessons Learned from Deployed Applications*

Milind Tambe

Computer Science and Industrial & Systems Engineering Departments
University of Southern California
Los Angeles, California, USA
tambe@usc.edu

Abstract. Security at major locations of economic or political importance or transportation or other infrastructure is a key concern around the world, particularly given the threat of terrorism. Limited security resources prevent full security coverage at all times; instead, these limited resources must be deployed intelligently taking into account differences in priorities of targets requiring security coverage, the responses of the adversaries to the security posture and potential uncertainty over the types of adversaries faced. Game theory is well-suited to adversarial reasoning for security resource allocation and scheduling problems. Casting the problem as a Bayesian Stackelberg game, we have developed new algorithms for efficiently solving such games to provide randomized patrolling or inspection strategies: we can thus avoid predictability and address scale-up in these security scheduling problems, addressing key weaknesses of human scheduling. Our algorithms are now deployed in multiple applications. ARMOR, our first game theoretic application, has been deployed at the Los Angeles International Airport (LAX) since 2007 to randomize checkpoints on the roadways entering the airport and canine patrol routes within the airport terminals. IRIS, our second application, is a game-theoretic scheduler for randomized deployment of the Federal Air Marshals (FAMS) requiring significant scale-up in underlying algorithms; IRIS has been in use since 2009. Similarly, a new set of algorithms are deployed in Boston for a system called PROTECT for randomizing US coast guard patrolling; PROTECT is intended to be deployed at more locations in the future, and GUARDS is under evaluation for national deployment by the Transportation Security Administration (TSA). These applications are leading to real-world use-inspired research in scaling up to large-scale problems, handling significant adversarial uncertainty, dealing with bounded rationality of human adversaries, and other fundamental challenges. This talk will outline our algorithms, key research results and lessons learned from these applications.

* This is joint work with several researchers, including former and current members of the Teamcore group, please see http://teamcore.usc.edu/projects/security

D. Kinny et al. (Eds.): PRIMA 2011, LNAI 7047, p. 1, 2011.