Preface to the Focused Issue on Dynamic Games in Cyber Security

Saurabh Amin¹ · Karl Henrik Johansson²

Published online: 1 November 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

Dynamic games offer a natural paradigm to model and analyze security of networked systems. Many game-theoretic models have been introduced in recent years to capture the strategic interactions between multiple agents or decision makers, with a focus on security and efficiency as conflicting objectives. More sophisticated models include asymmetric information or dynamically evolving network security. Realistic models that can be analyzed rigorously and offer relevant insights are needed to address important issues such as vulnerability assessment, analysis of network security and cyber-induced failures, incentivizing investments in security, and design of mechanisms to reduce risks. To promote further research in this subject, *Dynamic Games and Applications* is publishing the focused issue “Dynamic Games in Cyber Security.” This issue features five papers on game-theoretic models and analysis approaches for cyber and cyber-physical security of networked systems.

The first paper “Dynamic Games in Cyber-Physical Security: An Overview,” by Etesami and Başar, provides a comprehensive survey of the field and serves as an introduction to the special issue. The authors focus on cyber-physical security (as opposed to just cyber security) problems where dynamic interaction between the main players (i.e., attackers and defenders) is a key feature. The paper is structured around applications and topical areas so that the reader can get a broad perspective on how game theory can be applied to a range of topics in the field. Specific topics include: Network security including intrusion detection and risk assessment; Security games including signaling, deception, and Stackelberg models; Physical-layer security against jamming and eavesdropping attacks; Applications of incentive or mechanism design to security problems; Optimal resource allocation for security; and Learning algorithms for finding optimal attack and defense strategies. In their discussion of these topics, the authors include references to recent advancements and discuss key issues in the analysis of dynamic games for security problems.

The second paper “An Efficient Dynamic Allocation Mechanism for Security in Networks of Interdependent Strategic Agents,” by Farhadi, Tavafoghi, Teneketzis, and Golestani, contributes to the topic of incentive design in dynamic networked systems. The authors consider a model of networked system with strategic agents who have private information about their security state. Over time, the agents face security threats of outside attacks as well as from

✉ Karl Henrik Johansson
kallej@kth.se

¹ MIT, Cambridge, USA

² KTH Royal Institute of Technology, Stockholm, Sweden

their insecure neighbors. The model is quite general in that it considers agents with correlated private state (types) and interdependent valuations (owing to the network structure). The authors address the problem of dynamic allocation of limited security resources by designing an incentive mechanism that aligns the selfish objective of each agent with the social welfare. In contrast to the existing negative results in static mechanism design, the authors show that, in addition to being efficient, their dynamic monetary mechanism is *ex ante* individual rational and budget balanced. Importantly, by exploiting the inter-temporal correlation among the agents' security states, the authors show that it is possible to determine a set of inference signals for all agents that are independent of their own reports. By using a collection of past inference signals, the mechanism also achieves approximate *ex post* individual rationality and budget balance.

The third paper "Iterative Computation of Security Strategies of Matrix Games with Growing Action Set," by Li and Langbort, is motivated by cyber security scenarios in which attackers can suddenly start exploiting new or previously unknown vulnerabilities in their strategic play against the defender. To study such scenarios, the authors adopt a zero-sum game model in which one player's action set gradually increases. The main contribution is an approach to efficiently update saddle-point or security strategy of the game. Essentially, the equilibrium strategy of one player can be solved by a linear program, and adding actions of the other player is equivalent to adding constraints to the program. The authors develop an iterative shadow vertex method for solving the linear program with large number of constraints. They show that the computational complexity of their method is strictly less than that of the original shadow vertex method. Moreover, the paper provides a method to identify whether or not the saddle-point strategy changes, and it analyzes the probability of recomputing it.

The fourth paper "Supervisory Control of Discrete-event Systems under Attacks," by Wakaiki, Tabuada, and Hespanha, is motivated by issues in computer security where the cyber defense system must make decisions based on sensor outputs that may have been compromised by an attacker. The authors consider a zero-sum multi-adversary version of the supervisory control problem for discrete-event systems. In this problem, the supervisor faces multiple adversaries with distinct action spaces and needs to find a policy that wins against any of its possible adversaries, without knowing the opponent's identity. On the other hand, the adversary manipulates the string of output symbols used by the supervisor in making decisions. The authors provide a necessary and sufficient condition for this multi-adversary game to have a "solution," i.e., for the existence of a supervisor that can win against any of the adversaries. This condition is expressed in terms of a well-known controllability condition and a novel observability condition (that accounts for the presence of adversaries). The authors further explore this condition for the case of "output-symbol attacks," in which each adversary is limited to insert symbols into or remove symbols from the output string. For this case, the authors show that a supervisor for the multi-adversary setting can be obtained using tools developed for the classical discrete-event supervisory control problem, without incurring additional computational complexity.

Finally, the paper "Securing Infrastructure Facilities: When Does Proactive Defense Help?" by Wu and Amin investigates the resource allocation problem faced by an infrastructure agency in securing a set of facilities (components) to reduce the impact of an attacker who can strategically target a single facility. The proposed game-theoretic model captures the trade-off faced by the agency between system efficiency and costly defense investment, as well as the priority of facilities in terms of criticality. To quantify the effectiveness of proactive security investments, the authors characterize the equilibrium structure of the simultaneous game and the sequential game in which defender moves first. They show that the defender

has “first mover advantage” if and only if the per-facility defense cost is lower than an identified threshold, which is a function of the attack cost. Under this condition, the attack can be fully deterred by proactively securing all vulnerable facilities (i.e., the ones which are profitable targets for the attacker) at an appropriate level of effort. The authors also show that more critical facilities (i.e., the ones that result in higher usage cost when compromised) are secured more by the defender and hence will be targeted less by the attacker. Furthermore, increasing the technological cost of attack makes fewer facilities vulnerable to attack. On the other hand, reducing the defense cost leads to defender investing on a larger set of vulnerable facilities and attacker dispersing the attack effort on less critical facilities.

We hope that the five papers presented in this focused issue will lead to more interest in dynamic games for cyber and cyber-physical security applications. We believe that sustained progress in topics such as dynamic and stochastic games of incomplete information, mechanism design for networked systems, resource allocation games for optimal security investment, and models of learning in strategic environments will enhance our ability to analyze important problems in security and resilience of networked systems.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.