1-2013

Raising the Game: Applying Theory and Analytics to Real-world Threats

Singapore Management University

Raising the game: Applying theory and analytics to real-world threats

Published: 30 Jan 2013

Safety and security are, on many levels, essential priorities for governments, businesses and individuals. While an increase of defence and security budgets may bring some assurance of peaceful times to come, it seems the world has no lack of insane perpetrators who can still somehow evade, breach, ambush, assail and attack as they please.

An example might be the series of mass shootings that have occurred across the United States in 2012 – tragedies that (a) were largely unexpected and (b) involved unlikely perpetrators that (c) did not come off as likely security threats.

Enter the “Bayesian Stackelberg Game”, a game theory model that can, and has been applied rather successfully to the allocation of security resources in the United States.

A pioneer in this highly specialised field, Milind Tambe, a professor of computer science and industrial and systems engineering, and the Helen N. and Emmett H. Jones Professor in Engineering at the University of Southern California (USC), spoke about the payoffs and challenges of implementing such game theory-based models at a workshop organised by Singapore Management University's (SMU) Living Analytics Research Centre (LARC).

“Security is a global concern. We have to protect our ports, our airports, national infrastructure, forests and wildlife... But, we have limited resources, which means we have to be selective in our checking and monitoring,” said Tambe.

Bayesian Stackelberg games are helpful insofar as they assume adversaries will make decisions based on their understanding of defenders’ prior moves. So an assailant looking to strike at an airport will, for example, assess the opportunities and risks posed by the security forces in place, before deciding on a move that will yield maximum payoff.

Under this game theory, calculations are made in decision matrices aimed at increasing uncertainty, so that the assailant cannot easily decide on a next move, which, in turn, should increase the defender's expected reward, and in practical terms, optimise the allocation of limited security resources through such analytics, Tambe explained.

In 2007, Tambe and his team introduced and deployed the Stackelberg games at the Los Angeles Airport (LAX). The system, known as AMOR or Assistant for Randomised Monitoring Over Routes, was built to address challenges in determining where to place checkpoints and special units. Calculations had to include other external variables too, such as adversary type and “visibility” of security personnel to potential adversaries.

AMOR randomised security patrols with the help of complex statistical weights to determine the costs and benefits of allocation decisions. The software provided not just a schedule for security checks, but also decisions on where and how long these patrols should last – and because of the built-in randomness, AMOR made it rather difficult for observers to find and to exploit patterns.

The project ultimately paid off as LAX security personnel seized more “guns, assault rifles and thousands of ammunition”, compared to the former method of regular scheduling. Media interest in AMOR followed soon after, catching the attention of other government organisations such as the US Coast Guard, Los Angeles (LA) Sheriff's Department, and Federal Air Marshalls Service (FAMS), all of whom engaged Tambe for help.

With the US Coast Guard, Tambe built a system known as the Port Resilience Operational / Tactical Enforcement to Combat Terrorism, or PROTECT, that had to facilitate the scheduling of patrols, not only beef up maritime security, but also, to serve as deterrence. Additionally, it would allow for a more efficient use of limited manpower resources.

Similar to AMOR, these schedules had to contain a sense of randomness without being haphazard, and so weights were assigned based on certain requirements."PROTECT has since been deployed in Boston and New York, and it will go to most of the ports across the US starting in 2013," Tambe announced proudly.

The following project with the LA Sheriff's Department differed, Tambe recalled, as it was aimed at tackling cheats rather than attackers. Unlike the subway train systems of most urban cities where tickets must be tapped or inserted into a machine at the gate, the LA metro subway did not have such a facility. “It's an honour system, it has no barriers… and it’s on evaluation now,” he explained.
To prevent fare evasion, the Sherriff’s department conducts randomised checks on trains and at the stations. Tambe and his team were embedded with patrolling teams, where they learnt procedures,

tactics and techniques – things that helped them formulate schedules that would enable the teams to tackle cheats more effectively, given the limited resources.

FAMS faced a different set of challenges, Tambe recalled. The project scope was moreover, massive, compared to the others. “They had some 30,000 flights a day internationally, and different flights carry different risks. A plane flying from New York to London will have a different risk to one going into a small town in Canada,” he said. The randomisation problem was made more interesting given that there were websites dedicated to “spot the air marshal”, and so the system not only had to take into account the risks of each flight, but also the predictability involved in personnel allocation.

Tambe had to contend with a very large number of combinations and probabilities, given the sheer number and varieties of flights, risks relating to destinations, travel periods, adversary types, adversary actions, types of attack – and to top it all off, the scale on which many of these different things can happen.

“We haven't solved all of these problems,” Tambe admitted. He recalled how he and his team had attempted to get around some difficulties, one of which involved fighting urges to enumerate combinations – something that often caused computers to crash, presumably due to data overload.

Then there are other limitations stemming from game theory assumptions. “We assume that everyone acts with perfect rationality that they will maximise their expected value and so on,” he noted. There is also the idea of bounded rationality, which is to say that even the most sophisticated system will never yield a truly complete picture.

Yet, despite these limitations, the game theory approach still provides a more robust outcome. “Humans tend to fall into predictable patterns,” Tambe argued. Asking a human to schedule air marshals on flights, for example, while taking into account the many different and complicated factors, such as types of flight, times, rules, risks, etc, is extremely challenging. “They will find a pattern, stick to it, and then we end up with a predictable pattern,” he added.

These problems are not fully addressed with game theory or with software, but a good question to ask, perhaps, is: “Are we better off with what we have, than what was done previously?” Tambe believes so – and he thinks government agencies are slowly but surely seeing great potential behind his approach. “The fact that [government agencies] are now using the software must mean they see some value in it,” he remarked.

While there are still many areas to work on, Tambe derives satisfaction in seeing how his work has empowered others to save lives and prevent catastrophes. “This is the real-world result of theoretical work,” he concluded.