Game Theory Meets Network Security and Privacy

Mohammad Hossein Manshaei[†]
Isfahan University of Technology (IUT), Iran
Quanyan Zhu
University of Illinois at Urbana-Champaign (UIUC), USA
Tansu Alpcan[‡]
University of Melbourne, Australia
Tamer Başar
University of Illinois at Urbana-Champaign (UIUC), USA
and
Jean-Pierre Hubaux
Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland

This survey provides a structured and comprehensive overview of research on security and privacy in computer and communication networks that uses game-theoretic approaches. We present a selected set of works to highlight the application of game theory in addressing different forms of security and privacy problems in computer networks and mobile applications. We organize the presented works in six main categories: *security of the physical and MAC layers*, *security of self-organizing networks*, *intrusion detection systems*, *anonymity and privacy*, *economics of network security*, and *cryptography*. In each category, we identify security problems, players, and game models. We summarize the main results of selected works, such as equilibrium analysis and security mechanism designs. In addition, we provide a discussion on advantages, drawbacks, and the future direction of using game theory in this field. In this survey, our goal is to instill in the reader an enhanced understanding of different research approaches in applying game-theoretic methods to network security. This survey can also help researchers from various fields develop game-theoretic solutions to current and emerging security problems in computer networking.

Categories and Subject Descriptors: C.2.0 [**Computer-Communication Networks**]: General—*Security and protection (e.g., firewalls)*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms: Algorithms, Design, Economics, Security, Theory

Additional Key Words and Phrases: Game Theory, Network Security and Privacy, Intrusion Detection System, Location Privacy, Revocation, Wireless Security, Cryptography, Multiparty Computation

---

[†] Mohammad Hossein Manshaei was with EPFL during part of this research.
[‡] Tansu Alpcan was with TU-Berlin and T-Labs during part of this research.
Correspondence to: Mohammad Hossein Manshaei[1] and Quanyan Zhu[2]
1. Department of Electrical and Computer Engineering, Isfahan University of Technology (IUT), Isfahan 84156-83111, Iran. *Email: manshaei@gmail.com*
2. Coordinated Science Laboratory, UIUC, 1308 W. Main St., Urbana, IL 61801, USA. *Email: zhu31@illinois.edu*

1. INTRODUCTION

The continuous evolution of computer networks and mobile applications has drastically changed the nature of their security and privacy. As networks play an increasingly important role in modern society, we witness the emergence of new types of security and privacy problems that involve direct participation of network agents. These agents are individuals, as well as devices or software, acting on their self behalf. As independent decision makers, they can be cooperative, selfish, or malicious (or anything in between). Consequently, there is a fundamental relationship between the decision making of agents and network security problems.

Security decisions in this context have recently been investigated analytically in a methodical way, instead of only relying on heuristics, which provides numerous advantages. This paradigm shift has led some researchers to employ *game theory* – a rich set of mathematical tools for multi-person strategic decision making – to model the interactions of agents in security problems. Furthermore, the theory of mechanism design [Nisan and Ronen 1999; Nisan 2007] has enabled researchers to design security and privacy mechanisms based on the analytical results obtained (e.g., equilibrium analysis of the game). Security decisions arrived at using such game-theoretic approaches help to allocate limited resources, balance perceived risks, and take into account the underlying incentive mechanisms.

The increasing numbers of books, journal articles, and conference publications that study network security problems using tools of game theory is clear evidence of the emerging interest in this topic. The main objective of this survey is to help develop a deeper understanding of existing and future network security problems from a game-theoretic perspective.

Security at the physical and MAC layers (e.g., jamming and eavesdropping attacks), *security of self-organizing networks* (e.g., revocation in mobile ad hoc networks), *intrusion detection systems* (e.g., collaborative IDS), *anonymity and privacy* (e.g., cooperative location privacy), *economics of network security* (e.g., interdependent security), and *cryptography* (e.g., security in multi-party computation) are among the well-known topics of network security and privacy that are analyzed and solved employing game-theoretic approaches. In practice, all these problems involve decision-making at multiple levels. This survey provides a structured and comprehensive overview of these research efforts. It also highlights future directions in this field where game-theoretic approaches can be developed for emerging network security problems.

The economics of information security is an emerging area of study. Researchers have already investigated dependability and software economics, behavioral economics, and the psychology of security for analyzing and solving certain security and privacy problems [Anderson and Moore 2006; Camp 2006; Bohme and Schwartz 2010]. One of the main tools that have been used to analyze the economics of security is *game theory* or microeconomics. Here we briefly address the main contributions of these works and we position our survey in relation to them.

In [Anderson and Moore 2006], the authors review recent results and challenges in the economics of information security. They provide a list of promising applications of economic theories and ideas to practical information security problems. They show that incentives are becoming as important as technical design in achieving de-

pendability. They also analyze the economics of vulnerabilities and privacy. Finally, they identify two main research topics in this field: (i) the economics of security, and (ii) the economics of dependability or strategy-proof design for network protocols and interfaces. In [Camp 2006], the author reviews the recent cross-disciplinary study of economics and information security for the understanding and management of security of computing environments in organizations. The topics range from system security management to security investment, from personal information privacy to security evaluation. Recently in [Bohme and Schwartz 2010], the authors propose a comprehensive formal framework to classify all market models of cyber-insurance that have been defined so far.

Our survey is different from the aforementioned works in two ways. First, our survey focuses on a class of specific applications related to the security and privacy of computer and communication networks rather than on general information security. Second, our survey does not aim to review the microeconomics literature of information security and privacy. We review, however, in Section 7, papers that apply game-theoretic approaches to technical problems in computer networks from the economics perspective.

We assume in this survey that readers have a basic knowledge of both *game theory* and *network security*. Still, we briefly review in the next section some important concepts of game theory. Interested readers are referred to [Başar and Olsder 1999; Alpcan and Başar 2011; Buttyan and Hubaux 2008] for introductory and tutorial material for game theory, network security, and cryptography. In the next section, we also discuss various security problems that are addressed using game-theoretic approaches, and we provide an overview of the survey and its structure.

2. NETWORK SECURITY AND GAME THEORY

Everyday use of networked computing and communication systems is ubiquitous in modern society. Hence, security of computers and networks has become an increasingly important concern. Network security problems are often challenging because the growing complexity and interconnected nature of IT systems lead to limited capability of observation and control. They are also multi-dimensional in that they entail issues at different layers of the system; for example, higher level privacy and cryptography problems, physical layer security problems, and issues on information security management.

Theoretical models at the system level play an increasingly important role in network security and provide a scientific basis for high-level security-related decision-making. In these models, the agents or decision makers (DMs) in network security problems play the role of either the attacker or the defender. They often have conflicting goals. An attacker attempts to breach security of the system to disrupt or cause damage to network services, whereas a defender takes appropriate measures to enhance the system security design or response.

Game theory provides mathematical tools and models for investigating multi-person strategic decision making where the players or DMs compete for limited and shared resources.

In other words, game theory allows for modeling situations of conflict and for predicting the behavior of participants. Let us first briefly review some important

concepts of game theory.

A game G is generally defined as a triplet $(\mathcal{P}, \mathcal{S}, \mathcal{U})$, where $\mathcal{P}$ is the set of players, $\mathcal{S}$ is the set of strategies, and $\mathcal{U}$ is the set of payoff functions. The payoff $u_i(s)$ expresses the benefit b of player i, given the strategy profile s minus the cost c it has to incur: $u = b - c$.

In a complete information game with n players [1], a strategy profile $s = \{s_i\}_{i=1}^{n}$ is the n-tuple of strategies of the players. Let us denote by $br_i(s_{-i})$ the best response function of player i to the remaining players' strategies, collectively represented as s_{-i}. This is the function that maximizes $u_i(s_i, s_{-i})$ over the set of all allowable strategies of player i (denoted by S_i), that is:

$$br_i(s_{-i}) = \arg\max_{s_i} u_i(s_i, s_{-i}) \tag{1}$$

If an n-tuple of strategies satisfies the relationship $s_i = br_i(s_{-i})$ for every i, then no player has the incentive (in terms of increasing his payoff) to deviate from the given strategy profile. This leads us to the concept of Nash Equilibrium [Nash 1951]. A strategy profile s^* is in *Nash equilibrium* (NE) if, for each player i:

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \forall s_i \in S_i. \tag{2}$$

What we have introduced above can be called *pure strategies*. In an actual game, a player is also allowed to play a pure strategy with some probability; such strategies are known as *mixed strategies*. More precisely, a *mixed strategy* x_i of player i is a probability distribution over his set S_i of pure strategies. A mixed strategy profile $x^* := \{x_i^*\}_{i=1}^{n}$ is a mixed-strategy Nash equilibrium solution if for every $x_i \in \mathcal{X}_i$,

$$\bar{u}_i(x_i^*, x_{-i}^*) \geq \bar{u}_i(x_i, x_{-i}^*), \tag{3}$$

where $\bar{u}_i$ is the expected payoff function, $\mathcal{X}_i$ is a set of distributions over the pure strategies S_i, and x_{-i} represents a set of mixed strategies of players other than player i.

For further information on NE in complete information games, as well as on equilibrium solution concepts in incomplete information games (such as Bayesian equilibrium) we refer the reader to [Gibbons 1992], [Fudenberg and Tirole 1991], and [Başar and Olsder 1999].

As a special class of games, *security games* study the interaction between malicious attackers and defenders. Security games and their solutions are used as a basis for formal decision making and algorithm development as well as for predicting attacker behavior. Depending on the type of information available to DMs, the action spaces and the goals of the DMs, security games can vary from simple deterministic ones to more complex stochastic and limited information formulations and are applicable to security problems in a variety of areas ranging from intrusion detection to privacy and cryptography in wireless, vehicular and computer networks.

In this survey, we review various game-theoretical formulations of network security issues. In Table I, we outline the security problems to be discussed in the subsequent sections. We summarize their adopted game-theoretical approaches and main results obtained from the respective models. Most of the security games are

[1] A game with complete information is a game in which, roughly speaking, each player has full knowledge of all aspects of the game.

defined between one attacker and one defender, where **zero-sum games** are analyzed and possible equilibria are investigated. However, there is a class of security games where several players cooperate or compete against each other to maximize their utilities. These games are mainly defined to design an optimal security or privacy mechanism for a given distributed system.

Table I. Security and Privacy Games in Computer Networks.

Section	Security or Privacy Problem	Game Approach	Main Results
3.1	Jamming in Communication Channel [Başar 1983; Kashyap et al. 2004]	Zero-sum game	Optimal defense strategy
3.1	Jamming in Wireless Networks [Altman et al. 2009], [Sagduyu et al. 2009]	Zero-sum game Bayesian game	Optimal defense strategy
3.2	Eavesdropping in Wireless Networks [Saad et al. 2009]	Coalition game	Merge-and-split coalition algorithm
3.2	Jamming/Eavesdropping in Wireless Networks [Han et al. 2009]	Stackelberg game	Anti-eavesdropping algorithm
4.1	Vehicular Network Security [Buchegger and Alpcan 2008]	Zero-sum and Fuzzy game	Optimize defense strategy
4.2	Revocation in Mobile Networks [Raya et al. 2008]	Extensive game	Mobile revocation protocol
4.2	Revocation in Mobile Networks [Reidt et al. 2009]	Price auction	Robust revocation protocol
5.1	Configuration and Response of IDS [Zhu and Başar 2009], [Zonouz et al. 2009]	Stochastic game	On-line defense strategy
5.1	IDS Configuration [Liu et al. 2006]	Dynamic bayesian game	Hybrid monitoring system
5.2	Networked IDSs [Zhu et al. 2010b]	Stochastic game	Performance limits
5.3	Collaborative IDS [Zhu et al. 2009]	Non-zero-sum game	Incentive-based collaboration algorithm
6.1	Location Privacy [Freudiger et al. 2009]	Incomp. information static game	Pseudonym change protocol
6.2	Economics of Privacy [Acquisti et al. 2003]	Repeated game	Identify anonymity parameters
6.3	Trust vs. Privacy [Raya et al. 2010]	Dynamic incomplete information game	Incentive to build trust
6.4	Tor Path Selection [Zhang et al. 2010a]	Dynamic game	gPath for Tor
7.1	Interdependent Security [Kunreuther and Heal 2003]	Static security cost game	Equilibrium analysis of risks
7.1	Information Security [Grossklags and Johnson 2009] [Grossklags et al. 2008]	Static game	Equilibrium analysis insurance versus protection
7.2	Vendor Patch Management [Cavusoglu et al. 2008]	Static non-zerosum game	Vulnerability disclosure policies
7.2	User Patch management [August and Tunca 2006]	Population games	Incentive-based management policies for network security
8.1	Cryptographic Mediator [Katz 2008; Dodis and Rabin 2007] [Abraham et al. 2006]	Cheap talk game	Implement correlated equilibrium
8.2	Rationality in MPC [Halpern and Teague 2004] [Gordon and Katz 2006] [Lysyanskaya and Triandopoulos 2006] [Kol and Naor 2008]	Repeated game	Define random-length protocol secret sharing Secure-MPC

In Section 3, we focus on security problems at the physical and MAC layers. These security problems can be divided into two main groups: jamming and eavesdropping in communication networks. They are commonly modeled as zero-sum

games between malicious attackers and transmitter-receiver pairs. Depending on the role of the DMs, the game can be hierarchical (e.g., a Stackelberg game) if any of the DMs have certain information advantage over the others. Alternatively, it can be a cooperative or a coalitional game, if DMs can collaborate to achieve their goals. Given the appropriate choice of game framework, optimal defense strategies are derived taking into account adversarial conditions.

In Section 4, we address security games in self-organizing networks. We first present security games for vehicular networks that are modeled by a 2-player zero-sum game, fuzzy game, and fictitious play. These games can optimize the defending strategy of mobile nodes against homogeneous attackers represented by a single player. We also discuss revocation games in ephemeral networks where different revocation strategies of mobile nodes have been analyzed using a finite dynamic game. The results can then be used to design a revocation protocol.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions. As shown in Section 5, stochastic zero-sum games are commonly used to model conflicting goals of a detector and an attacker and uncertainties in the decision making. The game-theoretical model provides a theoretical basis for detection algorithm design and performance evaluation.

In Section 6, we discuss how to model the interactions between the agents when they want to improve their privacy. We show how incomplete information games can be used to model this strategic behavior for location privacy in mobile networks. We also address how a repeated-game with simultaneous moves can model the economics of anonymity. Finally, we show how to study the tradeoff between trust and privacy using the setting of a dynamic incomplete information game.

Security problems at the management level are often tackled from an economic perspective. The increasing interaction and collaboration between various organizations and companies leads to security interdependencies among them. The vulnerability of one organization may result in cascading failures and compromises for others. Such interdependence is commonly described using a linear influence network coupled with payoff functions related to costs and benefits of outcomes, as shown in Section 7. The equilibrium analysis of the games provides insights on the decisions on issues such as security investment and patch management.

Finally in Section 8, we address how game theory can help cryptography and *vice versa*. In particular, we show how cheap talk games can help develop cryptographic mediators and how repeated games can help analyze and design incentives for the agents in multi-party computational protocols. Section 9 concludes the paper and points out some future challenges.

3. SECURITY OF PHYSICAL AND MAC LAYERS

An important concern of security in communication networks is at the physical layer, where communication channels may suffer from jamming and eavesdropping attacks. Although these attacks pose a threat for both wired and wireless networks, they are of a greater concern for the latter. Figure 1 depicts such malicious behaviors in wireless networks.

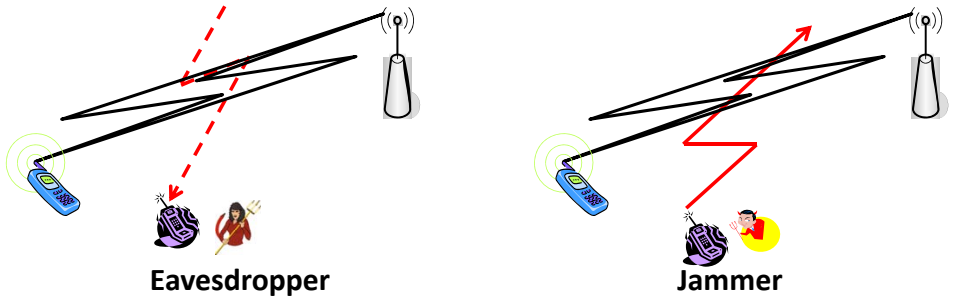

Fig. 1. Jamming and eavesdropping are two common adversarial behaviors in wireless networks. Several mobile devices communicate with the base stations (BS) and each other. A jammer actively transmits signals to interfere and interrupt the communication of mobiles with the BS and between mobile nodes, whereas an eavesdropper passively listens to the conversation between mobile nodes.

Eavesdropping is a passive attack that consists of listening to the network and analyzing the captured data without interacting with the network. For example, by placing an antenna at an appropriate location, an attacker can overhear the information that the victim transmits or receives on a wireless network. Protection against such misdeeds can be achieved by encrypting the information.

Jamming is an active attack that can disrupt data transmission. By transmitting at the same time the victim transmits or receives data, an attacker can make it impossible for the victim to communicate. Typical protection solutions include spread spectrum and frequency hopping techniques or a combination of the two [Ephremides and Wieselthier 1987; Buttyan and Hubaux 2008]. Jamming attacks also occur at the media access control (MAC) layer. An adversary either corrupts control packets or reserves the channel for the maximum allowable number of slots, so that other nodes experience low throughput by not being able to access the channel. In [Mallik et al. 2000], the authors study the problem of a legitimate node and a jammer transmitting to a common receiver in an on-off mode in a game-theoretic framework.

Malicious behavior in communication networks can be modeled by associating attackers with a different type of a utility function. The utility function represents gain at the expense of performance degradation of other users. Note that this is different from models capturing selfish behavior where all users aim to improve their own performance. At the physical layer, the interaction between a legitimate entity that abides by the communication protocol and an adversary who deviates from legitimate protocol operation is often modeled as a zero-sum game so as to capture their conflicting goals. The utility is often expressed in terms of consumed energy or achievable throughput on a link or end-to-end basis.

From the perspective of mathematical modeling, in a jamming game, the saddle-point equilibrium and the Nash equilibrium[2] solution concepts provide reasonable

[2]Noncooperative Nash equilibrium is one where no single player can benefit (in terms of improving his utility) through a unilateral deviation. Saddle-point equilibrium is a Nash equilibrium for two

noncooperative equilibrium solutions when the players enter the game symmetrically as far as the decision making goes, namely, when no single player dominates the decision process. However, in situations (say with two players) where one of the players has the ability to enforce his strategy on the other, the equilibrium solution concept is the **Stackelberg equilibrium** and the corresponding game is called a **Stackelberg game**. In such a game, the player who announces his strategy first is called the *leader* and the other player who reacts to the leader's decision is called the *follower*.

The interaction between a jammer and a passive defender can be reasonably captured by a Stackelberg game in that the jammer is an active player who sends signals at an intended level to interfere communication channels while the legitimate user rationally defends itself from such an attack. In the case where the defending user behaves actively or either side has information advantage, the **Nash equilibrium** becomes a reasonable solution concept. As eavesdropping is a passive attack where an eavesdropper receives information that "leaks" from a communication channel, the behavior of an eavesdropper can be viewed as that of a follower in a Stackelberg game against a user who employs active defenses. Depending on the role of a defender, the solution of the game may vary. **Table II summarizes the main message that comes out of this discussion.**

Table II. **Solution concepts and security game scenarios.**

	Active	Passive
Active	Nash Equilibrium	Stackelberg Equilibrium
Passive	Stackelberg Equilibrium	Nash Equilibrium

The next subsection focuses on jamming, which is followed by a subsection on eavesdropping. In the subsection on jamming, we review the game-theoretical formulations at the physical layer for communication channels, wireless networks and cognitive radios. In the subsection on eavesdropping, we introduce a game framework in which a friendly jammer can assist in reducing the effect of eavesdropping and a cooperative game model that allows nodes to self-organize into a network that maximizes the secrecy capacity.

3.1 Jamming

At the physical layer, jamming can adversely affect the quality and security of communication channels. The jamming phenomenon can be viewed as a game where a jammer plays against a legitimate user who follows the communication protocol. We organize our discussion below in different application domains of communications.

3.1.1 *Communication Channel.* The game-theoretic approach to jamming has been studied extensively over the last few decades [Başar 1983; Kashyap et al. 2004; Medard 1997; Borden et al. 1985]. The approach relies in many cases on the performance index chosen for a particular communication channel.

player zero-sum games, where there is a single objective function, minimized by one player and maximized by the other.

In [Başar 1983], the problem considered is one of transmitting a sequence of identically distributed independent Gaussian random variables over a Gaussian memory-less channel with a given input power constraint, in the presence of an intelligent jammer. In the problem formulation, a square-difference distortion measure $R(\gamma, \delta, \mu)$ is adopted, where γ, δ, μ are the strategies of the transmitter, the receiver and the jammer, respectively. The transmitter and the receiver seek to minimize R while the jammer seeks to maximize the same quantity. The conflict of interest between the receiver-transmitter pair and the jammer leads to an optimal transmitter-receiver-jammer-policy $(\gamma^*, \delta^*, \mu^*)$ as a **saddle-point solution** satisfying

$$R(\gamma^*, \delta^*, \mu) \leq R(\gamma^*, \delta^*, \mu^*) \leq R(\gamma, \delta, \mu^*), \quad \forall \gamma \in \Gamma_t, \delta \in \Gamma_r, \mu \in M_j, \tag{4}$$

where Γ_t, Γ_r, M_j are the sets of feasible strategies for the transmitter, the receiver and the jammer, respectively. It has been shown in [Başar 1983] that the best policy of the jammer is either to choose a linear function of the measurement it receives through channel-tapping or to choose, in addition, an independent Gaussian noise sequence, depending on the region where the parameters lie. The optimal policy of the transmitter is to amplify the input sequence to the given power level by a linear transformation, and that of the receiver is to use a Bayes estimator.

In [Kashyap et al. 2004], the authors consider a zero-sum mutual information game on MIMO Gaussian Rayleigh fading channels. Different from [Başar 1983], the effectiveness of the communication is measured by the mutual information $\mathcal{I}(\mathbf{x}, \mathbf{y})$, where $\mathbf{x}$ is the input to the channel from the output of the encoder; $\mathbf{y}$ is the output of the channel that follows a linear channel model

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} + \mathbf{v}, \tag{5}$$

where $\mathbf{H}$ is the channel gain matrix of appropriate dimensions, $\mathbf{v}$ is the jammer input and $\mathbf{n}$ is an additive noise. In this mutual information game, the encoder-decoder pair maximizes the mutual information and the jammer minimizes the same quantity. In their paper, Kashyap et al. have shown that, for a MIMO Rayleigh fading-Gaussian channel, a jammer with access to the channel input can inflict as much damage to communication as one without access to the channel input. The saddle-point strategy of the encoder is to transmit a circularly symmetric complex Gaussian (CSCG) signal and that of the jammer is to inject a symmetric CSCG signal independent of the transmitter's signal.

3.1.2 *Wireless Networks.* The application of game theory to wireless networks is a relatively new area. In [Altman et al. 2009], the authors consider the case of several jammers in wireless networks. The quality of communication is measured by the total signal to interference-plus-noise ratio (SINR) given by

$$v(T, J) = \sum_{i=1}^{n} \frac{\alpha_i T_i}{N^0 + \beta_i J_i}, \tag{6}$$

where $T_i, i = 1, 2, \cdots, N$, is the power level of each transmitter and J_i is the jamming power level for a jammer who attacks transmitter i. N^0 is the background noise level, and $\alpha_i, \beta_i > 0$ are fading channel gains for each transmitter. In their paper, Altman et al. consider the total transmission power constraint $\sum_{i=1}^{n} T_i = \overline{T}$ and

the total jamming power constraint $\sum_{i=1}^{n} J_i = \overline{J}$. The solution obtained has the property that the jammers equalize the quality of the best sub-carriers to a level as low as their power constraint allows while the transmitter distributes its power among the jamming carriers.

In [Sagduyu et al. 2009], a game-theoretic framework with incomplete information is developed for denial of service attacks at the MAC layer of wireless networks. The wireless nodes in the network can be of two types, either selfish or malicious, and have incomplete information regarding the types of other nodes. The node types constitute private information and are represented by probabilistic beliefs at individual nodes. A selfish node seeks to maximize its throughput with minimum transmission energy. A malicious node has a conflicting interest with other selfish nodes, attempting to minimize their utility; however, it does not have any incentive to jam other malicious nodes. Sagduyu et al. have obtained conditions under which the type of identities should be concealed or revealed to improve the individual performance as a selfish user or to reduce the system performance as a malicious user. The one-stage **Bayesian game** is further extended to a dynamic **repeated game** with incomplete information and a Bayesian learning mechanism is used to update the beliefs on different types.

3.1.3 *Cognitive Radio.* Cognitive radio is a novel communication paradigm that can provide high spectrum efficiency for wireless communications, in which transmission or reception parameters are dynamically changed to achieve efficient communication without introducing interference to traditionally licensed users (i.e. primary users) [Haykin 2005; Hossain et al. 2009].

One effective attack in cognitive radio networks, which resembles jamming in traditional wireless communication systems, is *primary user emulation attack* that has been studied in [Chen et al. 2008]. An attacker can send signals that have the same feature as primary users during the common period of spectrum sensing. Other honest secondary users will quit the frequency band upon detecting the emulated primary user signal. Consequently, the attacker can take over the entire frequency band (if selfish) or successfully interrupt the operation of secondary users (if malicious). The emulation attack is easier for an attacker to implement than conventional jamming because such an attack requires very low power to dominate the frequency band.

Once an attacker is found to be present, the secondary user needs to evade the attack in a passive manner by switching to another channel. This is similar to anti-jamming techniques. In a multichannel cognitive radio system, a secondary user cannot sense or transmit over all channels. An honest secondary user can randomly choose a subset of channels for sensing and transmission. A tradeoff often exists between the exploitation of good channels and evasion from an attacker, as an attacker may tend to jam good channels to cause maximum damage to the users.

In [Zhu et al. 2010], the authors introduce a **stochastic zero-sum game** model to study the strategies of an attacker and a secondary user in a jamming and anti-jamming scenario. Primary users, secondary users and jammers are the three types of agents in the system. The primary users dictate the system states $s \in \mathcal{S}$ and their transitions $\mathbb{P}(s, s'), s, s' \in \mathcal{S}$, whereas the secondary users and jammers do not cooperate in order to achieve their goals independently under different system

conditions. A secondary user accesses the spectrum opportunistically by sensing unoccupied channels for data communication. An attacker launches a primary user emulation attack to block a secondary user from using the channel, regardless of the channel state. The jamming and anti-jamming interactions between a secondary user and a jammer are modeled as a zero-sum stochastic game in which the jammer chooses a channel l to jam whereas the secondary user chooses a channel m to send data. The instantaneous payoff function for the secondary user is described by

$$R(s^{(k)}, m, l) = \begin{cases} 1 & \text{if } m \notin \mathcal{I}_k \text{ and } m \neq l, \\ 0 & \text{otherwise.} \end{cases}, \tag{7}$$

where $\mathcal{I}_k$ is a set of unoccupied channels at time k. The secondary user and the jammer seek for a mixed-strategy saddle-point pair (u, v) where u maximizes and v minimizes the expected discounted long term pay-off

$$\widetilde{R}_\delta(s, u, v) := \sum_{k=0}^{\infty} \delta^k \mathbb{E}_s^{u,v} R(s^{(k)}, m, l). \tag{8}$$

The Markovian game model captures not only the zero-sum interactions between secondary users and the jammers but also the dynamics of the system. The results indicate that the secondary users can enhance their security levels or increase their long-term payoffs by improving their sensing capabilities to confuse the jammer by choosing to communicate under states where the available channels are less prone to jamming. Through numerical experiments, the authors have shown that the payoffs of the secondary users increase with the number of available jamming-free channels and are eventually limited by the behavior of primary users.

3.2 Eavesdropping

Jamming is an active malicious behavior whereas eavesdropping is a passive one. A node in a wireless communication network can listen to other nodes within a communication range and extract private or secret information. Although current wireless networks are equipped with numerous cryptographic methods at a higher level, the security on the physical layer remains vulnerable. A pivotal concept of eavesdropping at the physical layer is the *secrecy capacity* that quantifies the maximum rate of reliable information transmitted from the source to its intended destination. To define formally the concept, we let C_{ij}^d be the Shannon capacity for the transmission between source i and its destination j and $C_{i,k}^e$ be the Shannon capacity of user i at the eavesdropper $k \in \mathcal{K}$, where $\mathcal{K}$ is a set of K eavesdroppers. The secrecy capacity is defined by,

$$C_{ij} = \max\left(C_{ij}^d - \max_{1 \leq k \leq K} C_{i,k}^e, 0\right). \tag{9}$$

This line of research started with the pioneering work of Wyner on wire-tap channel [Wyner 1975] and was followed in [Leung-Yan-Cheong and Hellman 1978], and [Csiszar and Korner 1978] for the scalar Gaussian wire-tap channel and the broadcast channel, respectively.

In [Han et al. 2009], a game-theoretical framework is established to investigate the interaction between a source that transmits the desired data and its friendly jammer that helps to jam the eavesdropper's channel. The helpful jammer reduces

the useful data rate from the source to the destination but also reduces the data rate that leaks from the source to the eavesdropper. The game is formulated from an economics perspective. The source is modeled as a buyer that determines the amount of "service" to buy from the jammers to optimize his secrecy capacity at minimum cost. A friendly jammer determines its price on its "services" to maximize its utility. The game has a hierarchical structure in which the friendly jammer acts as a leader, whereas the source behaves as a follower, and Stackelberg equilibrium is adopted as a solution concept for the game.

In [Saad et al. 2009], the authors consider using cooperation between wireless network nodes to improve the physical layer security of wireless transmission in the presence of multiple eavesdroppers. The cooperation problem is modeled as a **coalitional game** with non-transferable utility, and the authors propose a distributed algorithm for coalition formation based on the merge-and-split algorithm in [Apt and Witzel 2006], where also different concepts of stability of cooperation are introduced. Wireless users can autonomously cooperate and self-organize into disjoint independent coalitions and maximize their secrecy capacity by taking into account the security costs during an information exchange. It is shown that the proposed physical layer security coalitional game converges to optimal $\mathbb{D}_c-$stable partition[3], if such a partition exists. Otherwise, the final network partition is $\mathbb{D}_{hp}-$stable[4].

3.3 Discussion

At the physical layer of communication, jamming and eavesdropping are two major security issues. The literature on jamming is comparably richer than that of eavesdropping because the metrics used to quantify the jamming behavior are well defined by Shannon capacity, whereas the concept of secrecy capacity is relatively new. Different communication channels and networks have distinct payoff functions that can result in different security policies against jamming. From the recent works [Han et al. 2009] and [Saad et al. 2009], we can observe an emerging interest in studying eavesdropping in wireless networks for the privacy protection of users. In reality, jammers and eavesdroppers can coexist in communication networks. In [Mukherjee and Swindlehurst 2010], the authors consider the case where a malicious user can choose to behave as a jammer or an eavesdropper, and they formulate a zero-sum dynamic game to model the interactions between a transmitter and a dual eavesdropper/jammer. In addition, in [Zhu et al. 2011], the authors analyze the complex interactions between wireless users and a malicious node in the context of relay station-enabled wireless networks. The malicious node can eavesdrop, jam, or use a combination of both strategies, in a way to reduce the overall transmission rate of the network. These hybrid approaches yield a more realistic adversary behavior.

[3]A partition is $\mathbb{D}_c-$stable if no one in the partition is interested in leaving the partition through any operation to form other collections.

[4]A partition is $\mathbb{D}_{hp}$-stable if no one in the partition is interested in leaving the partition through merge-and-split to form other partitions.

4. SECURITY IN SELF-ORGANIZING NETWORKS

In this section, we address the security protocols that are designed for self-organizing networks using a game-theoretic approach. Since the early days of mobile networks, the structure and available services have seriously changed. In fact, today we are witnessing the emergence of a new generation of mobile networks with a large scale and high mobility of wireless devices, such as *vehicular networks* [Raya and Hubaux 2005], *delay tolerant networks* [Fall 2003], or *multi-hop wireless mesh networks* [Afanasyev et al. 2008]. Consequently, new types of services (e.g., *location based services*) are deployed in these networks. *Bluedating* [Braun and Schifferle 2005] [Hatt 2005], *Bluelocator* [Bretscher 2005], *Bluetella* [Weibel and Winterhalter 2005], *Aka-Aki*, *Friend Finders*, or *alert systems* in vehicular networks are some instances of these services that require active participation of mobile nodes in a distributed way. Note that these novel services can be provided with infrastructure or in an ad hoc manner. In most of these new services and infrastructures, the interaction between the wireless devices is rather short and we refer to such networks as *ephemeral networks*.

With these new services in ephemeral networks, the range of the types of misbehavior have extended beyond routing and packet forwarding problems to more application-oriented problems such as *false dissemination of data* or *Sybil attacks* [Douceur 2002]. Moreover, the certificate authority is not always present (or does not even exist), because the services are based on peer-to-peer communications.

There are also several economic aspects that should be kept in mind when designing efficient security protocols in these networks. For example, for any given network and application, the defender should consider the cost and benefit of deploying countermeasure techniques with different strategies. The defender can also better design its countermeasure, if he is aware of the strategies/payoff of the adversary. Note that *traditional reputation systems* cannot be merely transposed to these new types of networks, in view of these new services and infrastructures. In summary, we envisage new security threats that require new techniques to thwart them.

Game theory can be used as an efficient security mechanism-design tool in these networks. Using a game-theoretic approach, the designer of a security protocol can take into account the selfishness of individual mobile nodes and operators. It can also model the attacker's behavior and the interaction between defenders and attackers.

Some users (named *free riders* in game theory) can be tempted to avoid the contribution to the system and still benefit from its services. In game theory, *free riders* are those who consume more than their fair share of a public resource, or shoulder less than a fair share of the costs of its production. The free-rider problem is the question of how to limit free riding (or its negative effects) in these situations [Fudenberg and Tirole 1991]. With game theory, we can capture the cooperative and non-cooperative behavior of mobile nodes. We can design security protocols that provide incentives for individual nodes to contribute in the defense, i.e., avoid free riding.

Finally, using game theory we can avoid inadequate stability points (bad equilibria) and design security mechanisms that converge to the optimal possible solution.

In the following subsection, we first present how the interactions between an attacker and a defender can be modeled using game theory, in vehicular networks [Buchegger and Alpcan 2008]. Then we address security protocols that are designed for mobile networks, using a game-theoretic approach [Raya et al. 2008; Reidt et al. 2009; Bilogrevic et al. 2010]. In the literature reviewed below, the authors first define the security problems that are solved by the active participation of mobile nodes. Then they analyze the equilibrium of the game between mobile nodes or the adversary and mobile nodes. The results of the equilibrium analysis can be used to design an efficient protocol to be performed in a distributed manner. Note that there exist mechanisms based on reputation to address the security problems. Michiardi and Molva present a game-theoretical approach that analyzes the robustness of such collaborative mechanisms in [Michiardi and Molva 2002].

4.1 Security Games for Vehicular Networks

In [Buchegger and Alpcan 2008], the authors study several security problems of vehicular networks within a game-theoretic framework. They model security games as two-player **zero-sum games**. One of the players is the attacker who wants to perform *jamming* and *Sybil* attacks against a vehicular network. The attacker can also inject bogus messages that *disseminate false information*, in order to disrupt traffic. The second player of the game is a set of mobile nodes that wants to deploy countermeasures in the most effective manner.

Buchegger and Alpcan present a set of graphs that models the network structure including the road network, the vehicular traffic, and the data traffic. Using these graphs, they calculate the centrality measures that show how important a particular road segment is. The centrality measures are then used to calculate the payoffs of the players in the game. The payoffs represent the risks or penalty for the attackers to be captured or they represent the benefit for the defender.

As an example for the defined security game, an attacker jams (attacks) one road segment with some probability according to its mixed attack strategy. Figure 2 shows a simple example. In response, the defender, i.e. the network stakeholder (designer, city planner, law enforcement agency), allocates defense resources (e.g., deploy roadside unites) to the same or another road segment according to his own strategy. The outcome of a specific game is determined by the game matrix that contains the cost (payoff) values for each possible action-reaction combination.

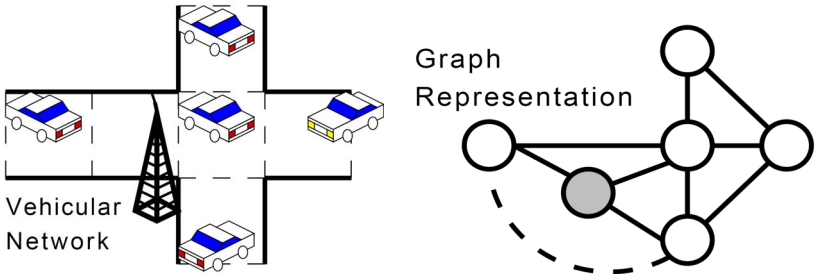

Fig. 2. Connectivity of a vehicular network (including roadside unites). The dashed line represents indirect communication, e.g. via wired cables.

The game matrix maps player actions (attack or defend) on the road segment graph (or here the grid obtained by quantizing the region map) to outcomes, payoff and cost, for the attacker and defender, respectively. For convenience the action space (graph or grid) is represented as a vector. The game matrix entries can be a function of the importance of each road segment (as characterized by, e.g., the betweenness centrality [Wasserman and Faust 1994]) and the risk of detection (gain from capture) for the attacker (defender), as well as other factors. Assuming that the attacker is the row player (maximizer) and the defender is the column player (minimizer), the game matrix P is defined as:

$$P = [P(i,j)] := \begin{cases} \overline{C}(i) & \text{if } i \neq j \\ r & \text{if } i = j, \ \ \forall i,j \in \mathcal{N}_r \end{cases},$$

where $\overline{C}$ is the betweenness centrality of the road segment as a function of the average traffic pattern and $\mathcal{N}_r$ is the set of nodes of the road graph. The parameter r is a fixed scalar that represents the risk or penalty of capture for the attacker (benefit for defender), if the defender allocates resources to the location of the attack, i.e. the same square on the map.

Buchegger and Alpcan first prove the existence of a Nash equilibrium for the complete information **zero-sum game**. But, as the players of the game often have limited information about the preferences of the opponents, they also evaluate a **fuzzy game** in which players attempt to maximize their utility using an imprecise payoff matrix [Garagic and Cruz 2003]. The **fuzzy game** is then solved using the fuzzy linear programming approach [Campos 1989]. A defuzzification method is also used and the equilibrium can be calculated solving a regular linear and dual linear programs. Finally, the authors assume that the players know only their own payoffs. They investigate a **fictitious play** mechanism for the defined game. In other words, players repeatedly use strategies that are best responses to the historical averages, or empirical frequencies of opponents they observe. The authors define a discrete and stochastic variant of fictitious play that results in an evolutionary version of the game.

All the above defined games are analyzed using realistic simulation data obtained from traffic engineering systems [Sommer 2007]. Buchegger and Alpcan then derive mix strategy Nash equilibrium for all games. The results show that in comparison, the mobile nodes can optimize their defense strategy in a **zero-sum game** better than with the naive strategy of defending locations that ignore attacker behavior. Moreover, the authors show that **fuzzy game** results are approximately similar to the **zero-sum game** solutions and the **fictitious play** leads to more randomized mixed strategies.

4.2 Revocation Games in Ephemeral Networks

In [Raya et al. 2008], the authors design and evaluate a revocation protocol for ephemeral networks, using a game-theoretic approach. They assume that mobile nodes can detect the malicious behavior with a certain probability. The adversary again tries to disseminate false information into the system. Figure 3 illustrates an example of revocation in a vehicular ad hoc network (VANET).

Raya et al. consider three revocation strategies for each player (i.e., mobile node) based on the existing protocols. First, a player can *abstain* from the local revocation

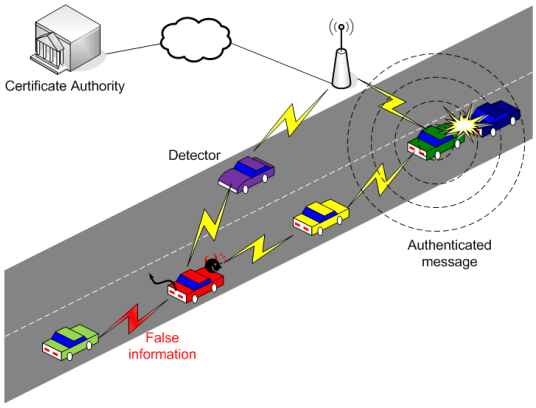

Fig. 3. An example of revocation in a vehicular network. The violet car initiates a revocation process against the malicious node (red car) that disseminates false information (no accident and traffic jam ahead). The green and the yellow cars will then participate in the revocation game and ultimately revoke the malicious node.

procedure by playing A. This strategy captures the fact that mobile nodes are unwilling to contribute to the local revocation procedure. Second, a player can participate in a local *voting* procedure by casting a vote V against a detected attacker [Chan et al. 2005]. Finally, following the protocol suggested in [Moore et al. 2007], a player can *self-sacrifice* by playing S, i.e., to declare the invalidity of both its current identity (the pseudonym it currently uses) and the identity of the attacker. The authors model the revocation problem using a **finite dynamic (sequential) game** with mobile nodes as players, as shown in Figure 4.

Using a backward induction technique, Raya et al. obtain the strategy of mobile nodes that lead to a subgame-perfect equilibrium. They show that in this game the revocation decision is left to the last players, either by voting or self-sacrifice. A new class of games called **variable costs game** is defined, where the cost of attack increases linearly with time. The authors evaluate the game and compute the subgame perfect equilibrium in that case. They obtain the strategies that lead the game to a *subgame perfect equilibrium*.

For example the authors show that for any given values of n_i (number of remaining nodes that can participate in revocation), n_r (number of remaining required votes), v, and δ (cost of attack in any single time slot), the strategy of player i that results in a subgame-perfect equilibrium is:

$$s_i = \begin{cases} A \text{ if } \begin{array}{l} [(1 \le n_i < \min\{n_r - 1, \frac{1}{\delta}\}) \\ \wedge(v + (n_r - 1)\delta < 1)] \vee [(1 \le n_i < \frac{1}{\delta}) \\ \wedge(v + (n_r - 1)\delta > 1)], \end{array} \\ V \text{ if } (n_i \ge n_r - 1) \wedge (v + (n_r - 1)\delta < 1), \\ S \quad \text{otherwise.} \end{cases}$$

The above results show that players are more concerned about quickly revoking

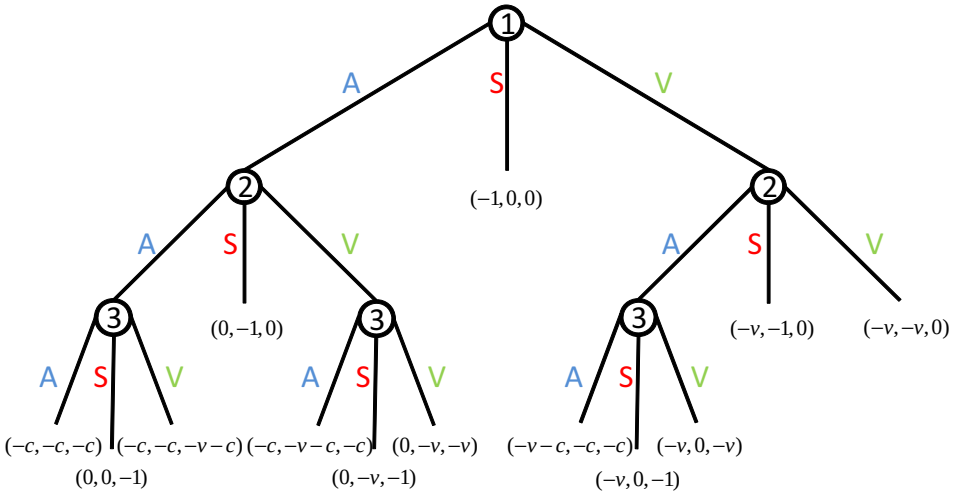

Fig. 4. Extensive form of the revocation game model when the cost induced by the attack is fixed, i.e., c. The game is represented by a tree and node 1 plays the first action. The game has three stages corresponding to the moves of the three players. The actions (abstain A, self-sacrifice S, and vote V) are represented on each branch of the tree. The leaves of the tree represent the costs of the game for all players. v and 1 are the costs of voting and self-sacrifice, respectively.

the attacker because the cost of the attack increases with time. Hence, under some conditions, they will begin the revocation process (by voting or self-sacrifice) in the early stages of the game.

Finally, Raya et al. use the results of the game analysis to design a revocation protocol by considering practical issues. The protocol provides incentive for mobile nodes to actively participate in revocation, and it results in an optimal and fast revocation process. Realistic simulation results in vehicular networks show that this game-theoretic approach achieves the elusive tradeoff between the approaches found in the literature.

In [Bilogrevic et al. 2010], the authors suggest to provide incentives to users that sacrifice themselves. This will guarantee the successful revocation of the malicious nodes even if they collude. They dynamically adapt the parameters to nodes reputations and establish the Nash equilibrium on-the-fly, minimizing the social cost of the revocation. Finally, they define a protocol to select a unique Nash equilibrium.

Reidt, Srivatsa, and Balfe [Reidt et al. 2009] consider the same scenario and design a distributed, active, robust, and detection error tolerant revocation scheme by using a game theoretic approach. The authors first design a revocation protocol called **karmic-suicide**, that provides rewards to the nodes that perform the self-sacrifice action. The self-sacrifice actions should then be reported to the certificate authority in order to be verified. After the verification by the certificate authority, the authority will give the reward to the nodes that contributed to the revocation by self-sacrifice. The authors design a judgment system at the certificate authority that takes into account the probability of false positives and negatives, in order to decide whether the self-sacrifice action has taken place against a malicious node.

Reidt, Srivatsa, and Balfe then verify whether their incentive for honest nodes to revoke is sufficient, and if so, how quickly honest nodes will revoke malicious nodes. To do so, they use a game-theoretic approach (using a **descending price auction**) and show that their scheme provides rational nodes with an incentive to self sacrifice. The authors show that the karmic-suicide revocation scheme works in a network environment with imperfect intrusion detection systems on the nodes' side and with an imperfect judgment system.

4.3 Discussion

In this section, we have presented security games in self-organizing networks. The decision makers are mainly mobile nodes that can be cooperative, selfish, or malicious. In [Buchegger and Alpcan 2008], the authors use **zero-sum games** to model the interaction between attacker and defender. This is an appropriate game, because it can capture the conflict of interest between the players. But in [Raya et al. 2008], the authors use a dynamic game because it appropriately models the sequential interaction between wireless nodes in the shared medium. They use a cost game as they want to model the incentive and stimulate cooperation between benign nodes against one malicious node. In [Bilogrevic et al. 2010] and [Reidt et al. 2009], the authors model the rewards of agents by including self-sacrifice benefits to payoff calculations.

In [Buchegger and Alpcan 2008], the authors also consider the **fuzzy** and **fictitious games**, due to lack of complete information. On the contrary, in [Raya et al. 2008; Reidt et al. 2009], the authors assume a complete information context to make the optimal decision. This model can be extended to consider incomplete information, in particular on the number of players participating in the revocation protocol. Moreover, the effect of estimated parameters before each revocation game can be investigated. In the games addressed in this section, we also had some examples of mechanism designs, where the equilibrium analysis results are used to design a revocation protocol.

5. INTRUSION DETECTION SYSTEMS

An Intrusion Detection System (IDS) is an important defense mechanism against a variety of attacks that can compromise the security of an information system [Debar et al. 2005]. It is designed and used to detect the unauthorized use of systems, networks, and related resources and in many cases it is also capable of deflecting or deterring them. In practice, IDSs are deployed at different levels to monitor the traffic of applications, key hosts, networks and gateways between two networks. IDSs can be signature based or anomaly-based. Signature-based IDSs, such as Snort [SnortTeam 2010] and Bro [Bro 2010], store a database of traffic or activity patterns related to known attacks used to compare attack signatures to recognize and prevent infected files, programs, or active Web content from intrusion. Anomaly-based IDSs work by comparing system behavior with normal behavior and by raising alerts whenever an abnormal behavior is detected.

Game theory is generally accepted as an appropriate technique to study IDSs due to the non-cooperative interaction between the attacker and the detector. In [Sallhammar et al. 2006], a game-theoretic method is used to compute probabilities

of an expected attacker behavior and these probabilities are used in a transition matrix model to assess security in an interconnected system. In [Årnes et al. 2006], the authors propose a real-time risk assessment method for information systems and networks based on IDS. The system risk is dynamically evaluated using hidden Markov models, providing a mechanism for handling data from sensors with different levels of trustworthiness. Stochastic games appear to be an appropriate tool to study stochastic transitions in an adversarial environment. In [Alpcan and Başar 2006], a two-person zero-sum Markov security game is proposed to capture the interactions between malicious attackers and an IDS. Games considered in that paper have the property that only partial and indirect observations of the moves of the opponents are available to the players. Methods such as Markov Decision Process (MDP) value iteration, minimax-Q, and naive Q-learning have been studied heuristically through numerical simulations and illustrative examples. In [Bohme and Moore 2009], a dynamic iterative model is devised from an economic point of view in the setting of a security investment problem that reflects dynamic interaction between a defender and an attacker who targets the weakest link.

Other earlier works on game-theoretical models in intrusion detection include [Alpcan and Başar 2003] and [Alpcan and Başar 2004], where game-theoretical frameworks are used to model access control systems and security warning systems. In [Liu et al. 2006], a **dynamic Bayesian game** approach is used to analyze the interactions between pairs of attacking and defending nodes in wireless ad hoc networks where the defender updates his belief on his opponent. The authors show that a Bayesian hybrid detection switching between lightweight and heavyweight monitoring leads to detection energy efficiency for the defender. In [Lye and Wing 2002], the authors present a two-person **stochastic general-sum game** between an attacker and an administrator for analyzing the security of computer networks. A more recent work, [Nguyen et al. 2008], focuses on **repeated zero-sum games** and generates mixed strategies from fictitious play, a dynamic learning algorithm that observes past history with either complete or incomplete observation.

In the following subsections, we discuss how game-theoretical methods can be used to automate and optimize the configuration and responses of IDSs. We start with a single IDS configuration problem in which a stochastic game is used to model the dynamic configuration policies of an IDS in response to an adversary who attempts with a sequence of attacks [Zhu and Başar 2009]. Similar problems also appear in networked IDS systems. We discuss the extension of the game model to an IDS network in which each IDS strategically employs its optimal security levels, which leads to interdependent security among different IDSs. We introduce the notion of security capacity, which quantitatively captures the maximum achievable network level of security. No policies exist to achieve a security target that is beyond the capacity [Zhu et al. 2010b]. The game-theoretical framework also applies in collaborative IDS networks. We will discuss the decentralized communication protocol that achieves effective collaboration proposed in [Zhu et al. 2009]. Finally, we present a Stackelberg stochastic game framework used to automate intrusion responses upon receiving alerts from IDSs [Zonouz et al. 2009].

5.1 IDS Configuration

An appropriate configuration and control for effective detection is a challenging problem for an IDS. This is mainly due to the large number of detection libraries or categories with a considerable set of configuration parameters. For example, a current version of Snort IDS contains 51 categories and nearly 10,000 signature rules [Boutaba and Aib 2007]. A concern with IDS configuration is to find an appropriate tradeoff between security enforcement levels and the performance of an information system. The usability of a system degrades when maximum security is applied at all times, but the system is prone to attacks when the enforcement of security is overlooked [Schaelicke et al. 2003]. Hence, a dynamic and iterative security system needs to be employed to detect attacks while minimizing the consumption of resources for the sake of balancing system performance and security.

A simple, two-player, static Bayesian game is described in [Liu et al. 2006]. A player can be either a regular node or a malicious one, which is private information to the node itself. A malicious node can choose to attack or to not attack, whereas a defending node can choose to monitor or to not to monitor. A defender's security is measured by the monetary value of his protected assets w. A loss of security is represented by $-w$ whose value is equivalent to a degree of damage such as loss of reputation, loss of data integrity or cost of damage control. The payoff matrix of the game in strategic form is given in Tables III and IV, for two different types of players. In the matrix, $\alpha, \beta \in [0, 1]$ represent respectively the detection rate and the false alarm rate of the IDS. The cost of attacking and monitoring are denoted by $c_a, c_m > 0$, respectively. A defender assigns a prior probability μ_0 to player i being malicious. The authors have shown that when $\mu_0 < \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$, the Bayesian game admits a pure-strategy equilibrium $\{(Attack$ if malicious, $Do\ not\ attack$ if regular), $Do\ not\ monitor$, $\mu_0)\}$ and the game does not have pure-strategy if $\mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$. The Bayesian game can be played repeatedly and the defender can update his prior belief using Bayes' rule based on the history of plays. The authors also propose a Bayesian hybrid detection approach that comprises two monitoring systems: lightweight monitoring and heavyweight monitoring. The defender decides whether to activate the heavyweight monitoring system in next stage game based on his updated beliefs. The advantage of implementing the IDS system as a Bayesian hybrid IDS is that it allows to save significant energy while minimizing the potential damage inflicted by an undetected attacker. It is a result of the following equilibrium property: the monitoring probability does not depend on the defender's current belief on his opponent's maliciousness, but rather influences the attacker's behavior.

Table III. Player i is malicious.

	Monitor	Not Monitor
Attack	$(1-\alpha)w - c_a, (2\alpha-1)w - c_m$	$w - c_a, -w$
Not Attack	$0, -\beta w - c_m$	$0, 0$

In [Zhu and Başar 2009], the authors use a **zero-sum stochastic game** which captures the dynamic behavior of the defender and the attacker. Different from a

Table IV. Player i is regular.

	Monitor	Not Monitor
Not Attack	$0, -\beta w - c_m$	$0, 0$

static zero-sum game formulation, a stochastic game involves a transition between system states that are controlled by the actions taken by the players at every time instant. As an example, the system state s can be considered to be binary, i.e., either in a healthy state or in a failure state. The action of the defender at a given time instant is to choose a set of libraries or options $\mathcal{L}$ as its configuration whereas the action of the attacker is to choose an attack a from a set of possible ones. A stationary optimal policy is a state-dependent strategy that suggests an action with certain probability at a state. The change of configurations from time k_1 to time k_2 implies for the defender to either load new libraries or features to the configuration or unload part of the current ones. On the other hand, the actions taken by the attacker at different times constitute a sequence of attacks used by the attacker. The dynamic interaction is hence captured by the stochastic game.

The optimal policies for both players can be found either by off-line calculations or by on-line learning. The discounted zero-sum, stochastic game has a value vector $\mathbf{v}_\beta = [v_\beta(s)]_{s\in\mathcal{S}}$, which is the unique solution of the fixed-point equation

$$\mathbf{v}_\beta = \text{val}\left[\mathbf{R}(s, \mathbf{v}_\beta)\right], \tag{10}$$

where val is a function that yields the game value of a zero-sum matrix game [Başar and Olsder 1999; Raghavan and Filar 1991], and $\mathbf{R}(s, \mathbf{v}_\beta)$ is an auxiliary matrix game defined by

$$\mathbf{R}(s, \mathbf{v}_\beta) = \left[r(s, a_t, a_d) + \beta \sum_{s'\in\mathcal{S}} \mathbb{P}(s'|s, a_t, a_d) v_\beta(s') \right]_{a_t\in\mathcal{A}, a_d\in\mathcal{L}^*}. \tag{11}$$

Here, $\mathcal{A}$ and $\mathcal{L}^*$ are the sets of actions available to the attacker and the defender, respectively. $\mathbb{P}$ is the transition law that depends on the chosen actions, $\mathcal{S}$ is the state space of the system, r is the instantaneous reward to the defender, and β is a discount factor.

A **value-iteration** method, as well as Newton's iterative scheme, are used to solve (10) for finding the optimal strategies for the attacker and the defender. A more practical learning approach, based on **Q-learning**, is adopted to learn optimal strategies from an iterative update of Q-functions based on the samples of outcomes from the game. An advantage of learning algorithms is that they mimic the online behavior of the players, and the knowledge of transition probabilities contingent on actions is not needed. It is proven in [Zhu and Başar 2009] that the Q-learning algorithm for zero-sum stochastic games converges, under mild assumptions on the step size, to an optimal Q-function that yields the equilibrium policies.

The dynamic online IDS configuration described in [Zhu and Başar 2009] can be used together with an optimal offline default IDS configuration discussed in [Zhu and Başar 2011a]. In [Zhu and Başar 2011a], the authors apply the concepts of indices of power, namely, Shapley value and Banzhaf-Coleman index, from cooperative game theory to quantify the influence or contribution of libraries in an IDS with respect to given attack graphs. Such valuations take into consideration the

knowledge on common attack graphs and experienced system attacks and are used to configure an IDS optimally at its default state by solving a knapsack optimization problem.

5.2 Networked IDS

The single IDS configuration problem can be extended to a networked intrusion detection system in which each IDS operates independently and the security of the subsystem protecting an IDS is dependent on the well-being of the others. In [Zhu et al. 2010b], the authors formulate a **stochastic nonzero-sum dynamic game** with N defending machines and M attackers in which, in every time slot, the defenders choose detection configurations and attackers choose the attacks to launch. The stationary Nash equilibrium policies of the $N+M$-person game can be characterized and found by solving a bilinear programming problem. The authors show the existence of the solution and obtain iterative algorithms that yield the $\epsilon-$Nash equilibrium. The authors propose the notion of security capacity defined as the largest worst state optimal value

$$\Omega_i = \max_h \min_s \mathcal{V}_i^*(s),$$

where s is the system state. $\mathcal{V}_i^*$ is the set of optimal payoffs at an equilibrium to a machine n_i that operates in a network and it is indexed by h, which corresponds to all (stationary or non-stationary) Nash equilibrium strategies.

The importance of knowing the security capacity is that it gives an upper bound on achievable security targets. It separates a realistic security goal from an unrealistic one. The authors show that the feasibility of an optimization problem can serve as a test of the achievability of a given target capacity $\overline{\Omega}_i$.

5.3 Collaborative Intrusion Detection System Networks

An Intrusion Detection Network (IDN) is a collaborative IDS network designed to overcome the vulnerability to zero-day attacks by having each peer IDS benefit from the collective knowledge and experience shared by other peers. This enhances the overall accuracy of intrusion assessment, as well as the ability of detecting new intrusion types. However, many proposed IDS collaboration systems, such as in [Yegneswaran et al. 2004; Wu et al. 2003; Zhou et al. 2005], assume that all IDSs cooperate honestly. The lack of trust management leaves the system vulnerable to malicious peers.

A few trust-based collaboration systems (e.g. [Sen et al. 2008; Fung et al. 2008]) and distributed trust management models (e.g. [Fung et al. 2008; C. Duma and Caronni 2006; Fung et al. 2009]) have been proposed for IDSs to cooperate with each other effectively. However, none of these proposed models study incentives for IDS collaboration. Without incentives, a collaboration system might suffer from a "free-rider" problem [Keppler and Mountford 1999], where some IDSs can take advantage of others by always asking for assistance from others but not contributing. This will eventually degrade the expected performance of the collaboration system. Therefore, an effective incentive mechanism is essential to encourage peers in the IDN to cooperate truthfully and actively.

More specifically, as shown in Figure 5, an IDN is composed of a group of inde-

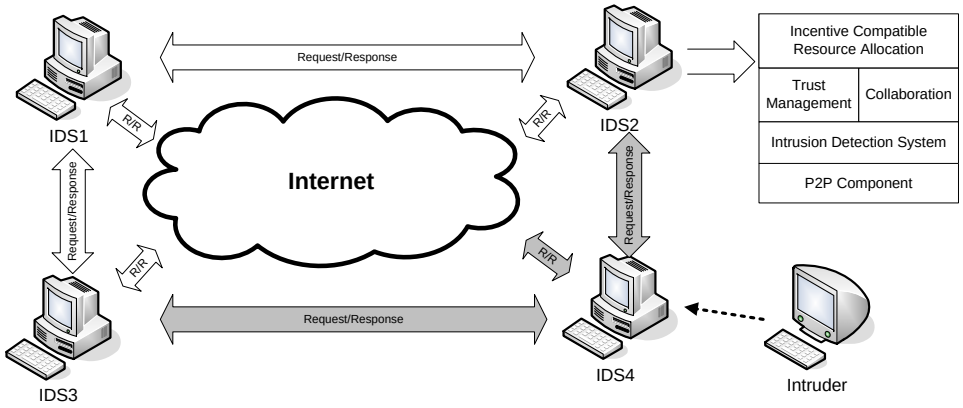

Fig. 5. Architecture of an IDS collaboration system: IDS communicates through P2P networks. The collaborative mechanism relies on the trust management and the resource allocation scheme.

pendent IDSs and the communication among the peers is through a peer-to-peer communication layer. An IDS sends requests to selected neighbors to seek assistance when suspicious activities are detected. These requests can be related to alert ranking, problem diagnosis, or blacklist identification. The responses from its neighbors can help the IDS to identify new types of intrusions. An IDS may receive requests from different peers. Responding to these requests requires a certain amount of computing resources, such as CPU, memory, or network bandwidth. An IDS may have a limited resource budget to assist other IDSs in the network and cannot satisfy all the requests. An IDS may also free-ride the system or send out false intrusion assessments. Therefore, an effective resource allocation scheme is needed for an IDS to manage responses to requests from neighboring IDSs.

Much work has been done on the collaborative framework and trust management among intrusion detection systems, such as [Fung et al. 2008; C. Duma and Caronni 2006; Fung et al. 2009]. In [Fung et al. 2009], the authors propose a trust management system where IDSs exchange test messages to build trust among themselves. Each IDS selects a trace of possible attacks from its knowledge database where the risk level of the attack is known by the IDS. Then, it sends the trace to its acquaintances for the purpose of testing their trustworthiness. Each acquaintance evaluates the risk of the possible attacks based on the trace it receives and sends back the feedback to the sender. The sender IDS compares the feedbacks from others with its own knowledge and generates a satisfaction level for each feedback using a satisfaction mapping function. A trust value is a numerical value used to predict the level of truthfulness for the next feedback from a certain peer. In [Fung et al. 2008], the authors use a simple weighted average model to predict the trust value whereas in [Fung et al. 2009] the authors use a Bayesian statistics model to estimate the trust value, as well as the confidence level of the trust estimation.

Incentive design has been well studied in peer-to-peer (P2P) networks. In [Ma et al. 2004], the authors use a game-theoretical approach to achieve differentiated services allocation based on the history of a peer's contribution to the community. However, this system relies on a centralized contribution ranking system, which ex-

hibits a single-point-of-failure. The authors in [Yan et al. 2007] propose an optimal resource allocation scheme for file providers. The resource allocation is based on the ranking of consumers of files shared by file providers. A max-min optimization problem is constructed to find the optimal solution that achieves fairness in the resource allocation. However, their approach relies on an independent ranking system, and the relation between ranking and the contributions of consumers has not been studied. The authors also do not study the convergence of the resource allocation of the entire system. The paper [Theodorakopoulos and Baras 2007] adopts a game-theoretical approach to study the impact of malicious users in P2P networks. The modeling of malicious behavior there is based on users' choices of either "cooperate" or "defect" at each time slot. A game learning algorithm is used for each peer to make a decision at each stage by aggregating the play history in a certain way. However, there is no theoretical result yet to show the convergence of fictitious play to a unique Nash equilibrium in the general topology for the proposed model.

Incentive compatibility has also been an important topic in auction design, whose analysis heavily relies on a game-theoretical approach, such as in [Semret et al. 2000] and [Krishna 2002]. For example, in [Semret et al. 2000], incentive compatibility relates to a mechanism in which bidders can only benefit the most by bidding at their true valuations. It is also shown in [Semret et al. 2000] that under certain conditions, the bidding profiles converge to a Nash equilibrium, which provides an efficient allocation of the resource under this mechanism.

In [Zhu et al. 2009], the authors propose an incentive compatible resource allocation scheme for trust-based IDS collaboration networks, where the amount of resources that each IDS allocates to help its neighbors is proportional to the trustworthiness and the amount of resources allocated by its neighbors to help this IDS. The authors introduce an $N-$person (or peer) non-cooperative game in which every IDS finds an optimal resource allocation to maximize the aggregated satisfaction levels of its neighbors. It is shown that under certain controllable system conditions, there exists a unique Nash equilibrium. The properties of the equilibrium is shown to be incentive compatible, i.e., if u, v are two collaborating IDSs in the network, the helping resource p_{uv} from u to v increases with helping resource p_{vu} from v to u, and when peer u trusts v more, the marginal helping resource from u to v increases. In addition, the marginal helping resource from u to v can be adjusted by system parameters.

Experimental results demonstrate that an iterative algorithm converges geometrically fast to the Nash equilibrium, and the amount of help an IDS receives from others is proportional to its helpfulness to others.

5.4 Intrusion Response

Aside from IDSs, intrusion response techniques also play important roles in taking responsive actions based on received IDS alerts to prevent attacks before they can cause potential damages and to ensure the safety of the computing environment. In [Zonouz et al. 2009], the authors aim to automate intrusion responses and employ a game-theoretic response strategy against adversaries in a two-player **Stackelberg stochastic game** to design an automated cost-sensitive intrusion response system called the Response and Recovery Engine (RRE). The interaction

between the defender and the attacker follows the same dynamic feature as in [Zhu and Başar 2009] but creates a hierarchical structure in which RRE acts as the leader and the attacker behaves as the follower. At each time instant, RRE uses the attack-response tree (ART) together with the received IDS alerts to evaluate various security properties of the system. ARTs provide a formal way to describe system security based on possible intrusion and response scenarios for the attacker and the response engine, respectively. In addition, ARTs enable RRE to consider inherent uncertainties in alerts received from IDSs when estimating the system's security and deciding on response actions. The RRE automatically converts the attack-response trees into partially observable competitive Markov decision processes to be solved to find the optimal response action against the attacker, in the sense that the maximum discounted cumulative damage that the attacker can cause later in the game is minimized. Applying the game-theoretic approach, RRE adaptively adjusts its behavior according to the attacker's possible future reactions, thus preventing the attacker from causing significant damage to the system by taking an intelligently chosen sequence of actions. To deal with security issues with different granularities, RRE's two-layer architecture consists of local engines, which reside in individual host computers, and the global engine, which resides in the response and recovery server and decides on global response actions once the system is not recoverable by the local engines. Furthermore, the hierarchical architecture improves the system scalability, facilitates the ease of design, and enhances the performance of RRE, so that it can protect computing assets against attackers in large-scale computer networks.

5.5 Discussion

In this section, we have discussed game-theoretical methods used for finding security policies in IDSs. Many models have been proposed, ranging from games of complete information to Bayesian games of incomplete information, from static games to repeated or stochastic games, from strategic games to Stackelberg games. Earlier works such as [Liu et al. 2006] and [Nguyen et al. 2008] consider two actions each for the defender and the attacker, i.e., "defend" or "not to defend" and "attack" or "not to attack". Recent works such as [Zhu and Başar 2009] and [Zonouz et al. 2009] have undertaken a more comprehensive investigation of IDSs, looking into more specific configurations and responses that an IDS can have. From [Lye and Wing 2002], [Zhu et al. 2010b] and [Zhu et al. 2009], we can see an emerging interest in studying IDSs in a network setting. The operation of cooperative or non-cooperative IDSs at a network system level is a more critical issue than the device-level configuration IDSs. In many works, an on-line learning approach to games is more favorable than an off-line determination of security policies. It allows IDSs to adapt to the changing environment and to take into account many uncertain factors due to either lack of knowledge or uncertainty in the environment.

The game-theoretic modeling of IDSs and cyber policies also enables new frameworks that allow to interface with physical layer security. In [Zhu and Başar 2011c], [Zhu and Başar 2011b] and [Zhu and Başar 2012], IDS configuration problems are studied in the context of resilient control systems in critical infrastructures. Cyber security is a pivotal aspect of resilience in control systems, and security models developed for IDSs can be used as a baseline model for studying security issues in

more complex cyber-physical systems.

6. ANONYMITY AND PRIVACY

Privacy is the ability to control what information (e.g., personal data and location) we reveal about ourselves. There are many privacy concerns in the new generation of mobile applications and the Internet in general. Fortunately, in many contexts, privacy can be achieved through cooperation amongst entities. Users should evaluate their privacy themselves and investigate different strategies to set their privacy at their chosen level. **Game theory** can help users to decide whether they want to participate in privacy-preserving mechanisms, how much they would be able contribute and how much privacy they would be able to achieve.

In this section, we first address a game-theoretic approach in order to analyze location privacy in mobile networks. We then focus on the economic aspects of privacy. Finally, we discuss how the tension between privacy and trust can be evaluated using a game-theoretic framework.

6.1 Location Privacy

A frequently proposed solution to protect *location privacy* suggests that mobile nodes collectively change their pseudonyms in regions called mix zones, as shown in Figure 6. In [Freudiger et al. 2009], the authors analyze the non-cooperative behavior of mobile nodes by using a game-theoretic model, where each player aims at maximizing its location privacy at a minimum cost.

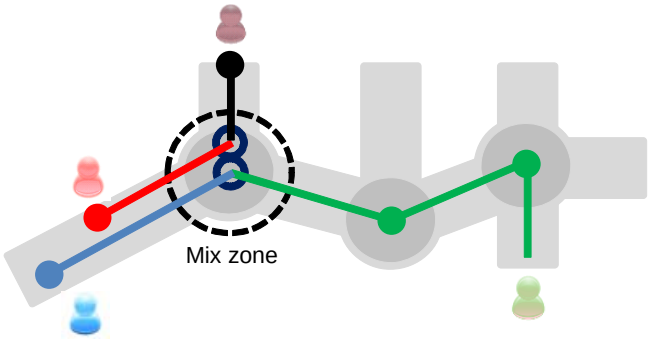

Fig. 6. An example of a 2-node mix zone, where mobile nodes change their identifiers at the mix zone. The adversary becomes confused about whether the green exiting node was blue or red before entering the mix zone.

Freudiger et al. first present a *user-centric location privacy model* to capture the evolution of location privacy for each user over time. The model considers the beliefs of users about the tracking power of the adversary, the amount of anonymity that users obtain in the mix zones, the cost of pseudonyms, and the time of changing pseudonyms. Using this model, a **static game** is defined where the players are mobile nodes. Each player has two strategies: Cooperate (C) and thus change her

pseudonym at mix-zones, or Defect (D). The payoff can be calculated using the user-centric location privacy model.

Freudiger et al. analyze Nash equilibria in an n-player **complete information game**. They show that the users can change pseudonyms only when it is necessary for themselves and can encounter cooperative nodes. They prove that the all defection strategy profile is always an equilibrium and an equilibrium with cooperation does not always exist, as payoffs in a n-player game can be very asymmetric.

Because mobile nodes in a privacy-sensitive system do not know their opponents' payoffs, the authors also consider and evaluate the **incomplete information game**. In this game, players decide their moves based on their beliefs about their opponents' types. The player type is defined as the level of location privacy for the user. The authors establish an equilibrium in which each player adopts a strategy based on a threshold: if the type of a player is above a *threshold* $\tilde{\theta}_i$, it defects, otherwise it cooperates. This is illustrated in Figure 7.

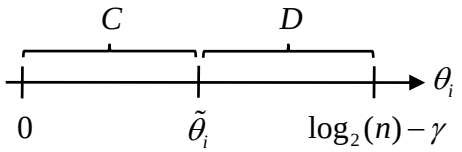

Fig. 7. Description of the threshold equilibrium in the 2-player incomplete information game. Threshold $\tilde{\theta}_i$ determines the best response of player i; n is the number of nodes in the mix zone.

Freudiger et al. establish that symmetric Bayesian-Nash equilibria exist with the above threshold strategies in n-player games and derive the corresponding equilibrium strategies. The results show that if pseudonyms are expensive, then users care more about the coordination success. In contrast, with cheap pseudonyms, users tend to become selfish. They also show that with more lower type users (users with low levels of location privacy), the probability of cooperation at equilibrium is smaller. In other words, selfish nodes cooperate less because they have enough partners whenever they need. Finally, they design a protocol to change pseudonyms in mix zones, based on the results of the game-theoretic analysis.

Humbert et al. consider a local adversary equipped with multiple eavesdropping stations [Humbert et al. 2010]. They study the interaction between the local adversary deploying eavesdropping stations to track mobile users and mobile users deploying mix zones to protect their location privacy. They use a game-theoretic model to predict the strategies of both players and derive the strategies at equilibrium in complete and incomplete information scenarios. Based on real road-traffic information, they quantify the effect of complete and incomplete information on the strategy selection of mobile users and of the adversary. Their results enable system designers to predict the best response of mobile users with respect to a local adversary strategy, and thus to select the best deployment of countermeasures.

6.2 Economics of Anonymity

Anonymity and privacy cannot be obtained by individual senders or receivers. The users should trust the infrastructure to provide protection, and other users must use the same infrastructure as well. In [Acquisti et al. 2003], the authors explore the incentives of participants to offer and use anonymity services with a game-theoretic approach. They analyze the economic incentive for users to send their messages through mix-nets [Chaum 1981].

The set of strategies for any given user includes four actions. First, the user can send and receive her traffic and receive the dummy traffic that is generated to increase anonymity. Second, she can act as an honest node who keeps the message secret and who creates the dummy traffic. Third, she can act as a dishonest node by eavesdropping on traffic and not participating in forwarding or generating the dummy traffic. Finally, she can avoid sending her traffic through an anonymous network. For each of the above actions, the authors define various benefits and costs and calculate the corresponding payoffs. Moreover, the authors also consider the costs and benefits of reputations.

The model is then applied to mix-nets with a **repeated-game and simultaneous moves**. Acquisti et al. assume the existence of a global passive adversary that can eavesdrop all traffics on all links. The authors also consider the case, where the adversary includes some percentage of the users. The game can aid in understanding the dynamics that might take place when the users decide to join and contribute to the anonymizer networks. The game is then analyzed with **myopic** or **strategic** users, with different equilibria. The authors show that the network can easily collapse under certain conditions; thus they investigate how economic incentives can provide alternative mechanisms.

For example, in order to avoid the problem of *public good with free riding*, the authors suggest a *usage fee* for the network. They also suggest deploying *special* users who consider in their payoffs the social value of having an anonymous network. These special users are paid by other users or the central authority. They also suggest the notion of public ranking and reputation in order to provide incentives for public recognition.

6.3 Trust vs. Privacy

Network nodes need to disclose some private information, in order to establish trust. This causes a tension between security and trust in computer networks. Using a game-theoretic approach, Raya, Shokri, and Hubaux [Raya et al. 2010] study this tradeoff. They model the strategies of rational users that try to establish data-centric trust in the presence of rational adversaries.

Figure 8 illustrates their game model. The two macroplayers are A (attacker) and D (defender) with two possible actions: S (send attributes to the information verifier V) and W (wait until the next stage). When sending, each macroplayer increases the level of trust in its information but the opponent can surpass it in the next stage, thus requiring the first macroplayer to disclose even more attributes in the subsequent stage. The winner has to provide a trust level at least equal to a defined threshold, θ. Let c be the privacy loss required to reach θ. Hence, each macroplayer is required to invest at least an amount c of privacy to win the game.

v_A represents how much the attacker benefits from a successful attack, whereas v_D represents the cost that the defender avoids by preventing the attack.

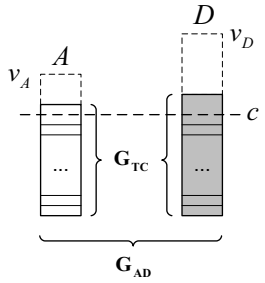

Fig. 8. Duality between the trust-privacy games. The game (G_{AD}) is between the two groups A and D, whereas G_{TC} determines how microplayers in each group contribute to G_{AD}. The winner of the game is indicated by the shaded rectangle (note that D reaches a higher level of trust, by revealing more private information, than A). The dotted rectangles represent the gains v_A and v_D of the macroplayers in the case of winning the game. c is the minimum amount of privacy required to reach the threshold trust θ.

The authors first prove that the strategy (W, WW) is a Perfect Bayesian Equilibrium (PBE) of the game. This means that D's best strategy is to play always W and A's best-response strategy is to play W regardless of whether D plays W or S. In practice, both macroplayers wait until the last stage where they rely on their respective probabilities of access to win. This means that the information verifier can decide on the information only at the deadline, which is not desirable. Accordingly, the authors prove that incentives can enable trust establishment and reduce the amount of disclosed privacy. They analyze the game with incentives and show that the resulting equilibrium is not constrained to waiting. They also analyze this tradeoff for the example of revocation (See Section 4.2) and show that no misbehaving nodes will be revoked by a voting mechanism unless there are enough incentives for revocation.

6.4 Miscellaneous

More recently, Zhang et. al [Zhang et al. 2010a] address the problem of defending against entry-exit linking attacks in Tor (The Onion Routing) network using a game-theoretic approach. They formalize the problem as a repeated non-cooperative game between the defender and the adversary. They extract three design principles, namely stratified path selection, bandwidth order selection, and adaptive exit selection, by using the results of the game between attacker and defender. Using these results, they develop gPath, a path selection algorithm that integrates all three principles to significantly reduce the success probability of linking attacks in the Tor network.

In [Kantarcioglu et al. 2010], the authors address the question of when firms invest in privacy preserving technologies, considering the customer's valuation of

his private information and the customer's profitability to the firm. They view the firms' evaluation processes as a variant of **Stackelberg leader-follower game** with the customer being the leader. They identify several cases where the government intervention might be required in order that firms invest in privacy-preserving technologies.

6.5 Discussion

All the problems discussed in this section are related to the economics of privacy. For example, the cost of pseudonym change in [Freudiger et al. 2009; Humbert et al. 2010] and the cost of cooperation in [Acquisti et al. 2003] are considered to model the economics of privacy with a game-theoretic approach. Interested readers can find more information about the economics of privacy in [Acquisti 2004; Odlyzko 2003; Varian 2009; Hui and Png 2006].

In all these models, **incomplete information game** framework is adopted, because it captures more accurately the fact that agents have limited knowledge in privacy problems. The authors analyze the equilibrium of the defined games and some design protocols based on their equilibrium analysis (e.g., in [Freudiger et al. 2009]). In [Acquisti et al. 2003], the model does not provide a specific solution (mechanism design) for providing anonymity, but the game-theoretic analysis suggests which parameters should be taken into account when such networks are designed. How to implement incentives in privacy-preserving protocols remains an open question.

The literature generally assumes a complete knowledge of some parameters, such as the cost of pseudonym as in [Freudiger et al. 2009; Humbert et al. 2010] or the cost of acting as honest or dishonest nodes as in [Acquisti et al. 2003]. We believe that it is a reasonable abstraction, but can be refined for specific scenarios.

7. ECONOMICS OF NETWORK SECURITY

Information security breaches pose a significant and increasing threat to national security and economic well-being. Security mechanisms or policies at many levels are crucial to the day-to-day operations and management of different businesses. In this section, we discuss the network security from an economics perspective. We first review the game-theoretical approach to security investment problems among interdependent firms and network users. In the second part, we focus our discussion on security management and policies, and review game-theoretical approaches to the vulnerability disclosure and patch management problems in software.

7.1 Interdependent Security

Security can be viewed as a social good. Everyone benefits when the network provides a strong security and everyone suffers if the security is breached and the network is compromised. However, the social well-being depends on the collective behavior of nodes in the network. The concept of security interdependence is depicted in Figure 9.

The interdependence of security was first studied in [Kunreuther and Heal 2003] by addressing the question of whether firms have adequate incentives to invest in protection against a risk whose magnitude depends on the actions of others. Their

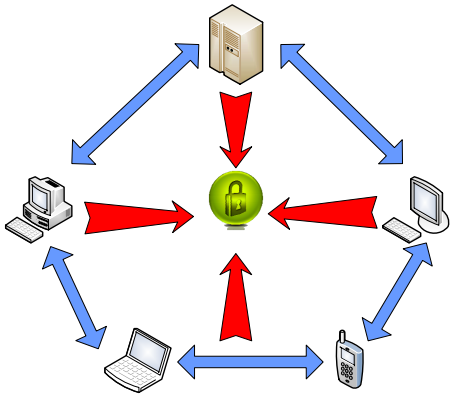

Fig. 9. Security interdependence in a computer network. Every agent in the network contributes to the social security of the network. The security of the entire network depends on the well-being of individuals.

paper characterizes the Nash equilibria for the interdependent security problem and examines the roles of insurance, liability, fines and subsidies, third party inspections, regulations and coordinating mechanisms for internalizing the negative externalities characteristic of the problem.

In [Grossklags and Johnson 2009; Grossklags et al. 2008], the authors consider different security game paradigms by studying the impact of individual security investment decisions on the entire Internet population. Each player chooses an insurance level and a protection level. In a total effort security game, an individual's utility depends on the average protection level of the network. Such a paradigm models the situation where an attacker needs to conquer the majority of the machines in the network one-by-one to succeed in its attack goal. In a weakest-link security game, the utility of a node depends on the minimum protection level among all individuals in the network. It describes a scenario where once the perimeter of an organization is breached, an attacker can leverage it as an advantage to compromise the entire network as a result of an inconsistent security policy, or infiltrating malicious codes.

In various computer security settings, such as when customers use the same password at several independent web sites, security decisions made by one organization may have a significant impact on the security of another. The incentive of individual organizations in security investment is often not aligned with the socially appropriate levels of security investment.

In [Miura-Ko et al. 2008], the authors use game-theoretic models of linear interaction networks to address the interdependent nature of security investment decisions. They provide an analysis of equilibria found in several security settings, thus enabling qualitative observations about the nature of incentives within the models including the concept of free-riding. In [Miura-Ko et al. 2008], the authors develop a model for security decision-making in interdependent organizations described by a linear influence network. An algorithm is determined to iteratively improve the equilibrium in a manner such that two nodes decrease their investments and all

other nodes continue to invest the same amount.

The linear interdependency model is further applied to describe the relationship between security assets as well as vulnerabilities in [Nguyen et al. 2009]. The term *security asset* refers to a node in a complex and interconnected system that plays a security-related role. A network of security assets can be modeled as a weighted directed graph where nodes represent different assets and edges the influence among the nodes. The interdependencies between security vulnerabilities in a network can also be modeled by a linear influence network. For example, in a corporate network, if a workstation is compromised, the data stored in this computer can be exploited in attacks against other workstations; these latter computers will thus become more vulnerable to intrusion.

In [Lelarge and Bolot 2008], the authors study a network of interconnected agents subject to epidemic risks such as viruses and worms where agents can decide whether or not to invest in the deployment of security solutions. An epidemic propagation model, together with an economic model, is proposed to capture network effects and externalities. The authors use local mean field approximation to show that the equilibrium under a strong or weak protection is not socially optimal. On the one hand, when all agents invest in self-protection, the incentive for self-interested agents to invest in self-protection is low and hence leads to the free-ride problem, resulting in an under-protected network. On the other hand, when no agents invest in self-protection, a small fraction of security-investing agents is not sufficient for the benefit of network security, hence leading again to an under-protected network. The mean-field model helps to explain the facts observed in the Internet, where under-investment in security solutions has long been considered an issue. The authors also show that insurance is a very effective mechanism and argue that using insurance would increase the security in a network such as the Internet [Bolot and Lelarge 2008].

7.2 Information Security Management

Information security management decisions are high-level policies that ensure the operation of information systems. In [Cavusoglu et al. 2008], the authors consider a patch management problem in which a vendor needs to determine how to release patches to fix vulnerabilities in its software and a firm needs to decide how to update vulnerable systems with available patches. In their paper, a game-theoretical approach is used to study the strategic interaction between a vendor and a firm by balancing the costs and benefits of patch management. Cavusoglu et al. show that a time-driven release by the vendor and a time-driven update by the firm is the equilibrium outcome under realistic settings in the decentralized system. In a centralized system, the socially optimal time-driven patch management requires synchronization of patch release and update cycles. In their paper, the analysis shows that vendors are better off by releasing periodically instead of releasing them as soon they become available.

In [August and Tunca 2006], the authors study the effect of user incentives on software security in a network of individual users under costly patching and negative network security externalities. The authors compare four alternative policies to manage network security. They conclude that, for proprietary software, when software security risk and the patching costs are high, for both a welfare-maximizing

social planner and a profit-maximizing vender, the policy that offers rebates to patching customers is a dominant strategy. For freeware, a usage tax is the most effective policy, except when both patching costs and security risk are low. Optimal patching rebates and taxes tend to increase with increased security risk and patching costs but they can decrease in the security risk for high-risk levels.

The management of information security involves a series of policy-making decisions on the vulnerability discovery, disclosure, patch development and patching. In [Zhu et al. 2011], the authors propose a systematic approach to tackle the management of control system information security by compartmentalizing these decision processes into multiple input-output blocks. Specifically, they establish a theoretical framework for making patching decisions for control systems, taking into account their functionability requirement and the risks of potential threats from patching delays. In the game-theoretic model, the system manager decides on the operation period of the plant, whereas the attacker chooses the attack rate on the critical infrastructure.

7.3 Discussions

Economics of security is an important subject that studies incentives behind actions and their economic consequences in the security domain. Game theory, already widely used in economics, opens promising new directions in this rapidly growing field of research. In this section, we have discussed security games in computer networks and communications from an economics perspective. First, we have addressed the central idea of interdependent security in networks, which has spawned a recent interest on studying games such as security investment, security insurance and security asset protection.

In the second part, we have reviewed literature on information security management, which involves a higher level decision-making on the support and maintenance of information systems. We find that it is important for the discussions from an economics perspective to relate closely to the fast evolving security technology. We advocate an integrative thinking that interconnects security economics with software engineering, intellectual property law, social behaviors and business so that we can have a comprehensive view towards security and its impact on different fields. In the literature, we find that there are more economics models to understand the user behavior than the ones to understand the attackers' incentives. An economic model that integrates both sides of the security may lead to a more comprehensive and insightful understanding of security and associated defense strategies.

8. GAME THEORY MEETS CRYPTOGRAPHY

Game theory and cryptography both deal with the interaction between mutually distrusted parties. In this section, we address how game theory can be applied to cryptography and *vice versa*. Note that cryptography is a vast subject and we only focus on the problem of *multi-party computation* (MPC) in this field [Dodis and Rabin 2007]. In such computations, game theory can help parties perform certain protocols. MPC also can help parties in the game to achieve a certain equilibrium. For an additional discussion on game theory and cryptography, we refer to [Katz 2008].

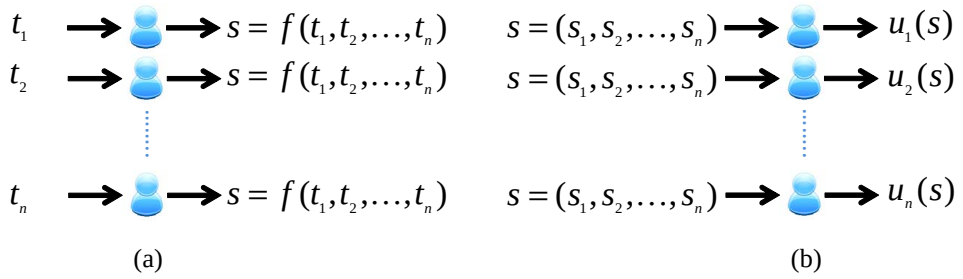

Fig. 10. A comparison between Multi-Party Computation and Game Theory. (a) In MPC n parties wish to compute together a function s, (b) whereas in game theory n parties calculate individual payoffs given the strategies of other parties.

As it is shown in Figure 10, in MPC there are n parties that want to compute a function collectively, with each one operating without knowledge about the inputs of the other parties, i.e. party P_i only knows the input t_i. This is in contrast to a complete information game, where the n parties know the strategies of each other (or can compute them) and, given the strategy profile $s = (s_1, s_2, \cdots, s_n)$, each party calculates its individual payoff. The parties in a game-theoretic framework are assumed to be rational and wish to maximize their payoffs. They are also content with being at equilibria, where no one can increase their payoff by unilaterally deviating from its strategy.

In MPC, it is assumed that some parties are honest and follow the protocol, but others are malicious. This means that some parties behave in an irrational manner, whereas game theory is built on *incentives* and assumes the *rationality* of players. *Privacy* is a goal for MPC, and having a *mediator* in games (who obtains private information) helps parties to choose the best equilibrium. With game theory we can *punish* malicious parties, but with MPC we have to resist against a certain number of malicious parties [Dodis and Rabin 2007].

Given the above dispositions of MPC and game theory, there are two research directions that are investigated [Katz 2008]. Some researchers analyze how cryptography can be applied to game theory. In fact, certain game-theoretic equilibria can be achieved if a trusted mediator is available. They analyze how this mediator can be replaced by a distributed cryptographic protocol. This protocol can be run by the parties [Dodis et al. 2000].

Some researchers focus on how game theory can be applied to cryptography [Abraham et al. 2006; Gordon and Katz 2006; Halpern and Teague 2004; Lysyanskaya and Triandopoulos 2006]. In fact, game theory can help us to model and design a meaningful protocol for honest as well as malicious parties, assuming that all parties are rational and self-interested. In the following two subsections we address some of the results in these two fields.

8.1 Cryptographic Mediator

In [Dodis et al. 2000], the authors address the problem of implementing a mediator in game theory. The mediator is designed using a cryptographic approach. This mediator can potentially lead the game to a preferable correlated equilibrium. A

similar idea was already investigated in the economics community, with a technique called **cheap talk** [Abraham et al. 2008]. This means that the parties can communicate amongst themselves to find and play the correlated equilibrium in advance.

In this protocol, the parties are supposed to play first a **cheap talk** extension of the game, named G_{CT}. Assume that σ is an efficient strategy profile in G_{CT}. Dodis et al. first prove that σ is a t-resilient[5] implementation of the correlated equilibrium of the game G under certain conditions. In other words, σ should be t-resilient equilibrium in G_{CT}. Moreover, the value of payoff at σ should be equal to the payoff at the correlated equilibrium.

If the parties are able to perform a completely fair and secure multi-party computation, then any correlated equilibrium of the game has a t-resilient implementation. Hence, the parties can run a completely fair protocol during the **cheap talk game** (G_{CT}). Then, each party plays the action that it received from the output of the protocol.

When a complete fair and secure multi-party computation does not exist, the authors focus on the 2-player scenario where the protocol of the **cheap talk game** is not fair [Dodis et al. 2000]. They show that if the party, who has not received the output of the protocol, plays the *minimax* profile against the other party, they can obtain a 1-resilient implementation of the correlated equilibrium.

The idea of playing *minimax* cannot easily be extended for a scenario with more players. Hence, in [Abraham et al. 2006] the authors define a stronger notion of *t-punishment* strategy with respect to correlated equilibrium of the game. In [Abraham et al. 2006; Abraham et al. 2008], the authors prove that if a *t-punishment* strategy is available for a given correlated equilibrium, then this gives hope that a variant of the above approach can be used to implement a t-resilient of the correlated equilibrium. In summary, the above examples show how a MPC protocol could help the players to find and implement a preferable correlated equilibrium. However, we need to further characterize when a correlated equilibrium can be implemented in the presence of a partially fair protocol.

8.2 Rationality in MPC

Let us consider the problem of secret sharing in MPC, where a secret can be revealed only by m parties out of n available parties. For example, Figure 11 shows how a secret S can be calculated by each party if and only if they have received the secret share of each of the two other parties.

The idea underlying this protocol is that the maximum number of bad parties is $n - m$, such that the rest of the nodes are still able to calculate the share. But it makes more sense to consider that the parties are rational and they cooperate if it is in their interest to share a part of the secret. This idea is first presented in [Halpern and Teague 2004]. They assume that each party has its preferences and decides to follow the protocol only if it increases its payoff. Given the rationality assumption, they first prove that rational parties will not broadcast their shares.

[5]A strategy vector is a t-resilient equilibrium, if for any set of coalitions among C players where $|C| \leq t$, no member of the coalition improves its situation no matter how the members of C coordinate their actions. Note that 1-resilient equilibrium is a Nash equilibrium.

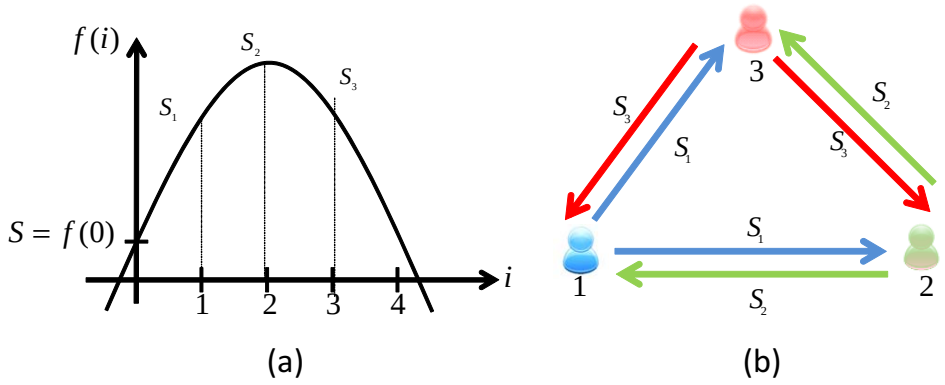

Fig. 11. A secret sharing protocol between 3 parties. (a) $S = f(0)$ is the secret and each S_i is calculated using a polynomial function. (b) Each party should receive the other two secret shares to calculate the secret.

In fact, they assume that each party prefers obtaining the secret and that the fewer of the other parties get it as well. Given these preferences, it is easy to see that *not sending the share* is a weakly dominating strategy in the game between the parties. Note that these results make sense, if we consider that the parties have common knowledge about the running time of the protocol. This is similar to the results of the finite **repeated prisoner-dilemma game** that always ends in the all defect strategy profile. Halpern and Teague also prove that the parties do not broadcast their shares, even if there is a trusted party.

Hence, the authors define a random-length protocol that can guarantee the participation of parties in the secret sharing protocol, with or without a trusted party. The main idea is to add a randomized secret reconstruction protocol to the end of multi-party computational protocol defined in [Goldreich et al. 1987]. To explain how their protocol works, let us again consider the example of three parties in Figure 11. Each party can toss a fair coin and be forced to reveal the outcome. The party then sends its share if the toss is *heads* otherwise it would be removed from the protocol and nobody will cooperate with him. Party i will not send its share if 2/3 of the agents' tosses are *heads*. If there are more than 3 players, we can divide the parties into 3 groups and each group leader collects some of the group's shares with the same protocol.

The main idea behind this protocol is the iterated deletion. This means that the protocol will be at Nash equilibrium, and must survive iterated deletion weakly dominated strategies. The protocol continues until there is no more weakly dominated strategies.

Concurrently and independently of each other, Lysyanskaya and Triandopoulos [Lysyanskaya and Triandopoulos 2006], Gordon and Katz [Gordon and Katz 2006], and Abraham et al. [Abraham et al. 2006] investigated the same problem and proposed several MPC protocols.

Contrary to the claim by Halpern and Teague [Halpern and Teague 2004] that a solution is impossible for 2 players, Gordon and Katz [Gordon and Katz 2006] and

Abraham et al. [Abraham et al. 2006] design similar protocols for rational secret sharing among 2 players. Gordon and Katz also extend the protocol to more than 2 players, where it is simpler than the Halpern and Teague solution. They also show how to avoid, in these protocols, the continual involvement of the dealer.

Moreover, Abraham et al. consider that the agents can form coalitions. They define an equilibrium to be k-resilient if it tolerates deviations by coalitions of a size up to k out of n players. They show that such a k-resilient Nash equilibrium exist for secret sharing, provided that players prefer to get the information rather than not get it [Abraham et al. 2006].

In [Lysyanskaya and Triandopoulos 2006], the authors study the same problem with a mixed-behavior model, where none of the n participating parties are honest. In their model the agents are either rational, acting in their selfish interest to maximize their utility, or adversarial, acting arbitrarily. They define a class of functions that can be computed in the presence of an adversary using a trusted mediator. They also propose a protocol that allows the rational parties to emulate the mediator and jointly compute the function. In their protocol the rational parties are protected from a malicious adversary that controls $\lceil \frac{n}{2} \rceil - 2$ of the participants.

All of the above protocols require simultaneous channels and assume that in any given round players do not know whether the current round is going to be the last round, or whether this is a just a test round designed to catch cheaters. In [Kol and Naor 2008], they suggest a coalition-resilient secret sharing and secure multi-party computation (SMPC) protocols with the property that after any sequence of iterations it is still a computational best response to follow them. Therefore, the protocols can run any number of iterations, and are immune to backward induction.

8.3 Discussions

In this section, we have addressed how game theory can help cryptography and vice versa. In the first part, we have addressed how the **cheap talk game** can help to implement a mediator and players can obtain better payoffs in the game. Moreover, they used the minmax and punishment techniques to obtain better equilibrium.

In Section 8.2, we have discussed how game theory can help MPC protocols. In [Halpern and Teague 2004], the authors analyze the interaction between agents by using **repeated games** and concluded that the protocol cannot work and the agents will not share the secrets. This analysis helps them to define new secure protocols to share the secrets. Furthermore, the authors in [Lysyanskaya and Triandopoulos 2006; Gordon and Katz 2006; Abraham et al. 2006; Kol and Naor 2008] define several new protocols that provide secure MPC for the same problem.

9. SUMMARY, OPEN QUESTIONS, AND FUTURE RESEARCH DIRECTIONS

Game theory has become one of the analytical tools that helps researchers design security protocols in computer networks. It can be used as a rich mathematical tool to analyze and model new security problems. Moreover, through the equilibrium analysis of the security game, the defender can gain a deeper understanding of the attacker's strategies, as well as the potential attack risks.

In this survey, we have presented an overview of security and privacy problems that are addressed and analyzed within a game-theoretic framework. We have reviewed and compared existing security games in computer networks in terms of players, game models, game-theoretic approaches, and equilibrium analysis. We have also discussed some security protocols that are developed by mechanism design. The general objective is to identify and address the security and privacy problems, where game theory can be applied to model and evaluate security problems and consequently used to design efficient protocols.

One of the criticisms of game theory, as applied to modeling decision-makers, is that agents are rarely fully rational. Moreover, they do not have complete information about each others' payoffs and strategy choices. Therefore, modeling the decision process by means of a few equations and parameters is questionable. In particular, we must consider *information limitations* and *learning aspects* of decision-makers in network security problems. This means that special care must be devoted to the assessment of the degree and accuracy of the information that each player can obtain. As we have discussed in this paper, the application of game theory with incomplete and imperfect information is an emerging field in network security and privacy, with only a few papers published so far (e.g., non-cooperative location privacy in Section 6.1). Moreover, agents need to correctly estimate the security game parameters. In fact, observation capabilities provide the necessary basis for attack prevention and security measures. But the observation and detection, in the context of network security, cannot be done manually by human beings and require computer assistance. *Machine (or statistical) learning* can provide a scalable and decentralized framework for detection, analysis, and decision-making in network security. In addition, recent advances in cloud computing, multiprocessor systems, and multicore processors, make *distributed machine learning* an important research field relevant to not only the security domain but also to many other domains.

Apart from the above criticism, one of the main problems with modeling network security from the defense perspective is the lack of motivation that partly stems from the difficulty of *quantifying* the value added by network security. There is much confusion on how to assess and quantify network security. This lack of quantification naturally affects the decision making process regarding security investments. Hence, the attitudes towards security seem to go back and forth between "*we are doomed if we don't invest heavily in security*" and "*no need to worry too much, it all seems fine*" depending on the economic situation. This shows that quantifying security-related concepts such as trust, privacy, and risk in game-theoretic models deserves particular attention. In summary, much research is still needed in *information limitations*, *learning aspects*, and *quantifying* security parameters, in particular to better capture the perception that each of the security decision-makers has of the security games in which he plays.

In wireless networks, the users (or the device manufacturer, or the network operator, if any) program their devices to follow a protocol (i.e., a strategy) and it is reasonable to assume that they rarely reprogram their devices. Hence, such a device can be modeled as a rational decision maker. From this point of view, the application of game theory in security of wireless networks is easier to justify than,

say, in economics, where the players are human beings. However, *mobility* and *computational complexity* should be taken into account for security games in these contexts. First, in highly mobile scenarios, the players have a very short time for interaction. Moreover, even if all the necessary information is available, computing the Nash equilibrium can be very complex and thus beyond the capabilities of low-tier wireless devices.

Mechanism design will also play a particular role in designing efficient security protocols in computer networks [Micali and Valiant 2008; Rehák et al. 2005]. In fact, *mechanism design* is concerned with the question of how to lead decision-makers to a desirable equilibrium by changing (designing) some parameters (incentives) of the game. This can also prevent the *free riding* effects in the designed protocols.

Most of the current works on network security focuses on system models and their equilibrium analysis. This is an initial step towards a quantitative study on security and privacy. As pointed out in the discussion sections, algorithms and implementations are often less discussed. One reason is that algorithmic issues can be studied separately, once the game models are determined. Many existing algorithms can be used to find the equilibrium offline given the system parameters [Zhu et al. 2010a; 2011].

However, the challenges lie in the implementation of on-line algorithms in network security. In some of our reviewed works, such as [Zhu and Başar 2009; Zhu et al. 2009; Liu et al. 2006], there is an explicit study of learning algorithms in the context of network security. We believe that algorithmic and learning in security games represents a new direction for future research in this area.

Last but not least, we witness an increasing number of applications of game theory for security problems at the network layer and application layer, e.g., [Zhang et al. 2010b; Yu and Liu 2007; Liu et al. 2005; Zhu et al. 2009; Zhu et al. 2010b; Chen and Leneutre 2009; Vratonjic et al. 2010; Vratonjic et al. 2010]. Security at network layer imposes future challenges for us to address security at a larger and more complex scale and game theory provides a versatile tool that enables a quantitative study of such complex systems. Finally, by applying game-theoretic approaches in [Vratonjic et al. 2010] the authors show that we can analyze security problems at the application layer, considering the business model of the Internet.

REFERENCES

Abraham, I., Dolev, D., Gonen, R., and Halpern, J. 2006. Distributed Computing meets Game Theory: Robust Mechanisms for Rational Secret Sharing and Multiparty Computation. In *Proc. of the 25th ACM Annual Symposium on Principles of Distributed Computing (PODC)*. 53–62.

Abraham, I., Dolev, D., and Halpern, J. 2008. Lower Bounds on Implementing Robust and Resilient Mediators. *Theory of Cryptography, Springer*, 302–319.

Acquisti, A. 2004. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce (EC)*. 21–29.

Acquisti, A., Dingledine, R., and Syverson, P. 2003. On the Economics of Anonymity. *Financial Cryptography (FC)*, 439–443.

Afanasyev, M., Chen, T., Voelker, G., and Snoeren, A. 2008. Analysis of a Mixed-use Urban WiFi Network: when Metropolitan becomes Neapolitan. In *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement*. 85–98.

Alpcan, T. and Başar, T. 2003. A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection. In *Proceedings of the 42nd IEEE Conference on Decision and Control (CDC)*.

Alpcan, T. and Başar, T. 2004. A Game Theoretic Analysis of Intrusion Detection in Access Control Systems. In *Proceedings of the 43rd IEEE Conference on Decision and Control (CDC)*.

Alpcan, T. and Başar, T. 2006. An Intrusion Detection Game with Limited Observations. In *Proceedings of the 12th International Symposium on Dynamic Games and Applications*.

Alpcan, T. and Başar, T. 2011. *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press.

Altman, E., Avrachenkov, K., and Garnaev, A. 2009. Jamming in Wireless Networks: the Case of Several Jammers. In *Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets)*.

Anderson, R. and Moore, T. 2006. The Economics of Information Security. *Science 314,* 5799, 610.

Apt, K. and Witzel, A. 2006. A Generic Approach to Coalition Formation. In *Proceedings of the International Workshop on Computational Social Choice (COMSOC)*.

Årnes, A., Sallhammar, K., Haslum, K., Brekne, T., Moe, M., and Knapskog, S. 2006. Real-time Risk Assessment with Network Sensors and Intrusion Detection Systems. *Computational Intelligence and Security*, 388–397.

August, T. and Tunca, T. 2006. Network Software Security and User Incentives. *Management Science 52,* 11 (November), 1703–1720.

Başar, T. 1983. The Gaussian Test Channel with an Intelligent Jammer. *IEEE Transactions on Information Theory 29,* 1, 152–157.

Başar, T. and Olsder, G. J. 1999. *Dynamic Noncooperative Game Theory*, 2nd ed. SIAM.

Bilogrevic, I., Manshaei, M. H., Raya, M., and Hubaux, J.-P. 2010. Optimal Revocations in Ephemeral Networks: A Game-Theoretic Framework. In *Proceedings of International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*.

Bohme, R. and Moore, T. 2009. The Iterated Weakest Link: A Model of Adaptive Security Investment. In *Proceedings of Workshop on the Economics of Information Security (WEIS)*.

Bohme, R. and Schwartz, G. 2010. Modeling Cyber-Insurance: Towards A Unifying Framework. In *Proceedings of the Workshop on the Economics of Information Security (WEIS)*.

Bolot, J. and Lelarge, M. 2008. Cyber Insurance as an Incentive for Internet Security. In *Proceedings of the Workshop on Economics of Information Security (WEIS)*.

Borden, J. M., Mason, D. M., and McEliece, R. J. 1985. Some Information Theoretic Saddlepoints. *SIAM Journal of Control and Optimization 23,* 1, 129–143.

Boutaba, R. and Aib, I. 2007. Policy-Based Management: A Historical Perspective. *Journal of Network and Systems Management 15,* 4, 447–480.

Braun, C. and Schifferle, S. 2005. BlueDating - Dating Application for Bluetooth Enabled Mobile Phones. Tech. Rep. ETH Zurich, TIK-SA-2005.08.

Bretscher, K. 2005. BlueLocation. Tech. Rep. ETH Zurich, TIK-SA-2005-17.

Bro. 2010. *Bro Intrusion Detection System Users Manual available at http://www.bro-ids.org.*

Buchegger, S. and Alpcan, T. 2008. Security Games for Vehicular Networks. In *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*. 244–251.

Buttyan, L. and Hubaux, J.-P. 2008. *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*. Cambridge University Press.

C. Duma, M. Karresand, N. S. and Caronni, G. 2006. A Trustaware p2p-based Overlay for Intrusion Detection. In *Proceedings of DEXA Workshops*.

Camp, L. J. 2006. Economics of information security. *Economics*.

Campos, L. 1989. Fuzzy Linear Programming Models to Solve Fuzzy Matrix Games. *Fuzzy Sets System 32,* 3, 275–289.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2008. Security Patch Management: Share the Burden or Share the Damage. *Management Science 54,* 4 (April), 657–670.

Chan, H., Gligor, V. D., Perrig, A., and Muralidharan, G. 2005. On the Distribution and Revocation of Cryptographic Keys in Sensor Networks. *IEEE Transactions on Dependable and Secure Computing 2,* 3, 233–247.

Chaum, D. 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM 24,* 2.

Chen, L. and Leneutre, J. 2009. A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks. *IEEE Transactions on Information Forensics and Security 4,* 2, 165–178.

Chen, R., Park, J., and Reed, J. 2008. Defense Against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications 26,* 1, 25–37.

Csiszar, I. and Korner, J. 1978. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory 54*, 2470–2492.

Debar, H., Dacier, M., and Wespi, A. 2005. Towards a Taxonomy of Intrusion Detection Systems. *Computer Networks 31,* 8, 805–822.

Dodis, Y., Halevi, S., and Rabin, T. 2000. A Cryptographic Solution to a Game Theoretic Problem. In *Advances in Cryptology, CRYPTO 2000*. Springer, 112–130.

Dodis, Y. and Rabin, T. 2007. Cryptography and Game Theory. *Algorithmic Game Theory*, 181–209.

Douceur, J. 2002. The Sybil Attack. *Peer-to-Peer Systems*, 251–260.

Ephremides, A. and Wieselthier, J. E. 1987. A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling. *Proceedings of the IEEE 75*, 56–73.

Fall, K. 2003. A Delay-tolerant Network Architecture for Challenged Internets. In *Applications, Technologies, Architectures, and Protocols for Computer Communications*. ACM, 34.

Freudiger, J., Manshaei, M. H., Hubaux, J.-P., and Parkes, D. C. 2009. On Non-cooperative Location Privacy: A Game-Theoretic Analysis. In *Proceedings of ACM Conference on Computer and Communications Security (CCS)*.

Fudenberg, D. and Tirole, J. 1991. *Game Theory*. MIT Press.

Fung, C., Baysal, O., Zhang, J., Aib, I., and Boutaba, R. 2008. Trust Management for Host-based Collaborative Intrusion Detection. In *Proceedings of 19th IFIP/IEEE International Workshop on Distributed Systems*.

Fung, C., Zhang, J., Aib, I., and Boutaba, R. 2009. Robust and Scalable Trust Management for Collaborative Intrusion Detection. In *Proceedings of 11th IFIP/IEEE International Symposium on Integrated Network Management (IM)*.

Garagic, D. and Cruz, J. 2003. An Approach to Fuzzy Noncooperative Nash Games. *Journal of Optimization Theory and Applications 118,* 3, 475–491.

Gibbons, R. 1992. *A Primer in Game Theory*. Prentice Hall.

Goldreich, O., Micali, S., and Wigderson, A. 1987. How to Play any Mental Game. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*. 218–229.

Gordon, S. and Katz, J. 2006. Rational Secret Sharing, Revisited. *Security and Cryptography for Networks*, 229–241.

Grossklags, J., Christin, N., and Chuang, J. 2008. Secure or Insure?: A Game-Theoretic Analysis of Information Security Games. In *Proceedings of the 17th ACM International Conference on World Wide Web (WWW)*. 209–218.

Grossklags, J. and Johnson, B. 2009. Uncertainty in the Weakest-link Security Game. In *Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets)*. 673–682.

Halpern, J. and Teague, V. 2004. Rational Secret Sharing and Multiparty Computation. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*. 632.

Han, Z., Marina, N., Debbah, M., and Hjørungnes, A. 2009. Physical Layer Security Game: How to Date a Girl with Her Boyfriend on the Same Table. In *Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets)*.

Hatt, N. 2005. BlueFramework - Application Framework for Bluetooth Enabled Mobile Phones. Tech. Rep. ETH Zurich, TIK-MA-2005-16.

Haykin, S. 2005. Cognitive Radio: Brain-Empowered Wireless Communications. *IEEE Journal on Selected Areas in Communications (JSAC) 23,* 2 (February).

Hossain, E., Niyato, D., and Han, Z. 2009. Dynamic Spectrum Access in Cognitive Radio Networks. *Cambridge University Press*.

Hui, K. L. and Png, I. 2006. The Economics of Privacy. *Economics and information systems*, 471.

Humbert, M., Manshaei, M. H., Freudiger, J., and Hubaux, J.-P. 2010. Tracking Games in Mobile Networks. In *Proceedings of the 1st Conference on Decision and Game Theory for Security (GameSec)*. LNCS.

Kantarcioglu, M., Bensoussan, A., and Hoe, C. 2010. When Do Firms Invest in Privacy-Preserving Technologies? In *Proceedings of the 1st Conference on Decision and Game Theory for Security (GameSec)*. LNCS.

Kashyap, A., Başar, T., and Srikant, R. 2004. Correlated Jamming on MIMO Gaussian Fading Channels. *IEEE Transactions on Information Theory 50,* 9, 2119–2123.

Katz, J. 2008. Bridging Game Theory and Cryptography: Recent Results and Future Directions. *Lecture Notes in Computer Science 4948*, 251.

Keppler, J. and Mountford, H. 1999. Handbook of Incentive Measures for Biodiversity: Design and Implementation. In *Organisation for Economic Co-operation and Development (OECD)*.

Kol, G. and Naor, M. 2008. Cryptography and Game Theory: Designing Protocols for Exchanging Information. *Lecture Notes in Computer Science 4948*, 320.

Krishna, V. 2002. *Auction Theory*, 1st ed. Academic Press.

Kunreuther, H. and Heal, G. 2003. Interdependent Security. *Journal of Risk and Uncertainty 26,* 2 (March), 231–249.

Lelarge, M. and Bolot, J. 2008. A Local Mean Field Analysis of Security Investments in Networks. In *Proceedings of the 3rd ACM International Workshop on Economics of Networked Systems (NETECON)*.

Leung-Yan-Cheong, S. K. and Hellman, M. E. 1978. The Gaussian Wiretap Channel. *IEEE Transactions on Information Theory 24*, 451–456.

Liu, P., Zang, W., and Yu, M. 2005. Incentive-based Modeling and Inference of Attacker Intent, Objectives, and Strategies. *ACM Transactions on Information System and Security 8,* 1, 78–118.

Liu, Y., Comaniciu, C., and Man, H. 2006. A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks. In *Proceedings of Workshop on Game Theory for Communications and Networks (GameNets)*.

Lye, K. and Wing, J. M. 2002. Game Strategies in Network Security. In *Proceedings of IEEE Computer Security Foundations Workshop (CSFW)*.

Lysyanskaya, A. and Triandopoulos, N. 2006. Rationality and Adversarial Behavior in Multiparty Computation. *Advances in Cryptology-CRYPTO*, 180–197.

Ma, R., Lee, S., Lui, J., and Yau, D. 2004. A Game Theoretic Approach to Provide Incentive and Service Differentiation in P2P Networks. *ACM SIGMETRICS Performance Evaluation Review 32,* 1, 189–198.

Mallik, R., Scholtz, R., and Papavassilopoulos, G. 2000. Analysis of an On-off Jamming Situation as a Dynamic Game. *IEEE Transaction on Communications 48,* 8 (August), 1360–1373.

Medard, M. 1997. Capacity of Correlated Jamming Channels. In *Proceedings of the 35th Allerton Conference on Communication, Control, and Computing*. 1043–1052.

Micali, S. and Valiant, P. 2008. Revenue in Truly Combinatorial Auctions and Adversarial Mechanism Design. Tech. Rep. MIT, MIT-CSAIL-TR-2008-039.

Michiardi, P. and Molva, R. 2002. Game Theoretic Analysis of Security in Mobile Ad Hoc Networks. *Research Report RR-02-070, Institut Eurecom, Sophia-Antipolis*.

Miura-Ko, A., Yolken, B., Bambos, N., and Mitchell, J. 2008. Security Investment Games of Interdependent Organizations. In *Proceedings of the Allerton Conference on Communication, Control, and Computing*.

Miura-Ko, R., Yolken, B., Mitchell, J., and Bambos, N. 2008. Security Decision-Making among Interdependent Organizations. In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF)*. 66–80.

Moore, T., Clulow, J., Nagaraja, S., and Anderson, R. 2007. New Strategies for Revocation in Ad-Hoc Networks. In *Proc. of the European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*.

Mukherjee, A. and Swindlehurst, A. L. 2010. Equilibrium Outcomes of Dynamic Games in MIMO Channels with Active Eavesdroppers. In *Proceedings of IEEE International Conference on Communications (ICC)*.

Nash, J. 1951. Non-cooperative games. *The Annals of Mathematics 54,* 2, 286–295.

Nguyen, K., Alpcan, T., and Başar, T. 2008. Fictitious Play with Imperfect Observations for Network Intrusion Detection. In *Proceedings of the 13th International Symposium Dynamic Games and Applications*.

Nguyen, K. C., Alpcan, T., and Başar, T. 2009. Stochastic Games for Security in Networks with Interdependent Nodes. In *Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets)*.

Nisan, N. 2007. Introduction to Mechanism Design (for Computer Scientists). *Algorithmic Game Theory*, 209–242.

Nisan, N. and Ronen, A. 1999. Algorithmic Mechanism Design. In *Proceedings of the 31 Annual ACM Symposium on Theory of Computing*. 129–140.

Odlyzko, A. 2003. Privacy, economics, and price discrimination on the Internet. In *Proceedings of the 5th ACM International Conference on Electronic Commerce (EC)*. 355–366.

Raghavan, T. E. S. and Filar, J. A. 1991. Algorithms for Stochastic Games – A Survey. *Mathematical Methods of Operations Research 35*, 437–472.

Raya, M. and Hubaux, J.-P. 2005. The Security of Vehicular Ad Hoc Networks. In *Proc. of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks*. 21.

Raya, M., Manshaei, M. H., Felegyhazi, M., and Hubaux, J.-P. 2008. Revocation Games in Ephemeral Networks. In *Proceedings of ACM Conference on Computer and Communications Security (CCS)*.

Raya, M., Shokri, R., and Hubaux, J.-P. 2010. On the Tradeoff between Trust and Privacy in Wireless Ad Hoc Networks. In *Proceedings of ACM Conference on Wireless Network Security (WiSec)*.

Rehák, M., Pěchouček, M., and Tožička, J. 2005. Adversarial Behavior in Multi-agent Systems. *Multi-Agent Systems and Applications IV*, 470–479.

Reidt, S., Srivatsa, M., and Balfe, S. 2009. The Fable of the Bees: Incentivizing Robust Revocation Decision Making in Ad Hoc Networks. In *Proceedings of ACM Conference on Computer and Communications Security (CCS)*.

Saad, W., Han, Z., Başar, T., Debbah, M., and Hjørungnes, A. 2009. Physical Layer Security: Coalitional Games for Distributed Cooperation. In *Proceedings of International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*.

Sagduyu, Y., Berry, R., and Ephremides, A. 2009. MAC Games for Distributed Wireless Network Security with Incomplete Information of Selfish and Malicious User Types. In *Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets)*. 130–139.

Sallhammar, K., Helvik, B., and Knapskog, S. 2006. On Stochastic Modeling for Integrated Security and Dependability Evaluation. *Journal of Networks 1,* 5, 31.

Schaelicke, L., Slabach, T., Moore, B., and Freeland, C. 2003. Characterizing the Performance of Network Intrusion Detection Sensors. In *Recent Advances in Intrusion Detection*. Springer, 155–172.

Semret, N., Liao, R., Campbell, A., and Lazar, A. 2000. Peering and Provisioning of Differentiated Internet Services. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*.

Sen, P., Chaki, N., and Chaki, R. 2008. HIDS: Honesty-Rate Based Collaborative Intrusion Detection System for Mobile Ad-Hoc Networks . In *Proceedings of Computer Information Systems and Industrial Management Applications (CISIM)*. 121–126.

SnortTeam. 2010. *Snort Users Manual available at http://www.snort.org*, 2.8.6 ed.

Sommer, P. 2007. Design and Analysis of Realistic Mobility Model for Wireless Mesh Networks. M.S. thesis, ETH Zurich.

Theodorakopoulos, G. and Baras, J. 2007. Malicious Users in Unstructured Networks. In *Proceedings of the 26th Annual IEEE International Conference on Computer Communications (INFOCOM)*.

Varian, H. 2009. Economic aspects of personal privacy. *Internet Policy and Economics*, 101–109.

Vratonjic, N., Manshaei, M., Raya, M., and Hubaux, J.-P. 2010. ISPs and Ad Networks Against Botnet Ad Fraud. In *Proceedings of Decision and Game Theory for Security (GameSec)*.

Vratonjic, N., Raya, M., Hubaux, J.-P., and Parkes, D. 2010. Security Games in Online Advertising: Can Ads Help Secure the Web? In *Proceedings of Workshop on the Economics of Information Security (WEIS)*.

Wasserman, S. and Faust, K. 1994. *Social Network Analysis: Methods and Applications*. Cambridge Univiversity Press.

Weibel, A. and Winterhalter, L. 2005. Bluetella: File sharing for bluetooth enabled mobile phones. M.S. thesis, Swiss Federal Institute of Technology Zurich (ETHZ).

Wu, Y., Foo, B., Mei, Y., and Bagchi, S. 2003. Collaborative Intrusion Detection System (CIDS): a Framework for Accurate and Efficient IDS. In *Proceedings of 19th Annual Computer Security Applications Conference*. 234–244.

Wyner, A. D. 1975. The Wire-tap Channel. *Bell System Technical Journal*.

Yan, Y., El-Atawy, A., and Al-Shaer, E. 2007. Ranking-based Optimal Resource Allocation in Peer-to-Peer Networks. In *Proceedings of the 26th Annual IEEE International Conference on Computer Communications (INFOCOM)*.

Yegneswaran, V., Barford, P., and Jha, S. 2004. Global Intrusion Detection in the DOMINO Overlay System. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*.

Yu, W. and Liu, K. J. R. 2007. Game Theoretic Analysis of Cooperation Stimulation and Security in Autonomous Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing 6,* 5, 459–473.

Zhang, N., Yu, W., Fu, X., and Das, S. K. 2010a. gPath: A Game-Theoretic Path Selection Algorithm to Protect Tor's Anonymity. In *Proceedings of the 1st Conference on Decision and Game Theory for Security (GameSec)*. LNCS.

Zhang, N., Yu, W., Fu, X., and Das, S. K. 2010b. Maintaining Defender's Reputation in Anomaly Detection Against Insider Attacks. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 40*.

Zhou, C., Karunasekera, S., and Leckie, C. 2005. A Peer-to-Peer Collaborative Intrusion Detection System. In *Proceedings of International Conference on Networks*.

Zhu, Q. and Başar, T. 2009. Dynamic Policy-Based IDS Configuration. In *Proceedings of the 47th IEEE Conference on Decision and Control (CDC)*.

Zhu, Q. and Başar, T. 2011a. Indices of Power in Optimal IDS Default Configuration: Theory and Examples. In *Proc. of 2nd Conference on Decision and Game Theory (GameSec 2011), College Park, MD, USA*.

Zhu, Q. and Başar, T. 2011b. Robust and Resilient Control Design for Cyber-physical Systems with an Application to Power Systems. In *Proc. of 50th IEEE Conference on Decision and Control and European Control Conference, Orlando, Florida*.

Zhu, Q. and Başar, T. 2011c. Towards a Unifying Security Framework for Cyber-Physical Systems. In *Proc. of Workshop on the Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS-11), CPSWeek 2011, Chicago*.

Zhu, Q. and Başar, T. 2012. A Hierarchical Security Architecture for Smart Grid: from Theory to Practice. *In Z. Han, E. Hossain and V. Poor (Eds.), Smart Grid Communications and Networking*.

Zhu, Q., Fung, C., Boutaba, R., and Başar, T. 2009. A Game-Theoretical Approach to Incentive Design in Collaborative Intrusion Detection Networks. In *Proceedings of the International Conference on Game Theory for Networks (GameNets)*. 384–392.

Zhu, Q., Li, H., Han, Z., and Başar, T. 2010. A Stochastic Game Model for Jamming in Multi-Channel Cognitive Radio Systems. In *Proceedings of the IEEE International Conference on Communications (ICC)*.

Zhu, Q., McQueen, M., Rieger, C., and Başar, T. 2011. Management of Control System Information Security: Control System Patch Management. In *Proc. of Workshop on the Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS-11), CPSWeek 2011, Chicago*.

Zhu, Q., Saad, W., Han, Z., Poor, H. V., and Başar, T. 2011. Eavesdropping and Jamming in Next-Generation Wireless Networks: A Game-Theoretic Approach. In *Proceedings of IEEE MILCOM*.

Zhu, Q., Tembine, H., and Başar, T. 2010a. Heterogeneous Learning in Zero-Sum Stochastic Games with Incomplete Information. In *Proceedings of IEEE Conference on Decisions and Control (CDC)*.

Zhu, Q., Tembine, H., and Başar, T. 2010b. Network Security Configuration: A Nonzero-sum Stochastic Game Approach. In *Proceedings of American Control Conference (ACC)*.

Zhu, Q., Tembine, H., and Başar, T. 2011. Distributed Strategic Learning with Application to Network Security. In *Proceedings of American Control Conference (ACC)*.

Zonouz, S. A., Khurana, H., Sanders, W. H., and Yardley, T. M. 2009. RRE: A Game-Theoretic Intrusion Response and Recovery Engine. In *Proceedings of IEEE International Conference on Dependable Systems and Networks (DSN)*.