# Game Theoretical Modelling of Network/Cybersecurity

**AZHAR IQBAL** [1,2,3], **LACHLAN J. GUNN** [4], **MINGYU GUO** [5],
**M. ALI BABAR** [5], **AND DEREK ABBOTT** [1], (Fellow, IEEE)

[1] School of Electrical and Electronic Engineering, The University of Adelaide, Adelaide, SA 5005, Australia
[2] Sage International Australia, Torrensville, SA 5031, Australia
[3] Interactive Decisions, Flinders Park, SA 5025, Australia
[4] Department of Computer Science, Aalto University, FI-00076 AALTO, Finland
[5] School of Computer Science, The University of Adelaide, Adelaide, SA 5005, Australia

Corresponding author: Azhar Iqbal (azhar.iqbal@adelaide.edu.au)

**ABSTRACT** Game theory is an established branch of mathematics that offers a rich set of mathematical tools for multi-person strategic decision making that can be used to model the interactions of decision makers in security problems who compete for limited and shared resources. This article presents a review of the literature in the area of game theoretical modelling of network/cybersecurity and identifies a number of challenges in this area that need to be addressed.

**INDEX TERMS** Cyberspace, mathematical model, optimization methods, cybersecurity, game theory, network security.

## I. INTRODUCTION

For most physical security situations the outcomes depend on the actions of both attackers and defenders. The attackers and defenders act rationally and can depend on various incentives that may be diametrically opposite or, under other circumstances, may have some overlap. Physical security thus provides the situations where the tools of game theory can be beneficially applied and can provide insights into making optimal security decisions. For various decision-making problems arising in physical security, game theory can provide a rich set of analytical methods and mathematical tools.

The pervasive use of the Internet opens up numerous network security situations. The attackers and defenders in typical situations are rational agents who have the ability to act strategically. The agents can be assumed to be interested in finding either the most damaging or the most secure use of available resources. In the domain of network security, game theory has been shown [1], [2] to provide useful insights in making decisions that lead to developing novel, analytic, computational, and practical approaches in the thought, policy, planning, and strategic action. Game theory provides methodical approaches in order to explain the inter-dependencies of the role of hidden and asymmetric information in networks, network security decisions [3], [4],

The associate editor coordinating the review of this manuscript and approving it for publication was Francesco Tedesco [ID].

the incentives/limitations of the attackers, the perception of risks and costs in human behavior, and much more. The elegant and powerful tools made available by game theory are found to be highly useful in order to build secure, resilient, and dependable networked systems [5], [6].

## II. GAME THEORY

Game theory [7]–[13] is an established branch of mathematics that develops mathematical models, allowing rigorous analysis, of strategic interaction between rational decision-makers. It studies complex, competitive, and multi-agent interactions in which one player's utility depends not only on his decisions, but also on the decisions of his opponents. Game theory is applied to a number of disciplines, including economics [14], [15], biology [16]–[18], political science [19], [20], electrical engineering [23], [24], business [25], [26], computer science [21], [22], law [27], [28], public policy [29], physical security [30], [31], mechanism design [32]–[34], and more recently to the quantum information [35]–[38]. Game theory can enable opponents to predict each other's rational behavior and suggest a course of action to be taken in any given situation.

### A. STATIC AND DYNAMIC GAMES

Games considered in the field of game theory are broadly classified as being the *static* or *dynamic* games [10], [11] .

In static games the players choose their strategies simultaneously whereas dynamic games involve a sequence of moves. In dynamic games [39], [40], a player chooses before others do, knowing that the others' choices will be influenced by his/her publicly observable choice. The dynamic character of the game results in models that can enhance the learning ability of the players. In turn, this learning can help security practitioners to develop high quality theoretical studies on real-life problems. Depending on a particular situation in cybersecurity that are amenable to game theoretical analyses, applying either static or dynamic game theory can considered appropriate. For instance, a cybersecurity situation involving a team of attackers and a plan of attack in which the attackers act simultaneously, the application of static game theory will be required. Whereas, dynamic game theory will be applied when some of the attackers act first and the reaction of the defenders is observed before the remaining attackers act while equipped with the knowledge of how the defenders have reacted.

### B. NASH EQUILIBRIUM

The rule for predicting how a game will be played defines the *solution concepts* in terms of which the game is understood by game theorists. The most commonly used solution concept in game theory is that of a Nash equilibrium (NE). Assume there are $N$ players in a game. Let $S_i$ and $U_i$ for $1 \leq i \leq N$ be the strategy spaces and the payoff, or utility, for each player $i$, respectively. The individual elements of the strategy space $S_i$ for player $i$ are called the *pure strategies* . The game can then be described [41] by the set $G$ :

$$G : \{N; S_1, S_2, \ldots S_N; U_1, U_2, \ldots U_N\}. \quad (1)$$

The presumable outcome of the game is determined by analyzing the behaviour of the players and their strategy choices. Let $s = \{s_1, s_2, \ldots s_N\}$ be the profile of pure strategies with $s_i \in S_i$. Let $s_{-1}$ be the profile of strategies excluding player $i$. A strategy profile $s$ with $s = (s_i; s_{-i})$ for all $i$, is a NE [7], [10], [13], [43], [44] such that for all $1 \leq i \leq N$ we have

$$U_i(s) \geq U_i(t; s_{-i}) \text{ for all } t \in S_i. \quad (2)$$

This is also described by stating that the strategy of each player $i$ is a *best reply* [7], [10], [13] to the strategies of other players. In the cybersecurity context, the defenders' strategy profile that is a NE will consist of a set of defensive strategies, one on the behalf of each defender, such that the strategy of each defender is a best reply to the strategies of the attackers.

### 1) NASH EQUILIBRIUM IN MIXED STRATEGIES

A *mixed strategy* [13] is a linear combination, with real coefficients, of two or more pure strategies, with their probability weights summing up to 1. This defines the probability distribution $\pi_i = (\pi_{i,t})_{t \in S_i}$ for player $i$ choosing randomly among the pure strategies $S_i$. The expected payoff for the player $i$ is then given [41] by

$$\bar{U}_i(s_1, s_2, \ldots s_N) = \sum_{j=1}^{N} \sum_{s_j \in S_j} U_i(s_1, s_2, \ldots s_N) \Pi_{k=1}^{N} \pi_{k,s_k}. \quad (3)$$

A set of probability distributions $\pi_i = (\pi_i)_{1 \leq i \leq N}$ defines a mixed NE, or a NE in mixed strategies, such that for all $i$ and any other probability distribution $\bar{\pi}_i = (\pi_{i,t})_{t \in S_i}$ we have

$$\sum_{j=1}^{N} \sum_{s_j \in S_j} U_i(s_1, s_2, \ldots s_N) \Pi_{k=1}^{N} \pi_{k,s_k}$$
$$\geq \sum_{t \in S_i} \sum_{j \neq i} \sum_{s_j \in S_j} U_i(t; s_{-i}) \bar{\pi}_{i,t} \Pi_{k \neq i} \pi_{k,s_k}. \quad (4)$$

A key result of Nash's thesis [43], [44] states that a NE always exists in mixed (randomized) strategies in games where each player has only a finite number of deterministic strategies. In a NE, no one player can improve his/her situation by unilaterally changing his/her strategy. This amounts to stating that each person is doing as well as they possibly can, even if that does not mean that an optimal outcome has been achieved for the collective of all players. In a cyber attack when a NE is determined for a team of defenders, neither is left with any motivation to deviate unilaterally from it.

### 2) PRISONERS' DILEMMA

The game of *Prisoners' Dilemma* (PD) [7], [10], [13] describes the following situation: a) Two criminals, called in the following as Alice and Bob, commit a crime together and are arrested. As the evidence is being investigated, they wait for their trial, b) Each suspect is offered the opportunity to confess the crime after placing him/her in a separate cell, c) Each suspect may choose between the strategies of confessing ($\mathcal{D}$) or not confessing ($\mathcal{C}$), where $\mathcal{C}$ and $\mathcal{D}$ represent the pure strategies of *cooperation* and *defection* with one's partner in the crime and not with the authorities, d) If neither of the two confesses, i.e. $(\mathcal{C}, \mathcal{C})$, they both go free, and divide between them the proceeds of their crime. We represent this in the following by 3 units of payoff to each prisoner, e) However, if one prisoner confesses ($\mathcal{D}$) and the other does not ($\mathcal{C}$), the prisoner who confesses testifies against his partner in exchange for going free and gets the entire 5 units of payoff. However, the prisoner who did not confess is sent to prison and that is represented by the payoff of zero, f) If both suspects confess, i.e. $(\mathcal{D}, \mathcal{D})$, then both are convicted while a reduced term is given to both. This is represented by giving each suspect 1 unit of payoff. This payoff is better than having the other suspect confess, but it is not so good as going free. The game between the prisoners can be represented by the following bimatrix of payoffs:

$$\begin{array}{c} \text{Bob} \\ \begin{array}{cc} \mathcal{C} & \mathcal{D} \end{array} \\ \text{Alice} \begin{array}{c} \mathcal{C} \\ \mathcal{D} \end{array} \begin{pmatrix} (3, 3) & (0, 5) \\ (5, 0) & (1, 1) \end{pmatrix} \end{array} \quad (5)$$

where the first and the second entry in a bracket correspond to Alice's and Bob's payoff, respectively. Let Alice play $\mathcal{C}$ with probability $p$ and play $\mathcal{D}$ with probability $(1 - p)$. Similarly, let Bob play $\mathcal{C}$ with probability $q$ and play $\mathcal{D}$ with probability $(1 - q)$. The players' payoffs for the PD matrix (5) are

$$U_A(p, q) = -p + 4q - pq + 1, \quad U_B(p, q) = 4p - q - pq + 1. \tag{6}$$

The inequalities that define the NE consisting of a pair of mixed strategies $(p^*, q^*)$ in PD can then be written as

$$U_A(p^*, q^*) - U_A(p, q^*) = -(p^* - p)(1 + q^*) \geq 0,$$
$$U_B(p^*, q^*) - U_B(p^*, q) = -(q^* - q)(1 + p^*) \geq 0, \tag{7}$$

which produces a unique NE in PD: $p^* = q^* = 0$. The NE corresponds to both players playing the pure strategy $\mathcal{D}$. Reference [42] Utilizes an international relations PD game to present an explanation of the complexities of cyber intrusions and the way forward for nation-states to deal with these new exigencies. The PD game is also discussed in the context of cybersecurity in [54].

### 3) REFINEMENTS OF NASH EQUILIBRIUM

Some of the largest problems in security applications come from actions that cannot be anticipated. This makes using NE problematic as the concept presumes that the structure of the game, as well as all possible moves, is common knowledge among the players. Several refinements of the NE have been introduced [8], [12] including *sequential equilibrium*, *proper equilibrium*, *trembling hand equilibrium*, and *rationalizability*.

### C. SEQUENTIAL OR STACKELBERG GAMES

A dynamic model of the duopoly game was proposed by Stackelberg (1934) [11], [45] in which a leader (or dominant) firm moves first and in view of the leading firm's move a follower (or subordinate) firm moves second. For instance, in the early history of US mobile industry, General Motors played this leadership role against more than one firm such as Ford and Chrysler who acted as followers. In the sequential game of duopoly a *Stackelberg equilibrium* is obtained using the solution concept of *backwards-induction outcome* of the game. As a solution-concept it is stronger than that of NE and refers to sequential nature of the game. Multiple NE may appear in sequential move games whereas only one of those is associated with the backwards-induction outcome of the game.

Consider the following simple three step game, a) Player 1 chooses an action $a_1$ from the set $A_1$ of his strategies, b) Player 2 observes $a_1$ and then chooses an action $a_2$ from the set $A_2$ of her strategies, c) Payoffs for the two players are $U_1(a_1, a_2)$ and $U_2(a_1, a_2)$. It is an example of the dynamic games of complete and perfect information whose key features are, a) Players take their moves in sequence, b) All previous moves are known to the players they make a next move, and c) The players' payoff functions are common knowledge. Given the action $a_1$ is previously chosen, at the second stage of the game when player 2 takes his turn to make the move he faces the problem:

$$\underset{a_2 \in A_2}{\text{Max}} \, U_2(a_1, a_2). \tag{8}$$

Assume that for each $a_1$ in $A_1$, player 2's above optimization problem has a unique solution $R_2(a_1)$, which is the best response of player 2. By anticipating player 2's response to each action $a_1$ that player 1 might take, Player 1 can now solve player 2's optimization problem. So that player 1 faces the problem:

$$\underset{a_1 \in A_1}{\text{Max}} \, U_1(a_1, R_2(a_1)). \tag{9}$$

Assuming that this optimization problem has a unique solution for player 1 and it is denoted by $a_1^\star$. The solution $(a_1^\star, R_2(a_1^\star))$ is then called as the *backwards-induction outcome* of this game. In [46] Damjanovic-Behrendt presents an approach to optimize the cybersecurity decisions in order to protect instances of a federated Internet of Things platform in the cloud. His solution implements the repeated Stackelberg security game. An overview of use-inspired research in Stackelberg security games is presented in [47].

### D. REPEATED GAMES

A specific class of dynamic games are the repeated games in which the players play the same game more than once. Players observe the outcome of the first play before the start of the second play. Payoffs for the entire game are then obtained as the sum of the payoffs from the previous stages. Generally, repeated games have a strategic structure that is more complex than it is in their one-stage counterpart. This is because the players' strategic choices in the following stages are influenced by the outcome of the choices they make in an earlier stage.

A two-stage game of complete but imperfect information is sequential in that the players' moves in the first stage are observed before the next stage begins. The simultaneity of the players' moves in each stage result in the imperfect information in the game. Such a game consists of these steps [11], a) Players $A$ and $B$ simultaneously choose their moves $p$ and $q$ from their strategy sets $\mathcal{P}$ and $\mathcal{Q}$, respectively, b) Players $A$ and $B$ observe outcome of the first stage of the game, $(p, q)$, and they then simultaneously choose actions $p_1$ and $q_1$ from the sets $\mathcal{P}$ and $\mathcal{Q}$, respectively, c) Payoffs are $U_i(p, q, p_1, q_1)$ for $i = A, B$. Usually, the games from this class are solved using the method of backwards-induction. This involves solving the simultaneous-move game between players $A$ and $B$ in the second stage, given the outcome from the first stage. Players $A$ and $B$ can anticipate that their second-stage behavior will be given by $(p_1^\star(p, q), q_1^\star(p, q))$. In view of this, the first-stage interaction between the players becomes equivalent to the following simultaneous-move game: a) Players $A$ and $B$ simultaneously choose actions $p$ and $q$ from sets $\mathcal{P}$ and $\mathcal{Q}$, respectively, b) Payoffs are $U_i(p, q, p_1^\star(p, q), q_1^\star(p, q))$ for $i = A, B$. When $(p^\star, q^\star)$ is the

unique NE of this simultaneous-move game, the set of four numbers $(p^\star, q^\star, p_1^\star(p, q), q_1^\star(p, q))$ is known as the *subgame-perfect outcome* [11] of this two-stage game. This solution concept is the natural analog of the backwards-induction outcome in games of complete and perfect information.

Consider the PD game given by the matrix (5) for which the players play the game twice and the outcome of the first play is observed before the second stage begins. Payoffs for the entire game are then obtained as the sum of the payoffs from the two stages of the game. The game is a two-stage game of complete but imperfect information [11] . Assume players $A$ and $B$ play the pure strategy $C$ with probabilities $p$ and $q$, respectively, in stage 1. Also assume the players $A$ and $B$ play the strategy $C$ with probabilities $p_1$ and $q_1$, respectively, in stage 2. Let $U_{A1}$ and $U_{B1}$ represent the payoffs to players $A$ and $B$, respectively, in the stage 1. From Eqs. (6) these payoffs are $U_{A1} = -pq + 4q - p + 1$ and $U_{B1} = -pq + 4p - q + 1$. The NE conditions for this stage are $U_{A1}(p^\star, q^\star) - U_{A1}(p, q^\star) \geq 0$, $U_{B1}(p^\star, q^\star) - U_{B1}(p^\star, q) \geq 0$ giving $p^\star = q^\star = 0$ (i.e. defection for both the players) as the unique NE in this stage. Similarly, in the second stage the payoffs to players $A$ and $B$ are expressed as $U_{A2}$ and $U_{B2}$ respectively, where $U_{A2} = -p_1q_1 + 4q_1 - p_1 + 1$, $U_{B2} = -p_1q_1 + 4p_1 - q_1 + 1$. Therefore, the strategy of defection, i.e. $p_1^\star = q_1^\star = 0$, once again comes out as the unique NE in the second stage. To compute the subgame-perfect outcome of this two-stage game, we analyze its first stage given that the second-stage outcome is also the NE of that stage — namely $p_1^\star = q_1^\star = 0$. For this NE the players' payoffs in the second stage are $U_{A2}(0, 0) = 1$, $U_{B2}(0, 0) = 1$. The players' first-stage interaction, therefore, in this two-stage game becomes equivalent to a one-shot game, in which the payoff pair $(1, 1)$ from the second stage is added to their first-stage payoff pair. We can write the players' payoffs in the one-shot game as $U_{A(1+2)} = U_{A1} + U_{A2}(0, 0) = -pq + 4q - p + 2$, and $U_{B(1+2)} = U_{B1} + U_{B2}(0, 0) = -pq + 4p - q + 2$. It has again $(0, 0)$ as the unique NE. The unique subgame-perfect outcome of the two-stage PD, therefore, is $(0, 0)$ in the first stage, and it is also $(0, 0)$ in the second stage. The strategy of defection in both the stages comes out as subgame-perfect outcome for the two stage classical PD.

### E. COOPERATIVE GAMES

In cooperative games, players are allowed to form coalitions, binding agreements, pay compensations, make side payments etc and there is a strong incentive to work together to receive the largest total payoff. In their pioneering work on game theory [14], von Neumann and Morgenstern offered models of coalition formation where the strategy of each player consists of choosing the coalition s/he wishes to join. In coalition games the players' possibilities are described by the available resources of different groups (coalitions) of players and joining a group, or remaining outside, is part of strategy of a player affecting his/her payoff. The notion of a strategy disappears in a cooperative game and the notion of a coalition and the value or worth of that coalition attain

significance. It is assumed that each coalition can guarantee for its members a certain amount that is called the *value of a coalition* [8], [13]. It measures the worth of the coalition that is obtained as the payoff which the coalition can guarantee for itself if it selects an appropriate strategy. However, the 'odd man' can prevent the coalition from receiving more than this amount.

An example of a three-player symmetric cooperative game is a classical three-person normal form game [48] that is defined by:

a) Three non-empty sets $\Sigma_A$, $\Sigma_B$, and $\Sigma_C$ that are the strategy sets of the players $A$, $B$, and $C$,

b) Three real valued functions $U_A$, $U_B$, and $U_C$ that are defined on $\Sigma_A \times \Sigma_B \times \Sigma_C$, and

c) The product space $\Sigma_A \times \Sigma_B \times \Sigma_C$ that is the set of all tuples $(\sigma_A, \sigma_B, \sigma_C)$ with $\sigma_A \in \Sigma_A$, $\sigma_B \in \Sigma_B$ and $\sigma_C \in \Sigma_C$.

For this game, a strategy is understood as such a tuple $(\sigma_A, \sigma_B, \sigma_C)$ and $U_A$, $U_B$, $U_C$ are payoff functions of the three players and the game can be denoted as $\Gamma = \{\Sigma_A, \Sigma_B, \Sigma_C; U_A, U_B, U_C\}$.

Let $\Re = \{A, B, C\}$ represent the set of players and assume that $\wp$ is an arbitrary subset of $\Re$. Players in $\wp$ may form a coalition so that the coalition $\wp$ can be considered as a single player. It is expected that players in $(\Re - \wp)$ will form an opposing coalition and the game has two opposing "coalition players" i.e. $\wp$ and $(\Re - \wp)$. One of the two strategies 1, 2 is chosen by each of the three players $A$, $B$, and $C$ . There is no payoff if the three players choose the same strategy. If the two players choose the same strategy, both receive one unit of money from the 'odd man.' The payoff functions $U_A$, $U_B$ and $U_C$ for players $A$, $B$ and $C$, respectively, are given as [48]:

$$U_A(1, 1, 1) = U_A(2, 2, 2) = 0,$$
$$U_A(1, 1, 2) = U_A(2, 2, 1) = U_A(1, 2, 1) = U_A(2, 1, 2) = 1,$$
$$U_A(1, 2, 2) = U_A(2, 1, 1) = -2, \tag{10}$$

with similar expressions for $U_B$ and $U_C$. Suppose $\wp = \{B, C\}$, hence $\Re - \wp = \{A\}$. The coalition game represented by $\Gamma_\wp$ is given by the payoff matrix:

$$\begin{array}{c} \\ [11] \\ [12] \\ [21] \\ [22] \end{array} \begin{array}{c} [1]\ [2] \\ \begin{pmatrix} 0 & 2 \\ -1 & -1 \\ -1 & -1 \\ 2 & 0 \end{pmatrix} \end{array}. \tag{11}$$

Here the strategies [12] and [21] are dominated by [11] and [22]. After eliminating these dominated strategies the payoff matrix becomes

$$\begin{array}{c} \\ [11] \\ [22] \end{array} \begin{array}{c} [1]\quad [2] \\ \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \end{array}. \tag{12}$$

It is seen that the mixed strategies:

$$\frac{1}{2}[11] + \frac{1}{2}[22], \text{ and } \frac{1}{2}[1] + \frac{1}{2}[2], \tag{13}$$

are optimal for $\wp$ and $(\Re - \wp)$ respectively. With these strategies a payoff 1 for players $\wp$ is assured for all strategies of the opponent; hence, the value of the coalition $\upsilon(\Gamma_\wp)$ is 1 i.e. $\upsilon(\{B, C\}) = 1$. Since $\Gamma$ is a zero-sum game $\upsilon(\Gamma_\wp)$ can also be used to find $\upsilon(\Gamma_{\Re-\wp})$ as $\upsilon(\{A\}) = -1$. The game is symmetric and one can write

$$\upsilon(\Gamma_\wp) = 1, \quad \text{and} \quad \upsilon(\Gamma_{\Re-\wp}) = -1 \text{ or,}$$
$$\upsilon(\{A\}) = \upsilon(\{B\}) = \upsilon(\{C\}) = -1,$$
$$\upsilon(\{A, B\}) = \upsilon(\{B, C\}) = \upsilon(\{C, A\}) = 1. \quad (14)$$

Cooperative game theory has been applied to cybersecurity in a number of studies: In a Masters thesis submitted to the Florida Atlantic University, Golchubian [56] has used cooperative game theory by developing a game theoretical approach to prevent collusion and to incentivize cooperation in cybersecurity contexts. Vakilinia and Sengupta [57] have investigated profit sharing in coalitional game theory using calculation for rewarding the players that is participation-fee. In particular, they analyze the well-known *Shapley value* concept [10], [11] by formulating a coalitional game between organizations in cybersecurity information sharing system.

### F. BAYESIAN GAMES
In other situations that are characterized by the players' access to only a partial knowledge about the game, game theory is still shown to be an effective modelling tool by exploiting the concepts from Bayesian games [11]. A Bayesian game is defined as a game of incomplete information in which the players do not have the complete knowledge of the rules of the game. The incomplete knowledge is described by the existence of the so-called state of Nature, which is decided probabilistically by some relevant random source. In Bayesian games, the probability distribution over the states of Nature is private to each player and which represents each player's knowledge about Nature. Nature is allowed to leak some information about its state in the Bayesian games, which is called the signal to the players. With the signal, the players can probabilistically work out their expected utilities. A Bayesian game [55] consists of a tuple $\langle N, \Omega, \langle S_i, T_i, C_i, \tau_i, p_i, U_i \rangle_{i \in N} \rangle$ where $\Omega$ is the set of natural states, and for each player $i \in N$,

　a) $S_i$ is the set of player $i$'s all available actions,

　b) $T_i$ is the set of player $i$'s signals/types, with $\tau_i : \Omega \longrightarrow T_i$ is the state-to-signal mapping,

　c) $C_i : T_i \longrightarrow 2^{S_i}$ is the set of $i$'s available actions after receiving $t_i \in T_i$,

　d) $p_i$ is the probability measure over $\Omega$, and,

　e) $U_i : \Omega \times S \longrightarrow \mathcal{R}$ is player $i$'s utility function where $\mathcal{R}$ is the set of real numbers.

The solution concept of a NE is adapted into Bayesian games and is called Bayesian NE. Some applications of Bayesian games include Liu et al's. [58] computation of Bayesian Nash outcomes for an intrusion detection game and under the conditions of limited information, Johnson et al's

[59] determination of Bayesian Nash equilibria for network security games.

## III. NETWORK/CYBERSECURITY AND GAME THEORY
The information technology landscape has been revolutionized by the recent advances in software and hardware technologies. Cyberspace has now become an integral part of the way the business is conducted. For current telecommunication and information networks, their network/cybersecurity is the main concern and the protection and security of cyberspace infrastructure is of key importance.

Game theory is applied to networks in settings in which agents are connected by physical or virtual links. Given the network structure and the actions of other users of the network, the agents must decide on some action in a strategic manner.

Heterogeneous, large-scale, and dynamic networks define the cyberspace of the present time. Cyberspace has become increasingly complex even within carefully designed network and software infrastructures. Ample and a large attack surface is available for evasive maneuvers of adversaries in the cyberspace. Cyberspace has become characterized by higher computational power and ubiquitous connectivity and these features have given birth to new risks and threats.

The miscreants launching cybersecurity attacks have various degrees of uncertainty and defenders have incomplete information about their intentions and capabilities. Improving cybersecurity thus involves difficult challenges and decision making on multiple levels and over different time scales. The goal of cybersecurity is to provide practical and scalable security mechanisms and to enhance the trustworthiness of cyber-physical systems.

As is the case with the physical security, in cybersecurity there exists a wide variety of the agents' utilities, including adversarial and antithetical types. Game theory, therefore, shares many common features with the cybersecurity problem. The success of a cybersecurity scheme depends not only on the actual cyberdefense strategies that have been implemented, but also on the strategic actions taken by the attackers to launch their attacks. Thus these scenarios are well-suited to the game theoretical analyses of the cybersecurity schemes. Such analyses can also be viewed from the perspective of establishing trust. When security is compromised, building trustworthy relationships, and deciding whether to trust received information becomes particularly relevant. It is well known [60] that the trust problem can be formulated as in game-theoretic strategic terms. Trust emerges as an important aspect in the design and analysis of security solutions and the implementations of security games involve several levels of trust.

### A. NETWORK/CYBERSECURITY GAMES
A significant motivation for cybersecurity games comes from earlier applications of game theory to the domain of physical security. These are examples of practical situations that demonstrate the potential for game theory in that domain.

Physical security considerations are important at airports, product transportation, national security patrols, etc. Usually, a defender allocates the available resources to defend against an attacker whereas the attacker can attempt to compromise targets that the defender is protecting from possible attacks. Most often, the defender can best allocate resources to minimize the chance of success for the attacker and minimize the cost incurred by the defender. How should the defender allocate agents, patrols, surveillance technology, and other resources to minimize the impact of attackers? Examples of physical security situations include, a) the airport security: where the defender can schedule optimal checkpoints and patrols for their agents, b) the coast guard: more efficiently protection can be provided to ferries or ports that are the targets for theft or terrorism. The finite number of agents and limited resources can be allocated in such ways to best counteract wide scale poaching.

In network/cybersecurity situations, the zero-sum games between malicious attackers and the transmitter-receiver pairs can model the problems of jamming and eavesdropping in communication networks. Attackers and defenders are most often considered as the agents in network security problems. Security games form a basis for formal decision making, algorithm development, and in predicting the behaviour of attackers. Security games can be deterministic or stochastic. They can be sequential or hierarchical (Stackelberg game) in which an agent has a certain information advantage over the others. In cooperative or coalitional security games the agents can cooperate to achieve their strategic objectives. Examples of security games in the network/cybersecurity domain include, i) intrusion detection [5], [75], ii) privacy concerns [74], [83], [84], iii) network jamming [76], [77], [79], and iv) eavesdropping in communication networks [78].

Scheduling and deployment of patrols is a key operational problem for those who are responsible for the security of airports, art galleries etc. Alpern *et al.* [49] have presented a class of patrolling games addressing the optimization problem involving randomized, and thus unpredictable, patrols. They have considered the facility to be patrolled as a network or graph Q of interconnected nodes (e.g. rooms, terminals) such that the Attacker has the option to attack any node of Q within a given time T. That is, the attacker requires m consecutive periods that are uninterrupted by the Patroller in order to commit his nefarious act and therefore win. In this approach, the Patroller can follow any path on the graph. The patrolling game turns out to be a win-lose game in which, given best play on both sides, the *Value* is the probability that the Patroller successfully intercepts an attack.

### B. EXAMPLES

We begin by reviewing two examples from the literature in some detail, as reported by Sokri [50] and Durkota *et al.* [65].

### 1) OPTIMAL RESOURCE ALLOCATION IN CYBERSECURITY

Sokri [50] has considered a security game between an attacker *a* and a defender *d* in a system for cyberinfrastructure.

Let $T = \{t_1, t_2, \ldots, t_n\}$ be a set of $n$ targets that are at the risk of being attacked and $S = \{s_1, s_2, \ldots, s_m\}$ a set of resources to protect the targets. Vector $\langle a_t \rangle$ can represent the attacker's mixed strategy where $a_t$ is the probability of attacking the target $t$. The defender's mixed strategy is the vector $\langle p_t \rangle$ where the marginal probability of protecting the target $t$ is $p_t$. Players' access to mixed strategies allows them to play probability distributions over their pure strategies. A strategy profile $\langle a, p \rangle$ is a combination of (mixed) strategies that the attacker and the defender may play. Let $r_d(t)$ be the defender's reward if the attacked target $t$ is covered and $c_d(t)$ his cost if the target is uncovered. Similarly, denote by $r_a(t)$ the attacker's reward if the attacked target $t$ is uncovered and by $c_a(t)$ the attacker's costs if the attacked target $t$ is covered. For the strategy profile $\langle a, p \rangle$ following are the expected payoffs of the two players:

$$U_d(a, p) = t \in T a_t \left[ p_t r_d(t) - (1 - p_t) c_d(t) \right], \quad (15)$$

$$U_a(a, p) = t \in T a_t \left[ (1 - p_t) r_a(t) - p_t c_a(t) \right]. \quad (16)$$

The payoffs in Eqs. (15,16) depend only on the attacked targets and their protection and these payoffs do not consider the targets that are not attacked. Now, if the players move simultaneously, the solution of this cybersecurity game is a NE. However, if the game is played sequentially in which the defender moves first (leader) and commits to a strategy and the attacker (follower) reacts to the defender's move, the Stackelberg equilibrium appears as the standard solution in this leader-follower interaction.

Given the defender's strategy $p$, the attacker's optimization problem can be presented as follows:

$$\text{Max}_a t \in T a_t \left[ (1 - p_t) r_a(t) - p_t c_a(t) \right], \quad (17)$$

$$\text{s. t. } t \in T a_t = 1, \quad a_t \geq 0, \ \forall t \in T. \quad (18)$$

It is optimal to assign 1 to any $a_t$ that is associated with a maximal value of

$$U_a(t, p) = (1 - p_t) r_a(t) - p_t c_a(t), \quad \forall t \in T. \quad (19)$$

The dual problem that corresponds to the above has the same optimal solution and it can be formulated as follows:

$$\text{Min } u, \quad (20)$$

$$u \geq U_a(t, p), \ \forall t \in T. \quad (21)$$

The complementary slackness condition then becomes:

$$a_t(u - U_a(t, p)) = 0, \quad \forall t \in T. \quad (22)$$

When the leader problem is completed by including the follower's optimality condition, it becomes a single *mixed-integer quadratic problem* [51]:

$$\text{Max}_p t \in T a_t \left[ p_t r_d(t) - (1 - p_t) c_d(t) \right], \quad (23)$$

$$\sum_{t \in T} p_t \leq m, \quad (24)$$

$$t \in T a_t = 1, \quad (25)$$

**TABLE 1.** Pay off table [50].

|  | Defender | | Attacker | |
|---|---|---|---|---|
|  | Reward | Cost | Reward | Cost |
| Target 1 | 4 | 3 | 9 | 6 |
| Target 2 | 3 | 2 | 7 | 6 |
| Target 3 | 6 | 4 | 10 | 8 |
| Target 4 | 3 | 2 | 12 | 6 |

$$0 \leq u - U_a(t, p) \leq (1 - a_t)M, \quad \forall t \in T, \quad (26)$$

$$p_t \in [0, 1], \quad \forall t \in T, \quad (27)$$

$$a_t \geq 0, \quad \forall t \in T, \quad (28)$$

$$u \in \mathcal{R}. \quad (29)$$

Eq. (23) maximizes the leader's expected payoff. The coverage to the available resources ($m$) is limited by Eq. (24) whereas Eq. (27) restricts the coverage vector to [0, 1]. The leader's mixed strategy is enforced to be feasible by these two constraints. Eq. (26), where $M$ is a large number, is the complementary slackness condition indicating that the follower's payoff $u$ is optimal for every pure strategy with $a_t > 0$.

Sokri [50] has considered the example of a game in normal form as shown in the Table 1 and that is adapted from the Refs. [52], [53]. There are 4 targets and two resources that can cover any of the two targets. For each target, there are two payoffs i.e. the payoffs of the attacker and the payoffs of the defender. Each payoff consists of two parts i.e. a reward and a cost.

Note that, a) If the target is attacked, the defender can cover a target and get a reward, b) He can also leave the target uncovered and incur a cost if it is attacked, c) If the target is uncovered, the attacker can attack a target and get a reward, and d) If the target is covered he can also incur a cost. By changing the static values in Table 1 to a range of values, an uncertainty can be placed on each variable. Using a three-point estimate (minimum, most likely, and maximum) approach that incorporates this uncertainty, Sokri [50] has determined the following solution, which is found to satisfy all the constraints as well as the numerical convergence criterion:

$$\langle p = (0.5549, \ 0.4994, \ 0.3411, \ 0.6025), \ a = (0, \ 0, \ 0, \ 1) \rangle. \quad (30)$$

The objective did not move significantly after many iterations, and even if it is heavily defended the attacker preferred to attack the most valuable target. The most likely payoffs have the corresponding cumulative distribution function (CDF). This can now be determined With this solution and the median of the defender's average payoff comes out to be approximately 0.95. This gives a 50% probability that the defender's average payoff will be less than 0.95. The values for minimum and maximum of defender's average payoff are then determined to be 0.4261 and 1.5166, respectively.

### 2) THRESHOLD-SETTING TO DETECT DATA EXFILTRATION

Data breach involves strategic interaction between defender and attacker for which game theory provides helpful insights. It is carried out through the process of information exfiltration and involves unauthorized transfer of information. A dynamic (sequential) game model of data infiltration is described by Durkota *et al.* [65] in which the attacker's objective is to exfiltrate as much data as possible before the activity is detected. The defender's objective is to minimize the loss of data before the breach is detected.

The defender records the volume of data that each host at the network uploads over time while using windows of time with fixed lengths. Defender selects a detection threshold $\theta$, chosen from a set $\Theta$ of thresholds, such that if the host uploading data that is more than $\theta$ in the time window then it triggers an alarm.

The defender can set the detection threshold $\theta$ for each host individually. However, it is possible to identify groups of hosts with similar behaviours. For instance, a group can be of type $\lambda$ from the set $\Lambda$ of all types. For a randomly selected host, $P(\lambda)$ then defines the probability that the host is of the type $\lambda$. That is, $P(\lambda)$ is the probability of the concurrence of the host types. It is assumed that both the attacker and the defender know the probability $P(\lambda)$. Two hosts of same types have the common activity pattern i.e. $P(o \mid \lambda)$ gives the probability that a host of type $\lambda$ transfers the amount of data $o \in O$ in a time interval.

It can be the case that even without an attacker's activity a selected threshold $\theta$ is surpassed along with the alarm triggered. These instances are called the false positives and usually it is a time consuming task for the administrators to determine their cause. Certain number of false positives are expected in the defender's strategies and usually their bound is expressed as the constant FP.

The external and internal attackers are called the outsider and the insider, respectively. The nature of information that the insiders and the outsiders have about the targeted organization can be different from each other. Although the outsider may know which host types exist but cannot know which types were compromised. In contrast, the insider knows which host types exist and also which were compromised.

### 3) DEFENDER'S STRATEGY

Defender's pure strategy $\psi$ is a map from the set $\Lambda$ of all types to the set $\Theta$ of thresholds, i.e. $\psi : \Lambda \to \Theta$. Defender's mixed or randomized strategy is $\sigma(\theta \mid \lambda)$ that defines a probability distribution of thresholds $\theta$ given host types $\lambda$. The false positive constraint for a defender strategy $\sigma$ is then written as

$$\sum_{\lambda \in \Lambda} \sum_{\theta \in \Theta} \sigma(\theta \mid \lambda) P(\lambda) \text{FP}(\theta \mid \lambda) \leq \text{FP}, \quad (31)$$

where

$$\text{FP}(\theta \mid \lambda) = \sum_{o \in O: \, o > \theta} P(o \mid \lambda), \quad (32)$$

is type $\lambda$'s amount of false positives when the threshold is $\theta$.

### 4) ATTACKER'S STRATEGY

It consists of choosing the amount of data $a \in A$ that the attacker infiltrates in the next time window. By controlling one of the users, the attacker uploads as much data as possible before being detected. The attacker is awarded a utility when the sum of the host's activity $o \in O$ and the amount of data that the attacker infiltrates $a \in A$ is less than the detection threshold $\theta \in \Theta$. A belief state

$$b \in \Delta(\Lambda \times \Theta) \tag{33}$$

is a probability distribution over possible host types and threshold settings. It is assumed that first the defender selects the threshold $\theta$ and the attacker acts in response to knowing $\theta$. Attacker's expected utility is then defined as $u_a(\sigma, \pi)$ where $\sigma$ is the defender's mixed strategy whereas $\pi$ is the attacker's policy chosen from the set $\Pi$. The attacker's policy

$$\pi : \Delta(\Lambda \times \Theta) \rightarrow A, \tag{34}$$

is defined as a mapping from the set of belief states $\Delta(\Lambda \times \Theta)$ to the set $A$ of the amounts of data. During the course of interaction with the defender, the attacker takes into account the last action and observation and uses Bayesian update rule in order to keep track of his belief $b$. Attacker's action $\pi$ depends on his belief $b$ i.e. $\pi = \pi(b)$. The defender's expected utility is defined as

$$u_d(\sigma, \pi) = -Cu_a(\sigma, \pi), \tag{35}$$

where $C > 0$. This requires that the attacker and the defender have opposite objectives and their payoffs are proportional to each other's. Also, $C$ being greater than 1 means that the defender's disutility is greater than the attacker's utility.

### 5) THE INSIDER vs. OUTSIDER ATTACKS

The data breach attacks can be performed by agents who are inside an organization/company or who are inside. The outsiders usually does not know the type of the host that is compromised even though s/he can know which types (group) exist within the company, for instance, IT admins and secretaries. The insiders, however, know their host types as they use the network regularly and they are also knowledgeable on the defences that are deployed. For instance, an insider because of him/her knowing the exact values of the thresholds that has been fixed for each host type by the defender, can exfiltrate exactly at those values.

An approximate algorithm is used to compute the attacker's policy and to find an approximate Stackelberg equilibrium. The defender's strategy is also an approximate Stackelberg equilibrium and his utility presents as a close approximation to the exact Stackelberg equilibrium.

### 6) DEFENDER'S OPTIMAL STRATEGY AGAINST ATTACKS BY THE INSIDERS

Durkota *et al.* [65] present an algorithm that computes exact Stackelberg algorithm against attacks from the insiders. Knowing the type of the user, using whom the insider

can exfiltrate data, allows representing the game between the host and the attacker as a normal form game. For this game, the attacker's strategy consists of choosing for each host type a probability distribution over the actions from the set $A$. Similarly, the defender's strategy consists of choosing for each host type a probability distribution over thresholds from the set $\Theta$. The game between the attacker and all host types can then be formalized as one problem. To achieve this, the zero-sum normal-form linear program [66] is extended to include a false-positive constraint and multiple host types:

$$\min_{\sigma(\theta|\lambda)} U_a, \tag{36}$$

$$\text{s.t.: } (\forall \lambda \in \Lambda, \ \forall a \in A) : \sum_{\theta \in \Theta} u_a(\theta, a, \lambda)\sigma(\theta \mid \lambda) \leq U_{a,\lambda}, \tag{37}$$

$$\sum_{\lambda \in \Lambda} P(\lambda)U_{a,\lambda} \leq U_a, \tag{38}$$

$$(\forall \lambda \in \Lambda) : \sum_{\lambda \in \Lambda} \sigma(\theta \mid \lambda) = 1, \tag{39}$$

$$(\forall \lambda \in \Lambda, \ \forall a \in A) : \sigma(\theta \mid \lambda) \geq 0, \tag{40}$$

$$\sum_{\lambda \in \Lambda} \sum_{\theta \in \Theta} P(\lambda)\sigma(\theta \mid \lambda)\text{FP}(\theta \mid \lambda) \leq \text{FP}. \tag{41}$$

Here $\sigma(\theta \mid \lambda)$, $U_a$ and $U_{a,\lambda}$ are the variables in the linear program. In the above, the expected utilities of each type are $U_{a,\lambda}$ that is weighed by its probability given by (38). With the requirement (36), the expected utility of the attacker $U_a$ is minimized. With the requirement (37) it is ensured that against the given defense strategy, a best response is played in each host type. The requirements given by (39) and (40) are placed in order to ensure that the defender's strategy given by $\sigma$ is considered a proper probability distribution. The requirement (41) ensures that the false-positive rate is met by $\sigma$.

### 7) DEFENDER'S OPTIMAL STRATEGY AGAINST ATTACKS BY THE OUTSIDERS

As the outsider is unaware of the host's type, s/he tries to learn about it by observing host's activity. This results in the attacker's strategies becoming more complex when these are compared to the strategies of the insider. To achieve his objectives, the outsider can come up with stronger attacks which can vary over time. The uncertainty involved suggests using Partially Observable Markov Decisions Processes (POMDPs). The algorithms developed in order to solve POMDPs can be used to compute the attacker's best response and his/her optimal strategy. In every time step, the attacker exploiting the POMDP framework takes an action from a set of allowed actions and receives the environment's response to that action. Based on this response he then updates his beliefs about the environment. Also, in each time step, the attacker's utility is a function of his action and the environment's response. POMDP generates a solution in the form of a policy describing the list of actions for all belief states about the environment. Heuristic Search Value Iteration (HSVI) [67]

is the well established algorithm that is used to solve the POMDPs as it computes the Stackelberg equilibrium of the game. Using interations the HSVI computes the strategies constituting the best response of the attacker and the defender. A best response is then achieved by a convergence of the best response strategies.

## IV. APPLICATION SCENARIOS

Game theory has many security applications, and we cannot give detailed examples of all such analyses here. In this section, we review a number of other applications that have seen game-theoretic analysis.

### A. TRUST ASSIGNMENT

Rajtmajer *et al.* [83] (2017) consider the problem of multiparty access control [68]. Users of social networks have a shared interest in the privacy settings applied to content relating to them. They model the problem as a variant of the ultimatum game where all parties are motivated to reach some agreement, despite the need to compromise. They develop a model of how participants will vary their offers over time, and show empirically that the network tends to converge around the proposals of the more 'stubborn' users who are unwilling to vary their proposals. However, they also find that stubborn users are less likely to reach agreement with their neighbours at all, unlike less stubborn users who will quickly take an approach similar to that of their neighbours, resulting in a greater rate of successful interaction.

Raya *et al.* [84] (2010) consider the ''free-rider'' problem in systems based on data aggregation: participants gain a privacy benefit by refusing to trust other parties with their data, but with less data available, the system as a whole becomes less resistant to malicious behavior. They show that it is possible to design an incentive scheme that discourages free-riding to avoid a 'tragedy of the commons'-type scenario.

### B. RESOURCE ALLOCATION

Game theory is a natural tool for the analysis of resource allocation problems in cybersecurity. An example of this is the analysis by Panaousis *et al.* [73] (2014), which builds up a quantitative model of how various security controls interact with various classes of vulnerability, yielding different types of costs to the defender, for example in the form of reputational damage or data loss. This is then used to argue that certain controls are or are not worthwhile at a given budget and at a given depth in the network.

A related analysis is given by Cui *et al.* [69] (2017). In [69], it is hypothesized that an attacker can choose between attacking a customer database and attacking individual users. Gaining access to the database yields a greater reward for the attacker, but may lead to a more vigorous law-enforcement response. Conversely, targeting individual users—e.g. by phishing—leads to a reduced payoff, but may be less risky for the attacker. The defender is represented by two parties: a system administrator who manages the database, and a user who sets a security level for themselves only. One of the more interesting features of this model is the use of a two-stage process for compromising the database, in order to model the greater technical sophistication of such an attack, at least relative to the difficulty of acquiring user credentials by e.g. phishing.

### C. ANOMALY DETECTION

Intrusion detection systems based on anomaly detection [70] require the setting of a threshold parameter, that determines whether some data is reported as 'normal' or 'anomalous'. This leads to a trade-off: a low threshold will force attackers to sacrifice the efficacy of their attacks in order to stay covert, but will also lead to a high false-positive rate, resulting in excess cost to the defender. Conversely, a high threshold will reduce the time wasted investigating false-positives, but allows attackers to be less covert and use more powerful attacks that are more costly to the defender.

This interplay between the strategies of the attacker and defender is well-modelled by game-theory, and so game-theoretic methods can effectively inform the design of these anomaly detectors.

Schlenker [63] considers the problem of allocating investigative resources to security-relevant events in a more general sense. A system that triggers investigation in too-predictable a manner is vulnerable to an attacker that can tailor its behavior so as to avoid a follow-up investigation even if it is detected. For example, a system that directs all its investigative capacity toward targets labelled as high-value is easily circumvented by an attacker who has *carte blanche* to attack moderate-value systems without concern for covertness.

### D. INFORMATION FLOW

Durkota *et al.* [65] (2017) consider the problem of detecting data exfiltration in a heterogeneous network. Once an attacker is present inside a network, they must decide how quickly to exfiltrate the data that they acquire: a small flow of data is difficult to detect, but the value of the information to the attacker is less timely and therefore argued to be less valuable. Conversely, a large flow of data is more readily apparent, but more valuable to the adversary while it goes undetected. This leads to an interesting result: the optimum strategy for the defender is to vary their detection threshold randomly, yielding a 30% reduction in exfiltrated data relative to a deterministic choice of threshold.

Alvim *et al.* [72] (2017) consider information leakage in more general terms, defining a framework of *information leakage games*, and finding that in many cases, the *attacker* also benefits from a mixed strategy. They also show that the utility of a strategy for the defender is a convex function, allowing the optimal strategy to be determined using normal optimization techniques.

### E. DECEPTION

Others have used game theory to model techniques aimed at *deception* of attackers [62]. Underbrink (2016) [61] classifies

these into *passive methods*, which serve to frustrate reconnaissance and detect the attacker before it strikes, and *active methods*, which in which the defender takes actions predicted to interfere with an attack in progress.

Schlenker [64] considers the passive case where the defender manipulates their behavior so that an attacker scanning the defender's network will be uncertain about the type or value of each system, making it difficult for the attacker to effectively allocate their effort. Schlenker shows that determining the optimal strategy for the defender is NP-hard in general, but provides an algorithm to approximate this.

Alternatively, deception may be used to engage an attacker that has already compromised the defender's network. Horák *et al.* [71] (2017) consider a system in which the defender can feed the attacker with useless data once an attack has been detected. They argue that evicting the attacker immediately upon detection is suboptimal, as this leads to the attacker starting again from an 'undetected' state, only now armed with useful information on the defender's detection capabilities. The defender might therefore be better served by allowing the attacker to remain for a time, ideally fed with a stream of valueless disinformation.

### F. JAMMING

Game-theoretic analysis of channel jamming has a long history, tracing back to Basar [79] (1983), who shows that the optimum strategy of a single attacker seeking to jam a Gaussian memoryless channel is to either transmit a linear function of the transmitted signal or to transmit random symbols, depending on the relative signal and noise powers.

Other authors have carried out similar analyses in different situations: for example Kashyap *et al.* [80] (2004) consider a Rayleigh fading channel, and show that knowledge of the channel input does not affect the jammer's strategy.

Altman *et al.* [77] (2009) analyze the case of *multiple* attackers who seek to jam an orthogonal frequency-division multiplexing (OFDM) communication channel. The attacker and defender must each decide how to distribute their power across the available subchannels in order to minimize or maximise, respectively, the signal-to-interference-plus-noise ratio (SINR) of the channel.

Han *et al.* [78] (2009) consider a different scenario in which 'friendly' jammers broadcast their own signals, introducing noise to disrupt eavesdroppers. They consider the problem from an economic viewpoint: what price can the friendly jammers demand for their services, given some desired rate of secret communication? However, like all economic analyses, this depends strongly on the model of the participants: their analysis assumes that the sender gains a constant utility per unit bandwidth, and the jammers pay a constant amount per unit power. Nevertheless, the results are interesting: in their simulations, they find that there exists a cutoff price for jamming power above which the use of friendly jammers is no longer justifiable.

### G. SMART GRIDS

Smart grids can incorporate fine-grained demand-side data into their control systems, as well as provide demand-side management: with the right incentives, users will consent to automatic reduction of their power consumption at times of high load—for example, by slightly increasing the target temperature of their air conditioners, or by delaying the activation of refrigerator motors.

By incorporating incentives into the pricing scheme, users may be incentivized to lie about their usage in order to secure a reduced tariff. Mohsenian-Rad *et al.* [82] (2010) provide a game-theoretic analysis of a decentralized demand-side management system; they show how to design the system so that users do not benefit from lying to each other about their usage.

Though a decentralized system as in [82] might provide privacy benefits to its users, issues such as communication complexity and deployment considerations may result in a centralized system being preferable in practice. Hajj and Awad (2015) [81] describe a centralized system that uses game-theoretic methods to provides optimum scheduling. This comes at the cost of forcing users to reveal their projected demand to the supplier. In practice this may be a reasonable sacrifice: in order to take advantage of off-peak tariffs, users must already reveal some information on their demand schedule, so the difference in privacy might well be small in practice.

## V. CHALLENGES TO APPLYING GAME THEORY TO SECURITY

Although game theory has been shown to be significant for security, there exist many challenges that need to be addressed for developing a viable game-theoretic approaches to security. In this regard, some key challenges include the complexity of computing a game-theoretical equilibrium strategy, as the illustrative examples in Section (III-B) show. There are also difficulties in properly quantifying security parameters such as risk, privacy, and trust [83], [84], i.e. the parameters in terms of which the utility functions for the participants (players) in a security game are defined.

Choosing an appropriate game model for a given security problem comes out as a challenge for the game theory too. Such a model need to depend on the detail and particular aspects of the security problem/application scenario. Choosing a game can be solely based on the intuition and this choice may not substantiated by the available data. A two-player game can be a model for a security game involving an attacker and a defender. However, in the dynamic version of this game can involve multiple stages for attacking and defending. In fact, as described in Section (III-B), the games of later type are more likely to be representative of the network/cybersecurity challenges of the real world.

Another aspect of the security game models is that the players are assumed to have unbounded rationality. In real life and experimental studies, the players do not always act with rationality. As a consequence, there exists a significant

scope for studying the solution-concepts of Harsanyi's disturbed games or that of Selten's perturbed games [9], [13] in the network/cybersecurity situations. In Selten's perturbed games, a player's hand 'trembles', resulting in the erroneous move and the trembles are assumed to be determined by a random process. On the other hand, in Harsanyi's disturbed games, it is the payoffs or the utility functions, rather than the players' actions, that go astray.

Interpretation of game-theoretical notions such as mixed strategy Nash equilibrium also appears as a challenge, and particularly so for the security games. Usual approach in game theory in this regard involves considering repeated games whereas many security games are represented as one-shot games. Even within the game theory community, there is no consensus on how to interpret a mixed strategy. There is clear need for interpreting the notion of a mixed-strategy for network/cybersecurity games. In order to convert the game theoretic results into practical security solutions these challenges are required to be addressed.

## REFERENCES

[1] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tutr.*, vol. 15, no. 1, pp. 472–486, 1st Quart., 2013.

[2] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Jan. 2010, pp. 1–10.

[3] T. Alpcan and T. Basar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[4] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A Markov game theory-based risk assessment model for network information system," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, Dec. 2008, pp. 1057–1061.

[5] T. Alpcan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Proc. 42nd IEEE Int. Conf. Decis. Control*, Dec. 2003, pp. 2595–2600.

[6] M. S. Abdalzaher, K. Seddik, M. Elsabrouty, O. Muta, H. Furukawa, and A. Abdel-Rahman, "Game theory meets wireless sensor networks security requirements and threats mitigation: A survey," *Sensors*, vol. 16, no. 7, p. 1003, 2016. doi: 10.3390/s16071003.

[7] R. B. Myerson, *Game Theory: Analysis of Conflict*. Cambridge, MA, USA: Harvard Univ. Press, 1991.

[8] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA, USA: MIT Press, 1991.

[9] J. C. Harsanyi and R. Selten, *A General Theory of Equilibrium Selection in Games*. Cambridge, MA, USA: MIT Press, 1988.

[10] E. Rasmusen, *Games and Information*. Cambridge, MA, USA: Blackwell, 1989.

[11] R. D. Gibbons, *Game Theory for Applied Economists*. Princeton, NJ, USA: Princeton Univ. Press, 1992.

[12] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA, USA: MIT Press, 1994.

[13] M. J. Osborne, *An Introduction to Game Theory*. New York, NY, USA: Oxford Univ. Press, 2004.

[14] V. J. Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*. Princeton, NJ, USA: Princeton Univ. Press, 1944.

[15] R. J. Aumann and S. Hart, Eds., *Handbook of Game Theory With Economic Applications*. Amsterdam The Netherlands: North-Holland, 1995.

[16] J. M. Smith, *Evolution and the Theory of Games*. Cambridge, U.K.: Cambridge Univ. Press, 1982.

[17] J. W. Weibull, *Evolutionary Game Theory*. Cambridge, MA, USA: MIT Press, 1997.

[18] J. Rychtar and M. Broom, *Game-Theoretical Models in Biology*. Boca Raton, FL, USA: CRC Press, 2013.

[19] J. D. Morrow, *Game Theory for Political Scientists*. Princeton, NJ, USA: Princeton Univ. Press, 1994.

[20] S. J. Brams, *Game Theory and Politics*. New York, NY, USA: Dover, 2011.

[21] K. R. Apt and E. Grdel, *Lectures in Game Theory for Computer Scientists*. New York, NY, USA: Cambridge Univ. Press, 2011.

[22] N. Nisan, T. Roughgarden, E. Tardos, and V. Vazirani, Eds., *Algorithmic Game Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[23] D. Bauso, *Game Theory With Engineering Applications* (Advances in Design and Control). Philadelphia, PA, USA: SIAM, 2016.

[24] A. B. MacKenzie and L. A. DaSilva, *Game Theory for Wireless Engineers* (Synthesis Lectures on Commnunications). San Mateo, CA, USA: Morgan & Claypool, 2006.

[25] P. Papayoanou, *Game Theory for Business: A Primer in Strategic Gaming*. San Mateo, CA, USA: Probabilistic Publishing, 2010.

[26] K. Chatterjee and W. Samuelson, Eds., *Game Theory and Business Applications*. New York, NY, USA: Springer, 2014. doi: 10.1007/b109681.

[27] D. G. Baird, R. H. Gertner, and R. C. Picker, *Game Theory and the Law*. Cambridge, MA, USA: Harvard Univ. Press, 1998.

[28] A. Iqbal, V. Masson, and D. Abbott, "Kidnapping model: An extension of Selten's game," *Roy. Soc. Open Sci.*, vol. 4, no. 12, 2017, Art. no. 171484.

[29] R. A. McCain, *Game Theory and Public Policy*. Cheltenham, U.K.: Edward Elgar Publishers, 2009.

[30] S. Rass and S. Schauer, Eds., *Game Theory for Security and Risk Management: From Theory to Practice*. Basel, Switzerland: Birkhäuser, 2018.

[31] *The Conference Website*. Accessed: Jun. 20, 2019. [Online]. Available: http://www.gamesec-conf.org/

[32] M. Guo, Y. Yang, and M. A. Babar, "Cost sharing security information with minimal release delay," in *Proc. Int. Conf. Princ. Pract. Multi-Agent Syst.*, Tokyo, Japan, 2018, pp. 177–193.

[33] M. Guo, H. Hata, and A. Babar, "Optimizing affine maximizer auctions via linear programming: An application to revenue maximizing mechanism design for zero-day exploits markets," in *Proc. Int. Conf. Princ. Pract. Multi-Agent Syst.*, Nice, France, 2017, pp. 280–292.

[34] M. Guo, H. Hata, and A. Babar, "Revenue maximizing markets for zero-day exploits," in *Proc. Int. Conf. Princ. Pract. Multi-Agent Syst.*, Phuket, Thailand, 2016, pp. 247–260.

[35] *Quantum Game Theory on Google Scholar*. Accessed: Oct. 21, 2018. [Online]. Available: https://scholar.google.com.au/citations?user=wkfPca QAAAAJ&hl=en

[36] A. Iqbal, J. M. Chappell, and D. Abbott, "The equivalence of Bell's inequality and the Nash inequality in a quantum game-theoretic setting," *Phys. Lett. A*, vol. 382, no. 40, pp. 2908–2913, 2018.

[37] A. Iqbal and D. Abbott, "A game theoretical perspective on the quantum probabilities associated with a GHZ state," *Quantum Inf. Process.*, vol. 17, p. 313, Nov. 2018.

[38] F. S. Khan, N. Solmeyer, T. S. Humble, and R. Balu, "Quantum games: A review of the history, current state, and interpretation," *Quantum Inf. Process.*, vol. 17, p. 309, Nov. 2018.

[39] A. Haurie and G. Zaccour, Eds., *Dynamic Games: Theory and Applications*. Boston, MA, USA: Springer 2005.

[40] T. Basar and G. Zaccour, Eds., *Handbook of Dynamic Game Theory*. Cham, Switzerland: Springer, 2018.

[41] P. Maillé, P. Reichl, and B. Tuffin. (2010). *Of Threats and Costs: A Game-Theoretic Approach to Security Risk Management*. Accessed: Oct. 20, 2018. [Online]. Available: https://archivesic.ccsd.cnrs.fr/ TELECOM-BRETAGNE/hal-00724808

[42] N. Kostyuk, "The digital prisoner's dilemma: Challenges and opportunities for cooperation," in *Proc. World Cyberspace Cooperation Summit IV*, Palo Alto, CA, USA, Nov. 2013, pp. 4–6.

[43] J. Nash, "Equilibrium points in n-person games," *Proc. Nat. Acad. Sci. USA*, vol. 36, no. 1, pp. 48–49, 1950.

[44] J. Nash, "Non-cooperative games," *Ann. Math.*, vol. 54, no. 2, pp. 286–295, 1951.

[45] H. von Stackelberg, *Marktform und Gleichgewicht*. Vienna, Austria: Springer, 1934.

[46] V. Damjanovic-Behrendt, "Stackelberg security game for optimizing security of federated Internet of things platform instances," *World Acad. Sci., Eng. Technol., Int. J. Comput., Elect., Automat., Control Inf. Eng.*, Vol. 11, no. 5, pp. 517–522, 2017.

[47] D. Kar, T. H. Nguyen, F. Fang, M. Brown, A. Sinha, M. Tambe, and A. X. Jiang, "Trends and applications in Stackelberg security games," in *Handbook of Dynamic Game Theory*, T. Basar and G. Zaccour, eds. Cham, Switzerland: Springer, 2016, pp. 1–47.

[48] E. Burger and J. E. Freund, *Introduction to the Theory of Games*. Upper Saddle River, NJ, USA: Prentice-Hall, 1963.

[49] S. Alpern, A. Morton, and K. Papadaki, "Patrolling games," *Oper. Res.*, vol. 59, no. 5, pp. 1246–1257, 2011.

[50] A. Sokri, "Optimal resource allocation in cyber-security: A game theoretic approach," *Procedia Comput. Sci.*, vol. 134, pp. 283–288, 2018.

[51] S. Coniglio, "Algorithm for finding leader-follower equilibrium with multiple followers," M.S. thesis, AI&R Lab., Laboratorio di Intelligenza Artificiale e Robotica del Politecnico di Milano, Dipartimento di Elettronica e Informazione, Politecnico di Milano, Milano, MI, Italy, 2014. [Online]. Available: https://www.politesi.polimi.it/bitstream/10589/92066/1/Algorithms%20for%20Finding%20Leader-Follower%20Equilibrium%20with%20Multiple%20Followers.pdf

[52] M. Jain, J. Tsai, J. Pita, C. Kiekintveld, S. Rathi, F. Ordóñez, and M. Tambe, "Software assistants for randomized patrol planning for the lax airport police and the federal air marshal service," *Interfaces*, vol. 40, no. 4, pp. 267–290, 2010.

[53] B. An, M. Tambe, F. Ordonez, E. Shieh, and C. Kiekintveld, "Refinement of strong Stackelberg equilibria in security games," in *Proc. 25th AAAI Conf. Artif. Intell.*, Aug. 2011, pp. 587–593.

[54] L. Metcalf and W. Casey, *Cybersecurity and Applied Mathematics*, 1st ed. Amsterdam, The Netherlands: Elsevier, 2016.

[55] V. H. Pham, "Applications of game theory in information security," M.S. thesis, Dept. Inf. Secur., Inf. Secur. Group, Dept. Math., Univ. London, London, U.K., 2015. [Online]. Available: https://core.ac.uk/download/pdf/77297452.pdf

[56] A. Golchubian, "Utilizing a game theoretical approach to prevent collusion and incentivize cooperation in cybersecurity contexts," M.S. thesis, Dept. College Eng. Comput. Sci., Florida Atlantic Univ., Boca Raton, FL, USA, 2017. Accessed: Oct. 20, 2018. [Online]. Available: https://pdfs.semanticscholar.org/c291/2ac3c918f3dbd997e2a3454b6b8b6b17c37f.pdf

[57] I. Vakilinia and S. Sengupta, "A coalitional game theory approach for cybersecurity information sharing," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2017, pp. 23–25.

[58] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. Workshop Game Theory Commun. Netw.*, 2006, p. 4.

[59] Johnson B., Grossklags J., Christin N., Chuang J. "Are security experts useful? Bayesian Nash equilibria for network security games with limited information," in *Computer Security* (Lecture Notes in Computer Science), vol. 6345, D. Gritzalis, B. Preneel, M. Theoharidou, Eds. Berlin, Germany: Springer, 2010, pp. 588–606.

[60] A. Witteloostuijn, "A game-theoretic framework of trust," *Int. Stud. Manage. Org.*, vol. 33, no. 3, pp. 53–71, 2003.

[61] A. J. Underbrink, "Effective cyber deception," in *Cyber Deception*. Cham, Switzerland: Springer, 2016, pp. 115–147.

[62] F. Cohen, "A note on the role of deception in information protection," *Comput. Secur.*, vol. 17, no. 6, pp. 483–506, 1998.

[63] A. Schlenker, H. Xu, M. Guirguis, C. Kiekintveld, A. Sinha, M. Tambe, S. Y. Sonya, D. Balderas, and N. Dunstatter, "Don't bury your head in warnings: A game-theoretic approach for intelligent allocation of cybersecurity alerts," in *Proc. 26th Int. Joint Conf. Artif. Intell.*, Melbourne, VIC, Australia, 2017, pp. 381–387.

[64] A. Schlenker, "Game theoretic deception and threat screening for cyber security," M.S. thesis, Dept. Graduate School, Univ. Southern California, Los Angeles, CA, USA, 2018. [Online]. Available: http://teamcore.usc.edu/papers/2018/Aaron_Thesis.pdf

[65] K. Durkota, V. Lisý, C. Kiekintveld, K. Horák, B. Bošanský, and T. Pevný, "Optimal strategies for detecting data exfiltration by internal and external attackers," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 10575, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham, Switzerland: Springer, 2017.

[66] T. Shoham and K. Leyton-Brown, *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[67] T. Smith and R. Simmons, "Heuristic search value iteration for POMDPs," in *Proc. 20th Conf. Uncertainty Artif. Intell.*, 2004, pp. 520–527.

[68] H. Hu, G. J. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 7, pp. 1614–1627, Jul. 2013.

[69] J. Cui, H. Rosoff, and R. S. John, "Deterrence of cyber attackers in a three-player behavioral game," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 10575, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham, Switzerland: Springer, 2017.

[70] Y. Wang, J. Wong, and A. Miner, "Anomaly intrusion detection using one class SVM," in *Proc. 5th Annu. IEEE SMC Inf. Assurance Workshop*, West Point, NY, USA, Jun. 2004, pp. 358–364.

[71] K. Horák, Q. Zhu, B. Bošanský, "Manipulating adversary's belief: A dynamic game approach to deception by design for proactive network security," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 10575, S. Rass, B. An, and C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham, Switzerland: Springer, 2017.

[72] M. S. Alvim, K. Chatzikokolakis, Y. Kawamoto, and C. Palamidessi, "Information leakage games," in *Decision and Game Theory for Security*. Cham, Switzerland: Springer, 2017, pp. 437–457.

[73] E. Panaousis, A. Fielder, P. Malacaria, C. Hankin, and F. Smeraldi, "Cyber-security games and investments: A decision support approach," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 8840, R. Poovendran and W. Saad, Eds. Cham, Switzerland: Springer, 2014.

[74] M. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, p. 25, 2013.

[75] L. Dritsoula, P. Loiseau, and J. Musacchio, "Computing the nash equilibria of intruder classification games," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 7638, J. Grosaklags and J. Walrand, Eds. Berlin, Germany: Springer, 2012.

[76] Y. Ai, M. R. Bhatnagar, M. Cheffena, A. Mathur, and A. Sedakov, "Game-theoretical analysis of PLC system performance in the presence of jamming attacks," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 10575, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham, Switzerland: Springer, 2017.

[77] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming in wireless networks: The case of several jammers," in *Proc. Int. Conf. Game Theory Netw.*, May 2009, pp. 585–592.

[78] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Proc. Int. Conf. Game Theory Netw.*, May 2009, pp. 287–294.

[79] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inf. Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[80] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[81] N. Hajj and M. Awad, "A game theory approach to demand side management in smart grids," in *Intelligent Systems* (Advances in Intelligent Systems and Computing), D. Filev, eds, vol. 323. Cham, Switzerland: Springer, 2015.

[82] A.-H. Mohsenian-Rad, V. S. W. Vincent, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 320–331, Dec. 2010.

[83] S. Rajtmajer, A. Squicciarini, J. M. Such, J. Semonsen, and A. Belmonte, "An ultimatum game model for the evolution of privacy in jointly managed content," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 10575, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham, Switzerland: Springer, 2017.

[84] M. Raya, R. Shokri, and J.-P. Hubaux, "On the tradeoff between trust and privacy in wireless ad hoc networks," in *Proc. 3rd ACM Conf. Wireless Netw. Secur.*, 2010, pp. 75–80.

**AZHAR IQBAL** received the B.Sc. (Hons.) degree in physics from the University of Sheffield, Sheffield, U.K., in 1995, and the Ph.D. degree in applied mathematics from the University of Hull, Hull, U.K., in 2006. He received the Postdoctoral Research Fellowship for Foreign Researchers from the Japan Society for Promotion of Science (JSPS) at the Kochi University of Technology, Japan, in 2006. In 2007, he received the prestigious Australian Postdoctoral Fellowship from the Australian Research Council (ARC) at the School of Electrical and Electronic Engineering, The University of Adelaide, Adelaide, SA, Australia. He is currently an Adjunct Senior Lecturer with the School of Electrical and Electronic Engineering, The University of Adelaide.

**LACHLAN J. GUNN** received the B.Eng. (Hons.) and B.Math. and Comp.Sc. (pure) degrees from The University of Adelaide, Australia, in 2012, and the Ph.D. degree in engineering from The University of Adelaide, in 2018. He is currently a Postdoctoral Researcher with the Secure Systems Group, Aalto University, Finland. Prior to this, he was a Research Associate with the Computational Learning Systems laboratory, The University of South Australia. He received the J. Mazumdar Prize in Engineering and Mathematics, in 2012, four DSTO Scholarships in Radar Technology, from 2009 to 2012, and the Australian Post-Graduate Award, in 2013. In 2014, he also received an Endeavour Research Fellowship by the Australian Government in order to undertake research into stochastic phenomena at the University of Angers, France. His research interests include consensus protocols and the use of trusted execution environments in protocol design.

**MINGYU GUO** received the B.S. degree in mathematics from Zhejiang University, in 2004, the M.S. degree in applied mathematics from the University of Florida, in 2006, and the Ph.D. degree in computer science from Duke University, in 2010. He held a position as a Lecturer with the University of Liverpool, until 2013, and has been a Lecturer with The University of Adelaide since then. His interests are in algorithmic game theory and multiagent systems. His work appeared in top computer science journals (e.g., the *Artificial Intelligence* and the *Journal of Artificial Intelligence Research*), top computer science conferences (e.g., AAAI, IJCAI, AAMAS, and EC), and top economics journal (*Games and Economic Behavior*). His Ph.D. dissertation, entitled *Computationally Feasible Approaches to Automated Mechanism Design*, was selected as one of the two runner-ups for the prestigious IFAAMAS-10 Victor Lessor Distinguished Dissertation Award (an annual award for the Best Ph.D. Dissertation in the field of multiagent systems). He has served as a Senior Program Committee Member for IJCAI 2015, AAMAS 2018, and AAMAS 2019 (CORE A*). He has continuously served on the program committee of many other CORE A* level computer science conferences, including AAAI, IJCAI, EC, AAMAS, and WWW.

**M. ALI BABAR** received the M.S. degree in psychology from the Government College University, Lahore, in 1994, the M.Sc. degree in computer sciences from the University of Technology Sydney, in 1999, and the Ph.D. degree in computer science and engineering from the University of New South Wales, in 2006. He is currently a Professor and the Chair of Software Engineering, School of Computer Science, The University of Adelaide, Australia. Prior to this, he was an Associate Professor (Reader) in software engineering with Lancaster University, U.K. Previously, he has worked as a Researcher and project leaders in different research centers in Ireland and Australia. His research projects have attracted funding from various agencies in Denmark, U.K., Ireland, and Australia. He has authored or coauthored more than 150 peer-reviewed research papers in premier software engineering journals and conferences such as the *ACM Transactions on Software Engineering and Methods* (TOSEM), the IEEE Software, and *ICSE*. He has recently co-edited a book on *Agile Architecting* published by Morgan Kaufmann, Elsevier. He is a member of the steering committees of several international software engineering and architecture conferences such as WICSA, ECSA, and ICGSE. He regularly runs tutorials and gives talks on topics related to cloud computing, software architecture and empirical approaches at various international conferences. More information on Prof. M. Ali Babar can be found at http://malibabar.wordpress.com.

**DEREK ABBOTT** (M'85–SM'99–F'05) was born in South Kensington, London, U.K., in 1960. He received the B.Sc. (Hons.) degree in physics from Loughborough University, Leicestershire, U.K., in 1982, and the Ph.D. degree in electrical and electronic engineering from The University of Adelaide, Adelaide, SA, Australia, in 1995, under the supervision of K. Eshraghian and B. R. Davis. From 1978 to 1986, he was a Research Engineer with the GEC Hirst Research Centre, London, U.K. From 1986 to 1987, he was a VLSI Design Engineer with Austek Microsystems, Australia. Since 1987, he has been with The University of Adelaide, where he is currently a Full Professor with the School of Electrical and Electronic Engineering. He has co-edited the book *Quantum Aspects of Life* (London, U.K.: Imperial College Press, 2008), has coauthored *Stochastic Resonance* (Cambridge, U.K.: Cambridge University Press, 2012), and has coauthored the *Terahertz Imaging for Biomedical Applications* (New York, NY, USA: Springer-Verlag, 2012). He holds over 1000 publications/patents and has been an invited speaker at over 100 institutions. His interests are in the areas of multidisciplinary physics and electronic engineering applied to complex systems. His research programs span a number of areas of stochastics, game theory, photonics, renewable energy, biomedical engineering, and computational neuroscience. He is a Fellow of the Institute of Physics. He has won a number of awards, including the South Australian Tall Poppy Award for Science (2004), the Premier's SA Great Award in Science and Technology for outstanding contributions to South Australia (2004), an Australian Research Council Future Fellowship (2012), the David Dewhurst Medal (2015), the Barry Inglis Medal (2018), and the M. .A. Sargent Medal (2019). He has served as an Editor and/or a Guest Editor for a number of journals, including the IEEE JOURNAL OF SOLID-STATE CIRCUITS, the *Journal of Optics B*, the *Microelectronics Journal*, *Chaos*, the *Smart Structures and Materials*, the *Fluctuation and Noise Letters*, the Proceedings of the IEEE, and the IEEE PHOTONICS JOURNAL. He is currently on the editorial boards of the IEEE ACCESS, the *Frontiers in Physics*, the *Royal Society Open Science*, and the *Nature's Scientific Reports*.

• • •