Center for Law & Human Behavior

The University of Texas at El Paso

DHS SYMPOSIUM SERIES NO. 6

Game Theory & Adversarial Reasoning

Modeling Decisions as Games

December 1, 2016

Research in Brief

BTI Institute

Borders • Trade • Immigration

A Department of Homeland Security Center of Excellence

Center for Law & Human Behavior
The University of Texas at El Paso
500 West University Avenue
Prospect Hall, Room 226
El Paso, Texas 79968
Tel: (915) 747-5920
Email: clhb@utep.edu
Website: http://clhb.utep.edu
Follow us on Twitter @1CLHB

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

This symposium is supported by the U.S. Department of Homeland Security, Science and Technology, Office of University Programs under Grant Award Number DHS-14-ST-061-COE-00.

Abstract

Many decisions in homeland security and law enforcement are fundamentally about adversarial interactions between multiple agents with opposing interests. We provide a broad overview of recent research that seeks to develop better data analysis and modeling techniques to provide decision support for complex security decisions, such as how to optimally allocate security resources. We provide simple examples to illustrate the basic concepts, and then discuss a number of examples of different applications of these methods to a wide variety of problems in the context of homeland security and law enforcement. We also highlight some of our ongoing research to improve the fundamental methods to make them scalable and broadly applicable to new types of problems. Finally, we provide examples of how close collaboration with end users and decision makers has led to useful deployments of adversarial reasoning to solve real-world problems leading to increased effectiveness.

Introduction

Game theory is a branch of applied mathematics that is used in the social sciences, most notably in economics. Game theory is also used in biology, engineering, political science, international relations, computer science, and philosophy. Game theory attempts to mathematically capture behavior in strategic situations where an individual's success in making choices depends on the choices of others. The key components of a game include: players, options/moves, sequence of moves, objectives/payoffs, information, time and equilibrium. Game theory has been applied to many domains, such as biology and population evolution, transportation, computer network, political sciences, health care, business and supply chain, insurance, cybersecurity, and personal life and thinking. Game theory has also been studied extensively in homeland security.

One of the most common uses of game theory in homeland security is to optimize the allocation of security resources, such as deployments of officers, vehicle patrols, K9 units, or the use of screening methods during inspections (Tambe, 2011). The basic problem in these cases is that there are limited resources that must be used as effectively as possible to increase security. For example, a limited number of units may be assigned to patrol a large number of possible locations that may be the target of attacks or other illegal activity.

One of the important aspects of allocating resources effectively in adversarial domains is ***unpredictability***. Since we are facing an intelligent, adaptive adversary who can learn about the security policy, it is not sufficient in most cases to use a static, predictable deployment strategy for allocating security resources. Instead, we focus on finding optimal randomized policies that keep the attacker guessing, limiting the effectiveness of surveillance and increasing deterrence, while maintaining protection of the most critical assets.

It is also possible to model both strategic attackers and random events (e.g., natural disasters or accidents) using this approach. For example, using attacker-defender games, Zhuang and Bier (2007) apply game

theory to identify the attacker's and defender's equilibrium strategies, in the resource allocation game to counter terrorism and natural disasters. Zhuang and Bier (2007) balance resource allocation between terrorism and natural disasters. Instead of a discrete choice, this work considers the attacker's choice using a continuous level of effort. It is found that when the defensive investment increases, an attacker can either increase his level of effort to compensate for the reduced probability or decrease his level since the attack becomes less profitable.

ARMOR: LAX Security

One of the first uses of game theory in a major deployed decision support system for homeland security was the ARMOR system developed for the Los Angeles, CA (LAX) airport (Pita, 2008). The ARMOR system uses game theory to find optimal schedules for two resource allocation problems at the airport. The first is the vehicle checkpoints problem. Checkpoints are used to screen vehicles entering the terminal areas of the airport. However, there are several potential access points. There are insufficient resources to man checkpoints on all inbound routes at all times, so the checkpoints must be allocated strategically. ARMOR-checkpoints utilizes game theory to randomly assign the checkpoints, balancing the importance of the different routes and terminals with the need to be unpredictable.

The second problem is the K9 scheduling problem. There are a limited number of K9 units available to patrol the LAX terminals, so there is a similar problem with deciding where and when to schedule K9 patrols in the terminals using the limited resource. ARMOR-K9 uses game theory to create randomized schedules for the K9 patrols. Again, optimizing the need for unpredictable schedules while taking into account risk information about the different terminals and time periods.

The ARMOR system has been in continuous use at LAX since 2007, and has been viewed as a highly successful program in improving the security of the airport.

IRIS: FAMS Scheduling

Following the success of ARMOR, our team worked with the Federal Air Marshals Service (FAMS) to develop a scheduling system for randomizing the flight scheduling for the air marshals using a similar game-theoretic approach (Kiekintveld, 2008). This system generates unpredictable flight schedules for a specified number of FAMS teams. The system, again, takes into account risk evaluations of the flights and airports to determine the optimal schedule. In addition, this system must account for a large number of complex scheduling constraints to generate a feasible schedule for the air marshals to fly. The complexity of the scheduling problem in combination with the scale of the resource allocation problem, due to the massive number of possible flights and large number of air marshals, required new breakthroughs in computational methods for security games to be able to develop the software system, IRIS.

After extensive evaluation by the research team and internal evaluation by FAMS, the IRIS system was initially deployed for scheduling international flights in 2009, and use of the system has been expanded

since that time. Ongoing research continues to provide more advanced game models and software tools to support scheduling (Tsai, 2009).

Modeling Secrecy and Deception

Different from natural disasters where the resource allocation is usually disclosed, in terrorism, attackers are adaptive, and the investments are not always disclosed to the public. It is important and challenging for the government to understand when and how such investment should be disclosed.

Zhuang and Bier (2010) study the conditions when a defender should choose secrecy or deception about the investments in a homeland-security context. In games with no private defender information, truthful disclosure is preferred to secrecy and deception as long as the cost of implementing truthful disclosure is lower than the costs of secrecy and deception. In games with private defender information, secrecy and deception may be strictly preferred by the defender at equilibrium, in order to mimic other types of defenders, even if the cost of implementing truthful disclosure is lower than the costs of secrecy and deception (Zhuang and Bier, 2010). Zhuang et al. (2010) model defender secrecy and deception in a multiple-period attacker-defender game. Three possible types of defender signals are allowed at each period, which are disclosure, secrecy, and deception. In addition, the attacker would update his knowledge based on the defender's signals as well as the result of a contest. This paper shows that more cost-effective security could be achieved through secrecy and deception. The three disclosure strategies are also studied in Zhuang and Bier (2011) where only one stage game is considered. In the context of terrorism, the attacker usually learns the defender's private information. Xu and Zhuang (2016) analyze the strategic interactions of the attacker's learning and the defender's counter-learning. They find that the attacker's best responses and the defender's equilibrium deception and defense strategies are significantly impacted by the attacker's cost of learning.

Multi-Period Attacker-Defender Games

It is important and challenging to understand how to defeat terrorist threats over time. We need to assess the terrorist's capacity to attack over time. Hausken and Zhuang (2011) study the timing of attacks and the terrorist's option of stockpiling attack resources using a two-period game, where the attacker chooses whether or not to stockpile resources from the first to the second period. Besides the terrorist's capacity to attack over time, how the attacks can be deterred as time passes is another issue which is studied in Hausken and Zhuang (2012). Hausken and Zhuang (2012) develop a model to study the timing and deterrence of terrorist attacks in a T-period game where a two-stage game (the defender moves first and the attacker moves second) is analyzed in each period. Keeping up with developments in technology is one of the key challenges to maintain security. The dynamics between a defender and an attacker, when considering the issue of technology in a multi-period sequential game with uncertainty, is investigated in Jose and Zhuang (2013), where "defenders can improve their chances of defending against an attack by investing in technology, whereas attackers can forego attacking by

using their time to accumulate knowledge, resources, or technology to improve their future chances of success."

Modeling Probable Pathways for Human Smuggling and Trafficking Along the U.S.-Mexico Border

Generally, there are three wars on the U.S.-Mexico border: drugs, immigration, and homeland security. To improve border security, enormous resources have been devoted, but the continuing vulnerability of adversaries potentially entering the United States through illicit pathways has been highlighted by multiple studies. According to the National Border Patrol Council, the open border is the greatest one among the physical and economic threats to Americans today. The border between the U.S. and Mexico runs through four American states: California, Arizona, New Mexico and Texas. The border consists of a highly diverse terrain, such as ocean waters, urban areas and arid deserts. Under the Secure Fence Act of 2006, it is required by congress that the entire border be 100% operationally controlled by the Department of Homeland Security. A Mexico–United States barrier including a series of walls and fences has been built to prevent illegal crossings from Mexico into the United States. However, experience along the southern border shows that even with fortifications, a wall could provide only modest capacity to prevent illegal crossings. Border Patrol agents utilize everything available (from horseback agents to helicopters) to stop illegal crossings and secure the border. On the other side, adversaries also are equipped with sophisticated resources to avoid capture.

We seek to provide greater clarity to these questions by applying game theory to detailed transportation networks in the Arizona border region. We identify the optimal implementation strategies for defensive assets to combat a range of different adversary types within these challenging environments given budget constraints. Using the data available, we conducted a regression analysis and found that the apprehensions from the southern border decreased as the fence length, US unemployment rate, and Customs and Border Protection budget increased. In Behlendorf et al. (2015) we propose a triangulated irregular network to model the transportation network along the Arizona-Mexico border. A bi-level max- min mix-integer problem is formulated, and a graphical user interface (GUI) is developed to assist decision making and demonstrate the results (Zhang et al., 2017).

Robust Homeland Security Game Models

Models that have been developed to study homeland security games between the defender and the attacker generally assume the attacker is rational or strategic. What if the attacker is not fully rational, but is strategic with a probability $0 \le q \le 1$? Non-strategic behaviors are specified exogenously, then what is the impact to the defender's real payoff, and what's the defender's optimal strategy as a function of q? What if the defender believes the attacker is fully rational/ irrational?

A hybrid model where the defender allocates defensive resource among multiple targets to minimize the total expected loss facing a terrorist being either strategic or non-strategic, is developed in

Shan and Zhuang (2013). The robustness of defensive resource allocations is studied by comparing the defender's total expected losses in the following cases: (1) the probability that the terrorist is strategic and is known by the defender; (2) the attacker is non-strategic, but the defender falsely believes the attacker is fully strategic; (3) the attacker is strategic, but the defender falsely believes the attacker is non-strategic. The robustness of resource allocation in homeland security is also studied in Hao et al. (2009) and Nikoofal and Zhuang (2012).

Screening Games

Security screenings play an important role in many fields, such as airport security screening, visa issuance, and cargo inspection. In-depth examination of applicants reduces security risk, but also entails high congestion which can deter normal applications. This may in turn conflict with the approver's interests. Very little research has simultaneously considered both the good and bad applicants' strategic behavior and congestion in determining the optimal screening policy. Strategic decisions by all types of potential applicants are studied in Wang and Zhuang (2011). Where potential applicants could adapt their behavior according to a disclosed security policy, e.g., smugglers may choose the weakest port to enter, leisure travelers may choose not to travel because of congestion, inconvenience, and foreign students may no longer apply to U.S. schools because of the long waiting period for visas. In this work, a model to determine the optimal screening policy to maximize the reward from admitting normal applicants net of the penalty from admitting bad applicants, is developed using an M/M/1 queueing system. In addition, to balance security and congestion in the face of strategic normal and adversary applicants, Song and Zhuang (2017) analyze optimal screening policies. Song and Zhuang (2017) utilize an imperfect two-stage screening system with potential screening errors at each stage, where game theory and queueing theory is integrated to study the optimal two-stage policies under discriminatory and non-discriminatory screening policies.

Audit Games

The HIPAA privacy law was passed in 1996 to prevent inappropriate flow of private health information. Hospitals have adopted post-hoc audits of health record access as the preferred means of detection and remediation of HIPAA breaches. This is mainly due to the undesirable consequences of restricting flow of health information (e.g., in a medical emergency). However, the complicated privacy policies do not permit completely automated auditing. Thus, the few human auditors are faced with a large number of suspicious cases to audit. Indeed, ad-hoc audit practices have failed to detect many HIPAA breaches in a timely fashion.

As part of our research to address this problem (AAAI, 2015; IJCAI, 2013), we propose a Stackelberg game model of the interaction between the auditor and auditee. An important component of this auditor-auditee interaction is punishments; judicious use of punishments can shape the behavior of the auditee resulting in desirable outcomes. The scalability challenge can be gauged by noting that even a small example of 100 audit cases to be inspected by 10 audit resources, results

in many (1.7 × 10^13) possible allocations. Adding to scalability problem, the decision variable for punishments makes the resultant Stackelberg equilibrium computation problem a non-convex optimization problem. We propose a fixed parameter tractable (FPT) and a fully polynomial time approximation scheme (FPTAS) for this non-convex problem, thereby allowing for efficient computation of the equilibrium. Further improving scalability, we propose a technique to transform the optimization problem into an equivalent compact optimization by reducing the number of variables and adding more constraints. We identify the conditions under which only a polynomial number of new constraints were added, which led to up to 3X improvement in runtime when these conditions were satisfied. These conditions are not restrictive as they capture many common auditing scenarios such as, centralized auditing by a group of auditors and localized auditing of employees by immediate managers. Based on the model, we could provide an economic guided explanation for known occurrences such as hospitals not punishing top doctors for privacy transgressions. We also identify the external incentives that could encourage hospitals to conduct more thorough privacy audits, thereby providing policy tools to stimulate more rigorous auditing in hospitals.

DARMS: TSA Screening Game

The TSA has launched a new initiative known as DARMS which aims to enhance aviation security. Dubbed as the "future of aviation security", this ambitious project aims to provide a mathematically sound basis for intelligent screening of passengers. The TSA utilizes a number of screening resources for screening passengers, e.g., x-ray machines, metal detectors, pat-downs, etc. However, the most effective screening resources cannot be used to screen every passenger as there exists capacity bounds on the usage of each screening resource, with lower capacity for more effective resources. Thus, given the risk category of each passenger, the number of passengers and the efficacy of resources in detecting threats, the goal is to maximize the quality of security screening subject to the underlying passenger flow constraints.

As part of the passenger screening component of the DARMS project, we propose a novel Stackelberg game model for screening of threats (AAAI, 2016). Combining team formation aspects for the capacity-constrained screening resources with the need to screen every passenger in every risk category as effectively as possible results in a large (exponentially large) linear program (LP) required to compute equilibrium of the Stackelberg game. For example, assuming 900 and 100 people arrive in one hour in two risk categories respectively and with 10 screening teams results in 4.7 × 10^33 variables in the LP; typically this number is much larger as the number of risk categories and teams are higher. We provide techniques for scaling up the equilibrium computation. The techniques include a novel temporal decomposition of the game and a novel alternate representation of the LP obtained by using a convex combination of a number of polytopes to represent the feasible space of the LP. Since we prove the NP hardness of the optimization problem (even after temporal decomposition), the guaranteed

optimal algorithm using the alternate representation of the LP has a large running time for the worst case. By trading off between the worst case solution quality and running time, we provide an efficient and practical algorithm that is not worst case optimal but performs extremely efficiently in practice with practically no solution quality loss (no loss observed in random tests). This work will hopefully be adopted by all airports in future.

USC Crime Prediction

Distinct from classic game theory, the availability of data on defender-adversary interaction in domains such as, wildlife and urban crime, has brought forth the opportunity to learn adversary behavior and predict outcomes based on the learned models. Our work on learning in games has been guided by the philosophy that adversary behavior should be directly learned from data with minimal prior assumptions, e.g., not assuming rationality (AAMAS, 2016).

The Department of Public Safety (DPS) at the University of Southern California (USC) is tasked with ensuring security in and around the USC campus, and similar to other security agencies, the number of patrol officers available is limited. DPS has records for past crime and patrol allocations over multiple years, and their goal is to conduct preventive patrols intelligently by predicting crime. We recognize that it is almost impossible to estimate utilities for petty criminals and moreover, it has been shown empirically that criminals do not exhibit perfectly strategic behavior in practice. We recognize that real adversaries are not completely arbitrary and are more likely to exhibit patterns in their behavior which can be exploited to obtain better guarantees. Thus, we propose a technique that directly learns the behavior of the criminals (AAMAS, 2015). We propose a Dynamic Bayesian Network (DBN) based model for predicting crimes from available crime and patrol data. The parameters of the model capture the behavior of the criminals. Distinct from the "crime predicts crime" approaches in criminology that rely only on crime data to predict future crime, this model learns the interaction between patrol officers and criminals using the patrol and crime data, resulting in better crime prediction than prior approaches. The learning approach uses the Expectation Maximization algorithm, and a number of independence assumptions to compactly represent the DBN model in order to avoid over-fitting and to scale up the computation. We also propose a dynamic programming based patrol planning algorithm, which projects crime reduction of up to 50% as compared to the existing patrol strategy used by DPS. This project is now part of the software used by USC police to aid in preventive patrolling.

Ongoing Research Topics in Game Theory for Security

Game theory and adversarial reasoning for security, including homeland security, is a very active area of research. This research includes both theoretical and computational research to improve our understanding of the theoretical foundations of adversarial reasoning, as well as applied research that seeks to use the methods to solve important real-world problems. Successful applied research requires strong collaborations between academic researchers, domain experts, and

end users. Applied research often exposes new fundamental challenges that must be addressed by the research, leading to a virtuous cycle of basic and applied research. We now highlight a few major areas of ongoing research in security games, providing a few examples in each area, while noting that this is far from an exhaustive list.

Scalability: One of the main challenges that arises in using game theory and adversarial reasoning for homeland security is that the decisions are very complex, with an enormous number of possible schedules or strategies that could be used, and difficult constraints that must be satisfied. This has led to a large number of efforts in developing faster computer algorithms for analyzing these problems (Jain, 2010; Shieh 2012).

Robustness: Decision making in the real world almost always involves uncertainty, and this is true in adversarial reasoning problems as well. For example, it may not be possible to predict the exact outcome of a specific type of attack scenario, or to specify exactly what value an attacker places on a specific target. However, these values can be estimated, with varying degrees of accuracy. We have worked to develop better ways to capture uncertainty in our game models, and to be able to find solutions robust to this uncertainty (Kiekintveld 2011 and 2013).

Human Behavior: Predicting the behavior of humans is always challenging, and many of the adversarial problems we face involve decisions against human opponents. While game theory usually assumes that opponents are perfectly rational, humans may have various limitations in their knowledge or reasoning that lead to different decisions. By predicting these weaknesses in human opponents and building these into our models, we can make even better decisions against human opponents (Yang, 2017).

Learning and Adaptation: While most game models to date have focused on static, one-time interactions, in many domains we have a large number of repeated interactions with a single opponent (or set of related opponents). This provides a rich source of data that we can use to improve our adversary models by using learning methods to identify and adapt to the opponent's strategy over time. For example, we have developed learning models that can learn and adapt to the strategies of illegal entrants in a border patrol scenario using apprehension data (Klima, 2014).

Evaluation: Evaluating deployed security systems is a significant challenge for a variety of reasons (Taylor, 2009). We have used a variety of different evaluation techniques, including theoretical analysis, simulation studies, experiments in controlled laboratory settings, evaluations by domain experts, analysis of data from deployed systems, and evaluations based on red team exercises. These evaluations consistently show the advantages of security policies based on adversarial reasoning and game-theoretic analysis over systems using other standard scheduling policies or schedules constructed by human schedulers (Tambe, 2011).

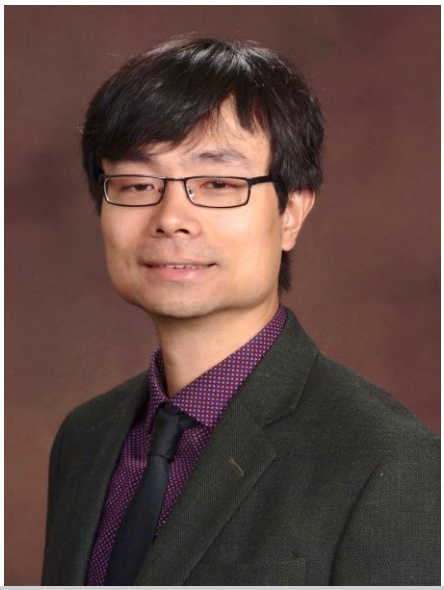
Conclusion

Homeland security and law enforcement represent large investments of resources to combat a wide variety of threats, ranging from terrorism to criminal activity and illegal immigration. Many decisions must be made about how to allocate limited resources effectively in different types of strategic and operating environments, and many of these decisions depend on understanding the behavior of intelligent, adaptive adversaries. Moreover, even though a risk-based method in guiding grant allocations has been implemented by the DHS since 2006, the risk-related measures are still limited. The ability of intelligent adversaries to adapt to defenses is not explicitly taken into account in traditional methods of decision and risk analysis. The next generation of decision support tools being developed based on game theory and adversarial reasoning presents a methodology with mathematical and computational tools to improve decision-making in these very challenging domains.

About the author

Dr. Christopher D. Kiekintveld is an Associate Professor in the Computer Science Department at the University of Texas at El Paso.

For further information related to this work please contact Dr. Kiekintveld at (915) 747-5564 or at cdkiekintveld@utep.edu



About the author

Dr. Jun Zhuang is an Associate Professor and Director of Undergrad Studies, Department of Industrial Systems Engineering at the University a Buffalo.

For further information related to this work please contact Dr. Zhuang at (716) 645-4707 or at jzhuang@buffalo.edu

About the author

Dr. Arunesh Sinha is an Assistant Research Scientist in the Computer Science and Engineering Department at the University of Michigan.

For further information related to this work please contact Dr. Sinha at arunesh@umich.edu

References

Behlendorf, B., Zietz, D., Zhang, J., Zhuang, J., Johns, M. (2015). *Countering the inhumane: modeling probable pathways for human smuggling and trafficking along the U.S.-Mexico border*, START report.

Blocki, J., Christin, N., Datta, A., Procaccia, A.D., Sinha, A. (August, 2013). Audit games. *Proceedings of 23rd International Joint Conference on Artificial Intelligence (IJCAI).*

Blocki, J., Christin, N., A. Datta, A, Procaccia, A.D., Sinha, A. (January, 2015). Audit games with multiple defender resources. *Proceedings of 29th AAAI Conference on Artificial Intelligence (AAAI).*

Brown, M., Sinha, A., Schlenker, A., Tambe, M. (2016). One size does not fit all: A game-theoretic approach for dynamically and effectively screening for threats. *Proceedings of 30th AAAI Conference on Artificial Intelligence (AAAI).*

Hao, M., Jin, S. & Zhuang, J. (2009). Robustness of optimal defensive resource allocations in the face of less than fully rational attackers. *Proceedings of the Industrial Engineering Research Conference*, 886-891.

Hausken, K. & Zhuang, J. (2011). Defending against a stockpiling terrorist, *The Engineering Economist, 56*(4): 321-353.

Hausken, K. & Zhuang, J. (2012). The timing and deterrence of terrorist attacks due to exogenous dynamics. *Journal of the Operational Research Society, 63*(6): 726-735.

Jain, M., Kardes, E., Kiekintveld, C., Ordónez, F. & Tambe, M. (2010). Security games with arbitrary schedules: A branch and price approach. *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI).*

Jose, V. R. R. & Zhuang, J. (2013). Technology adoption, accumulation, and competition in multi-period attacker-defender games. *Military Operations Research, 18*(2): 33-47.

Kiekintveld, C. Jain, M., Tsai, J., Pita, J., Ordóñez, F. & Tambe, M. (2009). Computing optimal randomized resource allocations for massive security games. *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*, 689-696.

Kiekintveld, C., Marecki, J. & Tambe, M. (2011). Approximation methods for infinite Bayesian Stackelberg games: Modeling distributional payoff uncertainty. *Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3*, 1005-1012.

Kiekintveld, C., Islam, T., & Kreinovich, V. (2013). Security games with interval uncertainty. *Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems*, 231-238.

Klíma, R., Kiekintveld, C. & Lisý, V. (2014). Online learning methods for border patrol resource allocation." *International Conference on Decision and Game Theory for Security*, 340-349. Springer International Publishing.

Nikoofal, M. & Zhuang, J. (2012). Robust allocation of a defensive budget considering an attacker's private information. *Risk Analysis, 32*(5), 930-943.

Pita, J., Manish, J., Marecki, J., Ordóñez, F., Portway, C., Tambe, M., Western, C., Paruchuri, P., & Kraus, S. (2008). Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport. *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*, 125-132.

Shan, X. & Zhuang, J. (2013). Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender attacker game. *European Journal of Operational Research, 228*(1), 262-272.

Shieh, E., Yang, R., Tambe, M., Baldwin, C., DiRenzo, J., Maule, B. & Meyer, G. (2012). Protect: A deployed game theoretic system to protect the ports of the United States. *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*, 13-20.

Sinha, A., Kar, D., & Tambe, M., (May, 2016). Learning adversary behavior in security games: A PAC model perspective. *Proceedings of 15th International Conference on Autonomous Agents and Multiagent Systems (AAMAS).*

Song, C. & Zhuang, J. (Forthcoming). Two-stage security screening strategies in the face of strategic applicants, congestions and screening errors. *Annals of Operations Research.*

Tambe, M. (2011). *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge University Press.

Taylor, M., Kiekintveld, C., Western, C., & Tambe, M. (2009). A framework for evaluating deployed security systems: is there a chink in your ARMOR?

Tsai, J., Kiekintveld, C., Ordonez, F., Tambe, M., & Rathi, S. (2009). IRIS-a tool for strategic security allocation in transportation networks.

Wang, X. & Zhuang, J. (2011). Balancing congestion and security in the presence of strategic applicants with private information. *European Journal of Operational Research, 212*(1), 100-111.

Xu, J. & Zhuang, J. (2016). Modeling costly learning and counter-learning in a defender-attacker game with private defender information. *Annals of Operations Research, 236*(1), 271-289.

Yang, R., Kiekintveld, C., Ordóñez, F., Tambe, M. & John, R. (2013). Improving resource allocation strategies against human adversaries in security games: An extended study. *Artificial Intelligence* 195, 440-469.

Zhang, J., Sinha, A., Tambe, M. (May, 2015). Keeping pace with criminals: Designing patrol allocation against adaptive opportunistic criminals. *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems (AAMAS).*

Zhang, J. & Zhuang, J. (Under Review). Modeling and validating multi-period, multi-type, and multi-target attacker-defender games. *Military Operations Research.*

Zhang, J., & Zhuang, J. (2017). Validation, verification, and uncertainty quantification for models with intelligent adversaries. In *Handbook of Uncertainty Quantification, R. Ghanem, D. Higdon and H. Owhadi (eds.), Springer, 1-19*.

Zhang, J., Zhuang, J. & Behlendorf, B. (Under Revision). Stochastic shortest path network interdiction considering partially strategic attackers with a case study of Arizona-Mexico border. *Reliability Engineering & System Safety.*

Zhuang, J. & Bier, V.M. (2007). Balancing terrorism and natural disasters-Defensive strategy with endogenous attack effort. *Operations Research 55*(5), 976-991.

Zhuang, J. & Bier, V.M. (2010). Reasons for secrecy and deception in homeland-security resource allocation. *Risk Analysis, 30*(12), 1737-1743.

Zhuang, J. & Bier, V.M. (2011). Secrecy and deception at equilibrium, with applications to anti-terrorism resource allocation. *Defence and Peace Economics, 22(1), 43-61.*

Zhuang, J., Bier, V.M. & Alagoz, O. (2010). Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research, 203*(2), 409-418.

Zhuang, J., Bier, V.M. & Guikema, S. (Eds.). (April 2016). Risk Analysis, Special issue on "Validating Models of Adversary Behavior.

BTI Institute

Borders • Trade • Immigration

A Department of Homeland Security Center of Excellence

http://www.uh.edu/bti

Twitter: @CBTIR_UH

CENTER FOR LAW AND HUMAN BEHAVIOR

http://clhb.utep.edu

Twitter: @1CLHB