Game Theory for Cyber Security and Privacy

Article *in* ACM Computing Surveys · May 2017

DOI: 10.1145/3057268

9 authors, including:

Do Cuong
Kyung Hee University
25 PUBLICATIONS **517** CITATIONS
SEE PROFILE

Nguyen H. Tran
The University of Sydney
240 PUBLICATIONS **2,919** CITATIONS
SEE PROFILE

Choong Seon Hong
Kyung Hee University
909 PUBLICATIONS **8,789** CITATIONS
SEE PROFILE

Erik Blasch
Air Force Research Laboratory
726 PUBLICATIONS **12,831** CITATIONS
SEE PROFILE

Game Theory for Cyber Security and Privacy

CUONG T. DO, NGUYEN H. TRAN, and CHOONGSEON HONG, Kyung-Hee University
CHARLES A. KAMHOUA, KEVIN A. KWIAT, and ERIK BLASCH, Air Force Research Laboratory, Information Directorate
SHAOLEI REN, NIKI PISSINOU, and SUNDARAJA SITHARAMA IYENGAR, Florida International University

In this survey, we review the existing game-theoretic approaches for cyber security and privacy issues, categorizing their application into two classes, security and privacy. To show how game theory is utilized in cyberspace security and privacy, we select research regarding three main applications: cyber-physical security, communication security, and privacy. We present game models, features, and solutions of the selected works and describe their advantages and limitations from design to implementation of the defense mechanisms. We also identify some emerging trends and topics for future research. This survey not only demonstrates how to employ game-theoretic approaches to security and privacy but also encourages researchers to employ game theory to establish a comprehensive understanding of emerging security and privacy problems in cyberspace and potential solutions.

CCS Concepts: • **Security and privacy** →

Additional Key Words and Phrases: Game theory, cyber security, privacy

ACM Reference Format:
Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, and Sundaraja Sitharama Iyengar. 2017. Game theory for cyber security and privacy. ACM Comput. Surv. 50, 2, Article 30 (May 2017), 37 pages.
DOI: http://dx.doi.org/10.1145/3057268

1. INTRODUCTION

Recent increases in cyber attacks and identity theft make the Internet seem like a daunting place. Cyber attacks can lead to a severe and rising threat to our society as economic and communication infrastructures heavily depend on computer networks and information technology. The National University of Singapore and International Data Corporation reported that cyber security breaches and malware worldwide cost around $491 billion in 2014, of which consumers will likely spend $25 billion to mitigate security threats [IDC and NUS 2014]. After surveying 951 consumers as well as 450 chief information officers and information technology managers, the researchers estimate that 1.2 billion hours will be wasted dealing with cyber attack aftereffects.

Ren, Pissinou, and Blasch were funded under the AFOSR DDDAS program. This research was funded by the Ministry of Education (NRF-2014R1A2A2A01005900) and supported by the Basic Science Research Program through National Research Foundation of Korea (NRF). Approved for Public Release; Distribution Unlimited: 88ABW-2017-0275; Dated 24 Jan 2017.

Authors' addresses: C. T. Do; email: dothecuong@gmail.com; N. H. Tran; email: nguyenth@khu.ac.kr; C. S. Hong (corresponding author); email: cshong@khu.ac.kr; E. Blasch; email: erik.blasch.1@us.af.mil; C. A. Kamhoua; email: charles.kamhoua.1@us.af.mil; K. A. Kwiat; email: kevin.kwiat@us.af.mil; S. Ren; email: sren@ece.ucr.edu; N. pissinou; email: pissinou@fiu.edu; S. S. Iyengar; email: iyengar@cis.fiu.edu.

DOI: http://dx.doi.org/10.1145/3057268

The target of these attacks can be anyone from individuals to firms or government agencies. For example, a major cyber attack that forced Canada's Finance Department and Treasury Board to disconnect from the Internet was reported in 2011 [CSIS 2014]. In 2014, the hacking of Sony Pictures led the news for some time [Houser 2015]. Growing cyber security and privacy concerns require more effective defense mechanisms to counter these threats.

Game theory can answer the question regarding how the defender will react to the attacker, and vice versa, in cyber security. The strategic interaction between them is captured by a two-player game in which each player attempts to maximize his or her own interests. The attacker's strategy depends heavily on the defender's actions and vice versa. Thus, the effectiveness of a defense mechanism relies on both of the defender's and attacker's strategic behaviors. Using the game-theoretic approach, tactical analysis is performed to investigate the attack from a single node or multiple nodes. Hence, game theory is useful to investigate the strategic decision-making situations of the defender and/or to analyze the incentives of the attackers.

Game-theoretical approaches overcome traditional solutions to cyber security and network privacy in many aspects, which are described below:

(1) *Proven mathematics*: Most conventional security solutions, which are implemented either in preventive devices (e.g., firewall) or in reactive devices (e.g., anti-virus programs), rely only on heuristics. However, game theory can investigate security decisions in a methodical manner with proven mathematics.
(2) *Reliable defense*: Relying on analytical outcome from the game, researchers can design defense mechanisms for robust and reliable cyber systems against selfish behaviors (or attacks) by malicious users/nodes.
(3) *Timely action*: While adoption of the traditional security solution is rather slow due to the lack of incentives for participants, game-theoretic approaches advocate for defenders by using underlying incentive mechanisms to allocate limited resources to balance perceived risks.
(4) *Distributed solutions*: Most conventional defense mechanisms make decisions in a centralized manner rather than in an individualized (or distributed) manner. In a network security game, the centralized manner is almost an impossible solution due to the lack of a coordinator in autonomous system. Using appropriate game models, security solutions will be implemented in a distributed manner.

These reasons make the game-theory paradigm of interest in cyber security and privacy problems. In this article, we review the present trends and future cyber security issues in game-theory applications. We show the advantages and limits of game theory by describing three main applications of game theory. These applications included game-theoretic approaches in cyber-physical security, communication security, and privacy. Integrating cyber systems and physical systems into cyber-physical systems can raise many security problems, requiring a survey of current approaches. In communication security, we focus on perfect and imperfect monitoring game-theoretic approaches, denial-of-service, and survivability to show the advantage of distributed manner of game theory. Since cyber communication involves in interaction between users, game theory plays a critical role in achieving an equilibrium strategy to survive from unexpected attacks and interrupts. Also, with regard to cyber privacy, game-theoretic approaches are applied in cryptography, anonymity, information sharing, and confidentiality. For some selected works, we present game models and their features and solutions and list their advantages and drawbacks from design to implementation of defense mechanisms.

We organize the rest of this survey as follows: Section 2 provides a short description of the game theory to improve cyber privacy and security. Section 3 presents cyber-physical security issues. Section 4 describes security problems in a communication system, such as packet-forwarding security, Denial-of-service (Dos) attacks, and survivability problems. Section 5 presents privacy issues such as cryptography, anonymity, information sharing, and integrity. Section 6 suggests some future directions and draws conclusions regarding future game theory methods for cyber security and privacy.

2. APPLICATION OF GAME THEORY FOR CYBER SECURITY AND PRIVACY

Interest in using the a game-theoretic approach to address network privacy and security challenges has increased in recent years. In general, the attacker focuses on causing maximum corruption to cyberspace while the defender aims to minimize the damage. The attacker's objective is in conflict with that of the defender, which supports the application of the game-theoretic approach to study cyber security and privacy issues.

The following section provides the fundamental concept of game theory and some game models are briefly introduced. We also provide a few related considerations when designing and implementing game-theoretic approaches for cyber security and privacy.

2.1. Game Definition

We can define game theory as the application of mathematical analysis of individual and/or cooperative behaviors between players that choose a certain strategy/action to satisfy their self-interest [Myerson 1991]. A game is represented in strategic/extensive form describing the action of players. A strategic form of a game is formalized as follows:

$$Game = (P, (S_j)_{i\in P}, (u_j)_{i\in P}). \tag{1}$$

There is a set of P players in a *Game*. The player i can select a strategy from S_j and u_j is the payoff/utility of the player i. A combination of selected strategies of the player is a strategy profile, and a *mixed strategy* is generated from a set of pure strategies. The payoff function u_j is the relation between the space of input all possible profiles $S = \{S_j, j \in P\}$ and the output space of real numbers $\mathcal{R}$.

In a *Nash equilibrium* strategy profile, there is no player who can improve his profit by unilaterally modifying their strategies if the actions of the rest are fixed. Furthermore, the Nash equilibrium strategy of a player is a best reaction, which maximizes his or her payoff, to other player's equilibrium strategies [Myerson 1991]. We have a mathematical definition of a Nash equilibrium as follows:

Definition 2.1. A strategy γ^* is a Nash equilibrium if

$$u_j(\gamma_j^*, \gamma_{-i}^*) \geq u_j(s_j, \gamma_{-i}^*)\forall s_j \in S_j, \forall j. \tag{2}$$

However, a Nash equilibrium is not always *Pareto efficient*, another well-known concept of a game. A strategy profile can achieve Pareto efficiency if, in this profile, any player cannot increase his payoff without decreasing another player's payoff. The mathematical definition of Pareto efficient strategy profile is as follows:

Definition 2.2. We call a strategy profile γ^p a Pareto efficient outcome if for a strategy profile γ

$$\begin{aligned} &\forall j \;\; u_j(\gamma) \geq u_j(\gamma^p), \\ &\exists j \;\; u_j(\gamma) > u_j(\gamma^p). \end{aligned} \tag{3}$$

2.2. Game Models for Cyber Security and Privacy

In this section, we review some game-theoretic approaches modeling the interaction between malicious attackers and defenders. Different sorts of games have been employed

Table I. Summary of Game-Theoretic Approaches

Game model	Security and privacy problems	Solution
Static Prisoners' dilemma game	Selfish in Multi-hop network [Kamhoua et al. 2010], Privacy in Mobile Social Networks [Liang et al. 2012]	Nash equilibrium
Static zero-sum game	Jamming and eavesdropping [Ara et al. 2012], Denial-of-service attack [Spyridopoulos et al. 2013], Hardware Trojans [Kamhoua et al. 2014]	Nash equilibrium
Stackelberg game	Cyber-physical security [Martinez 2011], Data integrity and availability [Djebaili et al. 2014]	Stackelberg equilibrium
Coalition game	Selfishness in packet forwarding [Akkarajitsakul et al. 2013], Eavesdropping [Saad et al. 2009]	Coalition formation algorithm
Zero-sum stochastic game	Cyber-physical security [Zhu and Basar 2011], Secure routing [Zhu et al. 2011], Steganography [Johnson et al. 2012]	Saddle-point equilibrium, Nash equilibrium
Bayesian game	Trajectory privacy [Jin et al. 2013], Denial-of-service attack [Liu et al. 2013a], Survivability [Kamhoua et al. 2012c]	Bayesian Nash equilibrium
Dynamic game	Secure routing [Zhu et al. 2011], Cyber-physical security [Zhu and Basar 2012]	Saddle-point equilibrium
Repeated game	Selfishness in packet forwarding [Ji et al. 2010]	Belief-based strategy
Markovian game	Configuration of Intrusion Detection System (IDSs) [Shen et al. 2007b], Smart-grid infrastructure protection [Ma et al. 2013a], Trust issue in Online Social Network [Park et al. 2014]	Markov equilibrium
Evolutionary game	Selfishness in Vehicular Ad Hoc Networks [Shivshankar and Jamalipour 2014], Trust in Autonomous Multi-hop networks [Kamhoua et al. 2011], Survivability [Ma and Krings 2011]	Evolutionary stable strategy (ESS)

to study the action of the defender and attacker. Table I summarizes game-theoretic models, security/privacy problems, and main solutions obtained from the respective models. We then present some major aspects that classify security and privacy games in different ways and some game approaches assigned to the respective classification as follows:

- *Complete versus incomplete information:* In a *complete information* game, all players' payoff functions and strategies are known. However, in an *incomplete information* game, at least one of the players cannot observe the others' payoff functions and strategies. Thus, we can resort to Bayesian rules to predict the outcome of the game [Liu et al. 2013a].
- *Perfect or imperfect monitoring:* A game is called a *perfect monitoring game* if each player can find out the strategies chosen by other players at the end of each step [Khirwadkar et al. 2010]. In a perfect monitoring game, each player precisely observes the past action of all other players without any ambiguity when the player makes his or her move. On the other hand, in a game of imperfect monitoring, the actions of other players cannot be accurately observed, and, thus, players have only a noisy observation about the past actions of the others for which stochastic methods apply.
- *Static or dynamic (based on the number of stages)*: In a *static game* (strategic game), the players are assumed to make their decision at the same time. Static Prisoner's dilemma games (PDGs), zero-sum, and Stackelberg games are typical static security games. For example, in a PDG, two players get the reward price C if both players cooperate [Srinivasan et al. 2003]. They get the punishment price D if both defect. If there is one defector and one cooperator, then the defector and cooperator will obtain the temptations price N and substandard price M, respectively. Figure 1 shows the PDG in strategic form. For a one-stage game in which a player can select cooperation or defection, and defection dominates strictly cooperation, with an assumption

		Player 2	
		Cooperating	Defecting
Player 1	Cooperating	C,C	M,N
	Defecting	N,M	D,D

Fig. 1. Prisoners dilemma game in strategic form.

is $N > M > D > C$. As a result, the only Nash equilibrium strategy is defecting for both players to obtain the punishment prize M. Nevertheless, Pareto efficiency can be achieved if the two players select cooperation and obtain the reward price C. We surprisingly observe that the efficiency may not be achieved even when player's actions are supposedly reasonable. This scenario demonstrates that Nash equilibrium may not be Pareto efficient in a one-shot game. However, when the players repeat the game, they may choose cooperation to obtain expected future gains and reach the efficiency. Consequently, cooperation among players can emerge.

A *dynamic game* can be defined as a game having many stages. *Backward-induction* is a typical approach to achieve *a subgame-perfect-equilibrium*, a common solution of a dynamic game. The players can repeat a static game in a finite or infinite number of games. An instance of a dynamic game is a repeated game having two categories, perfect and imperfect monitoring games. A repeated game is a perfect monitoring game if one player can observe the strategies chosen by other players. A history of the repeated game at period tth is defined as a list of all players' actions in all periods before time t. In the repeated game, the players' pure strategy is a mapping of all possible histories to the current stage game strategy. The repeated game can be played during a finite or infinite period of time, and thus we can classify a repeated game as a finite game or an infinite game. Most repeated games typically represent an infinite time horizon repeated game in which the payoff function of a pure strategy profile γ of player i is

$$u_i(\gamma) = (1-\sigma)\sum_{t=0}^{\infty}\sigma^t u_i(a^t(\gamma)), \tag{4}$$

where σ $(0 \leq \sigma \leq 1)$ is the discount factor and $a^t(\gamma)$ is the strategy in period t. In finite repeated games, if the number of stages is known, it is optimal to play Nash equilibria of the stage game, even though that may not be Pareto efficient.

A *stochastic game* is also derived from dynamic games. In stochastic games, the transition from one stage to another stage follows transition probabilities [Osborne and Rubinstein 1994]. The stage game can change randomly or deterministically from time to time depending on the history of a fixed set of players. In general, the probability of the current state relies on the previous state and players' behaviors. When the current state is independent of the previous state and players' actions, the stochastic game becomes a repeated game with random states.

A particular kind of stochastic game is the *Markovian game*, in which a transition relies on only current states of the game and a set of players' strategies [Shen et al. 2007a; Ma et al. 2013a]. Each player then may receive a different payoff/utility function and aims to increase the expected summation of the discounted payoff. The process of states in the Markovian game is a Markov process; that is, the probability distribution on the next state is determined only by the previous state and actions. We can obtain Nash equilibria of a Markovian game using the solution of a chain of Markov-decision processes.

Evolutionary games model population change over a long period. Similarly to biology, selection and mutation are primary processes. While selection promotes some varieties over others, mutation diversifies the population. In general game theory, players are assumed to be rational, but the assumption of rationality is relaxed in evolutionary game theory [Shivshankar and Jamalipour 2014]. This means that a small group of mutants can perform some irrational strategies in the evolutionary game. In a large population, players are not assumed to have common knowledge of the game. Players aim to maximize their self-interest or the average number of survival offspring. The common equilibrium solution in evolutionary game theory is evolutionary stable strategy (ESS) that can resists mutation. Thus, a population can be stable over a long period if players choose to play an ESS. A full description of an evolutionary game is provided in previous works [Myerson 1991].

- *Noncooperative versus Cooperative*. In a noncooperative game-theoretic approach, players choose a strategy to optimize their own interests. On the other hand, cooperative players have joint strategies to achieve mutual benefits in a cooperative game. A *coalition game* is a *cooperative game*, in which players form a coalition to maximize a common objective of the coalition [Saad et al. 2009]. To form a coalition, players should harmonize their actions and have a contract to share equally the total payoff of the coalition. To ensure that no players incentivize to change their coalition, an equilibrium of a coalition game should be resistant to the action of departing from an established solution of the game by any class of players.

2.3. Game Theory: From Design to Implementation

The game-theoretic approach can capture the interaction between defenders and attackers. When we use game-theoretical approaches to design or implement in cyber systems, we should consider the following issues:

(1) *Rationality:* Almost all game-theoretic models applied to cyber security and privacy mainly focus on equilibrium strategy in the action profiles of defenders and attackers. However, in a real cyber system, due to bounded rationality [Kahneman 2003; Acquisti and Grossklags 2005] (i.e., limited information or resources), it is difficult for both the attacker and the defender to always perform the best-response actions. Therefore, appropriate models are required to predict player behaviors such as Prospect Theory and Quantal Response Equilibrium [Yang et al. 2013; McKelvey and Palfrey 2015]. Furthermore, in cases where multiple equilibria exist, it is unclear which players will choose or even if they can agree to choose one at all.

(2) *Multiple layers of protection:* In the literature, one specific defense mechanism is targeted by the defender, who then tries to maximize its payoff by setting appropriate parameters. However, the existence of multi-layers of defenders protecting against an attack, which is often implemented in present cyber systems, is disregarded. Therefore, an appropriate game approach is required to answer how multi-layered defenders can protect against attacks when the defending layers are implemented at the same time and how they can enhance the other layers.

(3) *Implementation:* In a real cyber system, when the attacker and defender make their decisions, they often consider many uncertain but real factors such as how much traffic is generated in a general network, the signal-to-noise ratio, and/or power of nodes in a wireless network. However, in a realistic scenario, the defender cannot observe all information perfectly. Therefore, the defenders should be able to analyze and understand the environment. Learning the changes in the environment can decrease the convergent speed to equilibrium and make the implementation more complex. In addition, some game-theoretic works model a security and privacy game as two-player games in which multiple attackers or defenders are considered as one entity. The two-player game is a reasonable model if those multiple attackers or defenders have the same strategies and payoffs but may not be realistic in a

practical system due to the diversity of the strategies and payoffs of the attackers and defenders.

In next sections, we will present several game-theoretic approaches to investigate security and privacy issues in cyberspace.

3. CYBER-PHYSICAL SECURITY

A cyber-physical system (CPS) that incorporates computing and communications intelligence unfortunately also creates many new opportunities for potential attackers, which needs a holistic defense framework. Recently, a new field called “cyber-physical security” is getting attention in the literature. The defender needs to consider both physical and cyber systems when he or she designs a defense mechanism. This section presents several defense mechanisms invented for cyber-physical security using game theory.

A CPS is a system of collaborating computational elements controlling physical entities. By using collected data via intelligent communications, the CPS can perform predictive analysis to reduce the cost and improve the effectiveness. Cyber-physical security problems come from not only cyber attacks but also physical disturbances such as unexpected natural disasters or direct malicious behaviors. The tight coupling and strong dependence between the cyber and physical systems pose new threats that require new approaches. The common defense mechanisms are inappropriate, not applicable and able to be scaled, or not compatible to solve such a great security and privacy demand by complicated CPSs.

To solve the security issues in CPSs, the defense mechanism should integrate the cyber system with the physical system to make the CPS more robust and resilient. Varying from the goals of cyber security, cyber-physical security aims to protect both the physical and cyber components of the CPS. Dependence on computing and networking increases vulnerability, while the presence of the physical system also adds more security concerns and constrains the set of feasible countermeasures. Integration of the cyber and physical dimensions is an important criterion evaluated in this section.

There are several integration aspects of the cyber and physical systems when designing efficient security protocols for CPSs. For example, communication network integration with the physical system differ from the traditional network (e.g., public Internet), and the defender can better design countermeasures if they are aware of the physical system state process in closed-loop control systems, which are modeled as discrete-time linear time-invariant (LTI) systems. Both cyber and physical attacks should be considered at the same time.

In next subsections, we first present how to design an optimal defender for CPSs against both cyber attacks and physical disturbances. Then we introduce several defense mechanisms invented for discrete-time LTI systems using game theory. Finally, we study the security problem in the smart grid system. In the literature reviewed next, the authors use static games, stochastic zero-sum games, dynamic Stackelberg games, and Markov games to show how the defender reacts to the attacker. To summarize, we provide new possible security and privacy threats that demand new approaches to disable them. Some works with key features of the cyber-physical security game are presented in Table II.

3.1. Control Design under Cyber Attack and Physical Disturbance

Zhu and Basar [2011] introduce a CPS as a part of an industrial control system that is depicted in Figure 2. The CPS consists of a *cyber system* and a *physical system*. The physical system has two layers as follows: (i) The physical layer consists of the physical components such as the power plant and (ii) the control layer comprises several control

Table II. Summary of Cyber-Physical Security Games

Game model	Features	Solution	Reference
Zero-sum stochastic game	Integrate the robust controller of the physical space and the resilient controller of the cyber space into the defender	Apply the value iteration algorithm to obtain a saddle point equilibrium	[Zhu and Basar 2011]
Static games	The physical and cyber spaces are integrated using the payoff function	Nash equilibrium and Stackelberg equilibrium are adopted	[He et al. 2012, 2013; Ma et al. 2011]
Dynamic games	The jamming problem of the discrete-time LTI system is studied	A saddle-point equilibrium can be determined	[Gupta et al. 2010; Martinez 2011; Shoukry et al. 2013]
Zero-sum Markovian games	The players choose a pair of actions that may cause state transitions of the smart grid system	Nash equilibrium is also a Pareto-optimal solution	[Ma et al. 2013a, 2013b]
Markovian game	Derive the optimal response action of the defender in the power grid system	Apply the value iteration algorithm to obtain a saddle point equilibrium	[Zonouz and Haghani 2013]

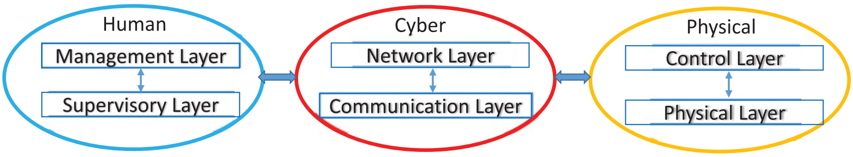

Fig. 2. An architecture for industrial control systems.

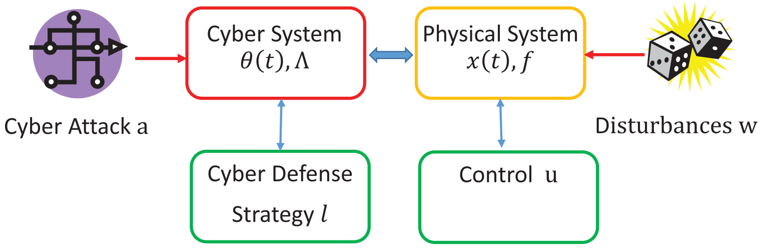

Fig. 3. The interaction between the cyber and physical system under cyber attack and physical disturbances.

units such as an observer/sensor, an intrusion detector, and an actuator. The physical system interacts with the cyber system via the communication layer, which consists of the physical communication channels, such as wireless systems and the Internet, for example. On top of the communication layer is the network layer, which provides topology of the network or has routing functions. The network layer and communication layer are considered the cyber world of the system. Supervisory and management layers together become the central processor of the system that makes decisions to control the physical system via the cyber system. The decisions are often made by humans; thus, supervisory and management layers are highly related to human actions.

The layered system makes it easy to understand why the cyber and physical systems are tightly coupled and heavily dependent. Figure 3 describes the holistic view of the interaction between the physical and cyber systems. In the cyber system, the discrete cyber system's state is described by $\theta(t)$, which is governed by transition law Λ. The law Λ relies not only on a behavior a of the attacker but also on an operation l of the defender. In the physical system, the continuous physical system's state is denoted by $x(t)$, which is governed by law f. The transition law f of the physical system depends on the disturbances w, the controller mechanism u, and the cyber state $\theta(t)$. The process of cyber state $\theta(t)$ is modeled by a Markov jump process that depends on actions of defenders and attackers [Zhu and Basar 2011].

Since defense against attacks repeats during a longer period, the physical system is assumed to reach the steady states when the system state is transiting. Thus, the defender should investigate the physical space at only stable states of every state θ in any moment t. Assume that the attacker aims to increase the damage of the system and the defender aims to decrease it. Then, the authors apply a *zero-sum stochastic game* to answer how the attacker and defender react to each other. Since the CPS is a hybrid system with continuous physical system states and discrete cyber system states, the combination of Markov chain dynamics and continuous time H^{∞} controlling systems [Basar 1995] is applied to derive long-term system performance.

From the literature, the game-theoretical approach was used to obtain the robustness in control systems under physical disturbance by Basar and Bernhard [2008]. However, with the growing integration of the physical system with the cyber system, modern control systems also need to consider the cyber attack for the design defence mechanism. Based on experience from designing the optimal control mechanism under unexpected *physical disturbance* in Basar and Bernhard's work [2008], Zhu et al. [2011, 2012] continue applying the game-theoretical approach for holistic control design for modern CPSs under cyber attack. While Zhu and Basar [2011] provide a general framework for physical disturbance, their following work [2012] investigates cascading failures in the CPS. Both of these works study how to combine a cyber security policy with robust control applied to modern CPSs using game-theoretic approaches.

From a different perspective, Ma et al. [2011] address the security of the CPS by analyzing the physical and cyberspaces together by integrating the payoff functions of two spaces. The article proves that there exists a Nash equilibrium of pure and mixed strategies for different payoff functions. In a similar approach, He et al. [2012] integrates the physical and cyber systems by modeling the probability of successful attacks on the CPS as a function of the number of components that are attacked and defended in both the cyber- and physical spaces. The authors study two possible games, *simultaneous-move* and *sequential-move*, between the defender and the attacker. By numerically comparing the *Nash equilibrium* in the former game and the *Stackelberg equilibrium* in the latter game, the authors show that the defender can gain more benefit when he or she moves first in the latter game. He et al. [2013] continue studying the resilience of CPSs by showing how defenders and attackers react to each other using the simultaneous-move game that takes both cyber- and physical spaces into account when designing payoff functions. The article illustrates that the way the payoff function is formed has a strong effect on the cyber and physical reinforcement strategies under unexpected attacks.

In the following section, researchers will take the physical system into account of the defense mechanism by considering physical system state processes that are modeled as discrete-time LTI systems in closed-loop control systems.

3.2. Control Design for a Discrete Time LTI Systems

Discrete-time LTI theory is applied for controlling physical systems (e.g., power plants) with so-called discrete time LTI systems. To protect them, game-theoretic approaches are employed. For example, the *dynamic zero-sum game* includes a controller (i.e., the defender) for a discrete-time LTI plant and a *jammer* (i.e., the attacker), who tries to disrupt the communicating channels between the plant and controller [Gupta et al.

2010], assuming that the jammer cannot disrupt more than M times during N periods. Thus, Gupta et al. [2010] derive the evolution of the plant state x under jamming as follows:

$$x_{k+1} = Ax_k + \alpha_k u_k + w_k, \quad k = 0, 1, \ldots, N-1, \tag{5}$$

where w_k is Gaussian white noise, u_k is the control signal, and α_k is a binary variable of the jamming node. $\alpha_k = 0$ shows that this jamming node is functioning; otherwise, this jamming node is not functioning in time slot k ($\alpha_k = 1$). Then, the authors construct a dynamic zero-sum game consisting of the following: (i) a cost function C; (ii) information sets $I_k = \{x_{[0,k]}, \alpha_{[0,k-1]}\}$ accessible by the jammer and controller; (iii) evolution Equation (5) that is a triple set $(x, s, t) \in \Upsilon$; and (iv) the defender's strategy $\tilde{\lambda}$ and jamming strategy $\tilde{\mu}$, which are measurable mappings from their information sets to their action sets (i.e., $u_k = \tilde{\lambda}_k(I_k) : \Upsilon \to \Re$ and $\alpha_k = \tilde{\mu}_k(I_k) : \Upsilon \to \{0, 1\}$). Then, a saddle-point equilibrium strategy is defined as a pair $(\tilde{\lambda}^*, \tilde{\mu}^*)$ such that

$$K(\tilde{\lambda}^*, \tilde{\mu}) \leq K(\tilde{\lambda}^*, \tilde{\mu}^*) \leq K(\tilde{\lambda}, \tilde{\mu}^*), \quad \forall \tilde{\lambda}, \tilde{\mu}. \tag{6}$$

At the *saddle-point* solution, cost K of the controller is minimum and cost K of the jammer is maximum. For general scenario (M, N), the analysis of the saddle-point solution is difficult. The authors suggest that rolling horizon control or approximate dynamic programming can be applied to calculate the solution. In a special scenario, $M = 1$ and an arbitrary N, the jamming strategy is threshold based. In other words, when a state value x is close enough to the threshold, a jammer is rewarding for jamming.

The jamming problem for a discrete-time LTI system is also studied using a *two-level receding-horizon* dynamic *Stackelberg game* by Martinez [2011]. The authors aim to find the control law for *the operator* and analyze the resulting performance and stability of the system under the jamming attack. There are two correlated attackers tampering with the wireless sensor and communication network of a control system: *a measurement jammer* and *a control jammer*. The current system state signal is a function of two components: a previous system state signal and a system input signal. *The measurement jammer* interferes with the previous system state signal while the control jammer interferes with the system input signal. At the first level, the measurement jammer makes its own decision as the *leader* of the game while the operator and the control jammer are *followers* of the measurement jammer. At the second level, the operator is the leader and the control jammer is the follower. Under these scenarios, the authors devise a receding-horizon Stackelberg control law to maintain regional stability of the control system.

Li et al. [2013] address the jamming problem in CPSs where a sensor node communicates with a remote estimator via a wireless channel. To avoid using complex dynamic games to cope with the discrete LTI process in CPSs, as in the previous work [Gupta et al. 2010; Martinez 2011], the author used two approaches: (i) a *Kalman filter* to estimate the system state x_k based on all of the measurements it collects up to time k and (ii) the average expected estimation error covariance at the estimator's side as the system performance measurement. As a result, a static game models how the defender and attacker react to each other. The game has a Nash equilibrium as the game solution.

Shoukry et al. [2013] handle the time-varying delay and the changing order of received packets under network packet scheduling attacks to CPSs. There are several methods for packet scheduling attacks, such as putting malicious code into one of the packets in the path between the destination and source, or performing unfairness attacks [Chen et al. 2009]. Shoukry et al. [2013] take a further step in studying a discrete-time LTI control system by considering not only the system state but also output signal disturbances. Based on the zero sum game, the authors develop a robust output feedback controller that has ability to recover quickly to network packet scheduling attacks.

3.3. Security Game for Smart Grid Systems

Another example of a CPS is a smart grid that consists of a system of power stations across a region and a communicating network for collecting information [Mo et al. 2012; Chen et al. 2012; Zonouz and Haghani 2013]. The operating effectiveness of the smart-grid depends strongly on assistance of the complex communicating network, part of which may be connected to a public Internet, such as the smart meter infrastructure [Mo et al. 2012]. Hence, it is easier for the adversary to execute cyber attacks to the smart grid.

Chen et al. [2012] study network robustness and consider network resilience protocols as *percolation-based connectivity*. The attacker aims to separate the network, whereas the defender tries to protect connectivity of the network in term of percolation. A *two-player game* is introduced to analyze the performance of defense mechanisms with different network configurations. The authors propose a *fusion-based* defense mechanism to collect the information in an effective manner by requesting a minimum amount of information (one bit) from each node. Based on the synthetic-network model and information of the topology at the Internet router level and of the European Union power station, the authors evaluate the proposed method and show that the network topology has major impacts on network robustness. Moreover, the power grid networks are more robust, because they have fewer hub nodes that are potential targets for attackers to reduce the network robustness.

Ma et al. [2013a] propose a defense mechanism for protecting the smart grid from attacks to connecting links between smart meters and the bidding that is vetted over a time-horizon. The authors apply the *Markov game* approach to model the interactions between the defender and the attacker. At every step, the attacker and defender select their strategies causing state transitions under probabilistic events of physical system. Since the network is large, this article uses a pruning algorithm to reduce time consumption but not to decrease the precision. Zonouz and Haghani [2013] also adopt the Markov game to derive the optimal response action of the defender in the power grid system. Eldosouky et al. [2015] proposed a contract-theoretic framework for resource allocation for critical infrastructure protection.

3.4. Summary

In summary, this section has presented security games in cyber-physical systems with different levels of integration between physical and cyber systems. Light integration is presented in Ma et al. [2011] and He et al. [2012, 2013] that simply couples two systems via the payoff functions. To integrate the physical system, some works [Chen et al. 2012; Ma et al. 2013a] only consider particular features, such as percolation and the general physical state of smart grids, respectively. However, Zhu and Basar [2011, 2012] combine stochastic game-theoretic and system control approaches to integrate the cyber attack to solve cyber-physical security issues based on well-studied works in physical disturbance of control systems by Basar [1995]. This is an appropriate approach, because it can provide a defense mechanism to manage the robustness and resilience of general CPSs. For a specific discrete-time LTI system, using different game-theoretic approaches, the researchers successfully integrate the physical system state jump process into the defense mechanism [Gupta et al. 2010; Zhu and Basar 2011, 2012; Shoukry et al. 2013]. Depending on how tight the integration is between the physical and cyber systems, game-theoretic approaches are dynamically applied as an effective means to create defense mechanisms in cyber-physical systems. However, some of the cyber-physical security game models are simplified to a zero-sum game [Gupta et al. 2010; Zhu and Basar 2011; Shoukry et al. 2013], thus, the researchers can extend this to a general-sum game model to make their scenarios more realistic.

4. COMMUNICATION SECURITY

As communication networks are more popular, privacy and security problems are getting more attention, and the game-theoretic approach is widely applied to enhance communication security. Moreover, there are more and more privacy and security concerns in the new generation of networks for which the game-theoretic approach can investigate the nature of competition between the defender and attacker in communication security. This section identifies the vulnerabilities and threats to communication networks and summarizes the defense mechanisms for the security of packet forwarding, denial-of-service, and survivability.

4.1. Security of Packet Forwarding

In this section, we present several defense mechanisms designed for *forwarding packet* issues using the game-theoretic approach. In a network, the transmitting nodes may behave selfishly to gain more benefit than the other nodes; consequently, the effectiveness of system may be reduced. To protect networks from selfish behaviors, security protocols ought to be investigated. Game theory was used to analyze strategic interactions among independent devices with conflicting interests [Srivastava et al. 2005]. Thus, game-theoretic approaches can be employed to show how malicious nodes generate selfish behaviors and to construct an appropriate defense mechanism.

With rapid advances in mobile and wireless communications devices and associated techniques, autonomous networks are becoming feasible and attracting more research attention. Future wireless communication will employ autonomous devices, such as sensors, smart phones, and computers, interconnected in an ad hoc manner and without any underlying networked infrastructure. Since the participating devices may strive toward their own interests, they could therefore misbehave by being *selfish* or *malicious* [Kamhoua et al. 2010]. Selfish nodes attempt not only to reduce cost but also to increase benefit without considering the other nodes. As a consequence, each node will strive to save its scarce resources while competing to gain access to others' resources with the goal of maximizing its own capacity.

An example of an autonomous network is an ad hoc network in which the network infrastructure is automatically constructed by nodes. The principal function of a node is to forward packets to ensure a viable network. Because there is no infrastructure in the ad hoc networks, intermediate nodes between the sender and the destination are requested to forward the packet for others. However, there is a cost in battery power and bandwidth associated with forwarding packets, and therefore, an intermediate node carefully makes a decision whether to forward or not to forward packets. Yet, if all nodes refuse to forward packets for others, then the network collapses. No node is interested in this situation. Thus, one of the important issues is packet forwarding if *selfish nodes* exist in networks.

A small number of selfish node behaviors may lead to performance degradation of the network [Tanachaiwiwat et al. 2004]; therefore, efficient mechanisms need to be designed to enforce node cooperation. *Virtual currency* and *reputation* are popular approaches to encourage cooperation using an economic approach. *Nuglets* [Buttyan and Hubaux 2001] and *Sprite* are the two most well-known solutions, in which a virtual currency system is employed to incentivize players to cooperate [Zhong et al. 2003]. Buttyan and Hubaux [2001] present models to pay for packet-forwarding services, in which intermediate nodes have some incentives to forward packets and earn Nuglets. However, these models need tamper-resistant components to collect a precise number

Table III. Summary of Forwarding Games

Game model	Features	Solution	Reference
Prisoners' Dilemma Game	Introduction of social morality to improve user privacy. Morality state is modeled as a Markov chain.	Nash equilibrium is adopted in an incomplete and a complete information game	[Liang et al. 2012]
Cooperative game	Forming coalitions to enhance a carry-and-forward-based packet-forwarding mechanism	A Nash bargaining formulation to obtain a Pareto-optimal solution	[Akkarajitsakul et al. 2013]
Stochastic game	Transmitting a packet is a Bernoulli process. The game is a repeated asymmetric game with random states.	Punish Only n Times: A distributed algorithm to achieve a Subgame Perfect Equilibrium	[Kamhoua and Pissinou 2010]
Repeated game	A formal-belief-system based on Bayes' rule to revise the other nodes' information under imperfect observation	An iterative update belief algorithm to find the sequential equilibrium	[Ji et al. 2010]
Evolutionary game	Decision-making of nodes based on the limited information of the others. Public Goods game is used to incentivize cooperation.	The strategy of the nodes is updated by comparing their payoff with a randomly chosen neighbor	[Shivshankar and Jamalipour 2014]

of Nuglets. Furthermore, nodes at the periphery of the networks do not have the same opportunity to accumulate the virtual currency. Unlike Nuglets, Sprite depends on the Credit Clearance Service (CCS) [Zhong et al. 2003]. Sprite does not require tamper-proof hardware; however, the fact that the CCS is a central authority violates the premise of ad hoc networks, which are distributed in their nature.

To model cooperation in a network, several game-theoretic approaches are used, such as game-theoretic approaches with perfect monitoring and imperfect monitoring. In an *imperfect monitoring* game, the players' actions may not be directly observable due to some noise. On the other hand, a game is categorized as a *perfect monitoring* game if a series of past actions is known by all players who can observe other players' actions directly and precisely. A static game is classified as a imperfect-information game, because there is only participator selecting his or her strategy at each time. Table III summarizes main factors of the packet-forwarding game.

In the following section, we first present works based on perfect monitoring and imperfect monitoring game-theoretic approaches, respectively. Then, we address security issues in the routing layers that are the center layers performing packet forwarding in multi-hop networks.

4.1.1. Perfect Monitoring. Srinivasan et al. [2003] motivate cooperation in a network using *Generous Tit-For-Tat* (GTFT), in which every participant imitates the other participants' strategy of the preceding round. The authors show that GTFT can be an equilibrium solution of packet-forwarding games. But, to compute this equilibrium solution, the utility function of every node must be revealed to the whole system. Utility awareness is a strong requirement for distributed networks.

Felegyhazi et al. [2006] employ a game-theoretic approach supported by *graph theory* to answer what circumstances can motivate nodes to cooperate. Although it is difficult to make whole nodes to cooperate, there is still a chance to have many cooperative groups formed from a small number of nodes. The proposal is based on a dependency loop. However, each node only knows its neighbors as opposed to the full network topology. Clearly, a dependency loop will not be common knowledge among nodes.

Jade et al. [2009] combine *virtual currency* and *stochastic game* theory to formulate an optimal policy to forward packets towards the route in peer-to-peer networks. When a source node requests data from the destination, each intermediate node is paid a virtual currency to relay the packet. The authors use cost and service capacity to calculate an optimal policy. Their incentive-based routing protocol shows better performance than the Dynamic Source Routing protocol.

Kamhoua and Pissinou [2010] apply game theory to design *Punish Only n Times*, a mechanism that can incentivize the cooperation of players in a distributed manner. The authors employ a *Stochastic Prisoners' Dilemma* game to characterize the behaviors of selfish nodes. Instead of rewarding intermediate nodes for delivering a packet, the authors propose to punish nodes for dropping a packet. The last intermediate node but not the originator of the packet can punish the other, and only the sender of a packet is rewarded. Moreover, this model incorporates the pragmatic case when some nodes do not have a packet to transmit in a number of time slots or do not have uniform traffic demand.

Liang et al. [2012] propose *social morality* to design an effective data-forwarding mechanism that does not intrude on user privacy in mobile social networks where privacy preservation severely conflicts with cooperative data forwarding if carelessly designed. The authors design a user-to-spot packet-forwarding mechanism, in which a *privacy preserving* mechanism is attached to help users hide their data. On the forwarding request, a user has two strategies: *cooperate* and *defect*. Based on the users' interest, morality level, and forwarding capability, the optimal data-forwarding strategy is determined. The tradeoff between the cooperation of information delivering and privacy preserving is achieved using a *nonzero sum two-player* game.

Akkarajitsakul et al. [2013] use a *coalitional game* to investigate dynamical behaviors of mobile nodes cooperating to delivery packets. The mobile nodes' objective is to maximize their payoffs in a *hybrid wireless mobile network* (with infrastructure and without infrastructure). A number of mobile nodes choose whether to join a coalition according to their self-interest utilities (e.g., average delivery delay and relay cost). Based on coalition formation, the authors show that the cooperative nodes can obtain greater payoffs than these of selfish nodes. For Vehicular Ad Hoc Network (VANET), based on coalitional game theory, an incentive mechanism in which nodes are rewarded for taking part in packet forwarding is proposed by Chen et al. [2011].

Shivshankar and Jamalipour [2014] combine *Evolutionary Game Theory* and *Public Goods Game* (PGG) to study cooperation for packet forwarding in VANET. The authors use PGG, which is a group interaction model for the study of cooperation, to investigate the effects of topological features on the evolution of cooperation. In PGG, cooperators secretly contribute a certain private token into the public pool, and the token is then multiplied by a multiplication factor r. This "public good" payoff is evenly divided among players, irrespective of the contribution. The factor r is an important element of PGG, since if the value of r is increased, the sharing benefits are also increased, which motivates the nodes to cooperate. In this packet-forwarding game, the authors show that cooperation diffusion cannot be forced but rather evolves with different networking conditions such as the average path length and user mobility.

4.1.2. Imperfect Monitoring. Most solutions of perfect monitoring games (e.g., Khirwadkar et al. [2010]) are robust with several conditions and not consistent with *noise* that often presents in a distributed wireless network. For example, the interruption of communication links, interference, or network congestion may lead to imperfect monitoring or nodes can disappear when they move out of communicating range. Moreover, to observe the other nodes' behaviors, a watchdog mechanism is implemented. However, the watchdog mechanism cannot observe during the sending or receiving of packets. All of these reasons can lead to inconsistent monitoring, and it motivates us to design an imperfect monitoring mechanism.

In Srivastava and DaSilva [2006], the authors investigate the noise in the packet delivering protocol and propose an *imperfect public monitoring* mechanism. The history of nodes' behaviors is not accurate; however, the authors assume that each node is able to access public information, but such public information may not be consistently available.

In Ji et al. [2006, 2010], the authors do not rely on the availability of public information. Instead of obtaining the same information of past actions of the other nodes, each node constructs its own knowledge of past actions of the other nodes. To overcome imperfect monitoring, the authors resort to a *belief-based* approach, since the equilibrium action of one node relies on the private history of the other nodes.

Under imperfect private monitoring, the *belief-free equilibrium* concept [Mailath and Samuelson 2006] is used to develop a packet-forwarding game model [Kamhoua et al. 2010; Wang et al. 2009]. To overcome inconsistent monitoring, Kamhoua et al. [2010] apply a stochastic dimension to investigate the variety of the packet delivery rate between wireless nodes. The packet-forwarding game equilibrium relies on only one factor: the probability of cooperation after recognizing a defection [Kamhoua et al. 2010]. To reduce the effect of the history of the game, these probabilities should be changed frequently to make them more correct. However, it is not certain that the belief-free equilibrium approach will be robust if there is private payoff information. In fact, in the two-node game, for instance, every node should know its opponent's payoff to perfectly balance the probability of cooperation after observing a defection so its opponent cannot distinguish between the cooperating and defecting actions over a long history. Although the authors show that the proposal is consistent to traffic inequality, mobilities, and noise using simulation results, considering private payoff information under a belief-free equilibrium approach is still an unresolved research problem.

4.1.3. Security for Routing. *Routing security* helps to establish stable communication paths between the source and destination. Therefore, if the routing mechanism is attacked, then the network is not available and reliable.

Game-theoretic approaches are employed in routing security in the literature [Buchegger and Boudec 2002; Kannan et al. 2003; Kannan and Iyengar 2004; Bohacek et al. 2007]. Here, we present several works using game-theoretic approaches to enhance security for routing for mobile ad hoc, multihop wireless, and cognitive radio networks.

For a mobile ad hoc network, which is *auto configurable* and *distributed* in nature, a *trust-based* secure routing protocol can be applied [Ghosh et al. 2004; Subbaraj and Sabarimuthu 2014]. Subbaraj and Sabarimuthu [2014] propose *a quality-of-service-contrained Eigen Trust-based* scheme to overcome *route failure*. They integrate a trust model and a non-cooperative game to encourages nodes to cooperate by learning. Kaliappan and Paramasivan [2015] use a *Dynamic Bayesian Signaling Game* to help regular nodes minimize the utilities of malicious nodes. Regular nodes continuously evaluate their neighbors by using belief evaluation. Regular nodes then choose a probability to cooperate with their neighbors for forwarding packets. This method could significantly decrease packet-dropping related to *misbehaving activities* from malicious nodes and thereby enhance secure routing.

In a multi-hop network, *selfishness* can create conflict between individual and collective interests. Instead of forwarding packets, self-interred nodes may not deliver data to reduce resource consumption. Thus, Kamhoua and Pissinou [2010] apply the *evolutionary game* approach to unfold the problem of *routing misbehavior*. The authors propose a distributed algorithm forcing cooperation between nodes to prevent the selfish nodes from dropping packets. Zhou and Cao [2012] utilize a *non-cooperative game* to analyze the behavior of the attacker under the operation of a *Trust Clearance Center*, which calculates and assigns a trust level based on the history of action of nodes. The proposed routing protocol can find the malicious activity and prevent it.

In cognitive radio networks (CRNs), Zhu et al. [2011] defeat jammers using the game-theoretic approach to design a dynamic secure routing protocol that considers packet error probability and delay as input parameters of a payoff function. The authors use a *stochastic multi-stage zero-sum* game to answer how the attacker will react to the honest node. Unlike the jamming attacks presented by Zhu et al. [2011], Wang et al. [2014] study the impact of malicious secondary users (SUs), which attempt to block the data transmission of the normal SU by routing packets towards the SUs around primary users (PUs). The authors propose a robust and spectrum-aware routing mechanism that models the interaction between non-malicious SUs and their one-hop neighbors as a stochastic game. Using simulation results, Wang et al. [2014] show that the proposed routing algorithms can minimize the routing delay in CRNs under attacks.

4.1.4. Summary. The principal intuition of the packet-forwarding game-theoretic approach is to motivate the cooperation of players using *repeated interaction* between them or punishing/rewarding mechanisms that facilitate players to achieve an equilibrium strategy in which self-interest nodes intend to cooperate. To incentivize the cooperation, delivering a packet is an optimal reaction to the other nodes' action, and a node cannot benefit by unilaterally discarding packets at the equilibrium solution.

Unlike virtual currency or reputation, the game-theoretic approach can avoid a centralized requirement to solve the problem of cooperation in *distributed* networks. In fact, solving the problem of cooperation with equilibrium or a utility function designed to incorporate full network parameters to be calculated will be demanding but less convenient and most likely subject to manipulation. Therefore, the main advantage of the game-theoretic approach is that it can be implemented in a distributed manner. This is consistent with the nature of a multi-hop ad hoc network.

We have also surveyed secure *routing protocols* in some modern networks and discussed several security problems relevant to routing. To enhance robustness and reliability, some protocols integrate trust mechanisms [Ghosh et al. 2004; Subbaraj and Sabarimuthu 2014; Zhou and Cao 2012]. The common game model in secure routing is the stochastic game that can capture the random selection of the next-hop/path of the nodes or the random misbehavior/attacks of the malicious nodes [Bohacek et al. 2007; Zhu et al. 2011; Kamhoua et al. 2010; Wang et al. 2014]. However, the stochastic game always assumes that the defender and attacker can detect the system state without error in each state, but this assumption is not true in many realistic scenarios where the devices are erroneous.

4.2. Denial-of-Service

This section investigates DoS attack issues and presents some defense mechanisms to prevent it using the game-theoretic approach. DoS attacks can cause severe threats to not only the Internet but also sensor and mobile ad hoc networks, and several defense mechanisms have been invented to reduce the damage from it. A DoS attack explicitly prevents the service providers from continuously providing their service to the user, and a distributed DoS (DDoS) attack organizes many attacking agents to achieve this [Zargar et al. 2013]. Figure 4 illustrates a common topology of a DDoS/DoS attack. The attacker frequently sends to a target a *stream of packets* consuming several main resources of the target. As a result, the target is unable to operate normally due to the lack of resources. The attacker also can deliver malicious packets to frustrate the defense mechanism of the target machine and mislead its function. Another attack approach is to control many computers to build an attacking army (e.g., Botnet), and then an arbitrary attacking node may launch a large and well-organized attack on

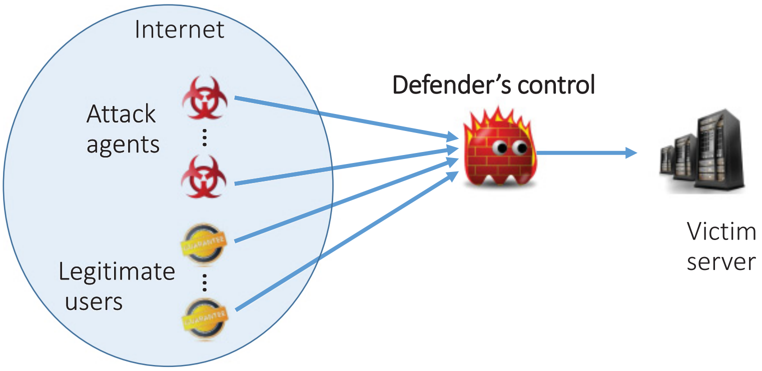

Fig. 4. A common topology of a DoS attack.

one or many targets. Because of the variety of attacks, it is difficult for researchers to design a defense mechanism to overcome DoS/DDoS attacks. Recently, Zargar et al. [2013] surveyed DoS attacks, but there is no game-theoretic approach in almost all of the DoS surveys. This section presents several works that use game theory to model and analyze attacker incentives in DoS attack problems.

In Fultz and Grossklags [2009], the authors employ a *static non-cooperative game* to analyze attackers incentives. Understanding attacker incentives can help researchers find a way to stop and respond to these attacks. The authors aim to answer how attackers react when facing different defense mechanisms, approaches, and degrees of independence. They apply a static non-cooperative game to analyze the decision-making process of both attacker and defender when they deploy their strategy simultaneously. Similarly to conventional games, a Nash equilibrium in this game may not exist, or this equilibrium becomes increasingly unbalanced when the number of attackers increases.

A *Bayesian game* model can be adopted to derive an optimal strategy for *security administrators* [Liu et al. 2013a]. For example, Mohi et al. [2009] resort to cooperation wireless sensor networks (WSNs) to prevent a passive DoS attack that is an internal DoS attack caused by dropping packets of self-interested nodes. Mohi et al. [2009] enforce node cooperation using a *two-player static Bayesian* game, in which wireless devices of WSNs and the monitoring device (IDS) are the players. Bayesian enforcement helps wireless nodes gain *reputation* if they operate properly; IDS is also able to improve its performance by utilizing the knowledge of a series of past events of this game. Furthermore, the game-theoretical framework can be established to show how the defender react to the attacker under *active bandwidth depletion attacks* for DoS/DDoS, where one or many attacking-nodes aim to interrupt connecting links by consuming as much bandwidth as possible [Bedi et al. 2011; Wu et al. 2010; Liu et al. 2013a]. While Wu et al. [2010] consider a general traffic scenario, Bedi et al. [2011] focus on a Transmission Control Protocol (TCP)/TCP-friendly scenario. Both static and dynamic *non-zero-sum games* are applied to achieve an optimal action to prevent fraud traffic while admitting appropriate traffic.

In Khirwadkar et al. [2010], the authors apply a repeated game model and *fictitious play process* to design a *pushback* defense mechanism that motivates cooperation between routers to reduce congestion. A fictitious play process is a repeated mechanism in which one node can store a history of actions and predict the others' responses. In every step, the player updates his or her prediction and reacts to the opponent player using the best response to the prediction. This process helps two players, the attacker and the defender, learn to achieve the Nash equilibrium even if the players do not have information about the other utility function in a two-player game.

Yan et al. [2012] use the *semi network-form* game to model stochastic system states and *level-K* thinking to capture the variant complex levels of strategic thinking. The advantage of the network-form game-theoretic framework is that it has ability to investigate different DDoS attacking plans in which the defender implements many protecting layers that depend on various variables. Constructing a Bayesian network is a key aspect of describing the dependencies of the decision-making elements. The outcome of the game depends on the value of K in level-K reasoning, where players maximize the payoff at level k using the information of level-$K-1$.

Not only DDoS attacks but also *scarce resources* of the network providers can lead to DoS. If the network provider does not invest to increase the QoS for users, then the users will experience low QoS or even DoS in peak periods. Consequently, the users choose to change their network provider. Kamhoua et al. [2012] employ a repeated game model to analyze user and network provider interactions. Then, the authors propose a practical mechanism, which can be easily implemented on a smartphone, to incentivize users to collaborate to achieve higher bargaining power.

In summary, game-theoretic approaches provide fundamental ideas to answer how the defender will react to the attacker in DoS/DDoS attacks, in which the defender can resort to filtering and/or rate limiting as attack countermeasures. While several works analyze the effectiveness of individual countermeasures, Spyridopoulos et al. [2013], Bedi et al. [2011], Liu et al. [2013a], and Yan et al. [2012] integrate filtering, rate-limiting, and bandwidth capacity extension in conjunction to study multi-layer protection. In the aforementioned works, payoff functions have parameters, such as the bandwidth share utilized by legitimate traffic and the number of legitimate packets incorrectly dropped, as in Spyridopoulos et al. [2013]; the number of bogus packets allowed to pass through the filter, as in Wu et al. [2010]; or the costs associated with adding more bandwidth or using more zombies, as in Yan et al. [2012]. Once the payoff function is defined, the payoff function is used to obtain Nash equilibrium actions for the defender and attacker. To calculate a Nash equilibrium solution, each player requires full knowledge of payoff function; however, the fictitious play mechanism does not need this assumption [Khirwadkar et al. 2010].

4.3. Survivability

The *survivability* (or availability) aims to provide stable service and figures out problems that might interrupt such availability. Unavailability of service such as connection, storage, or computing can have a severe impact on business. We summarize in this subsection a few recent works that take into account survivability in defensive mechanisms.

In Ma and Krings [2011], the authors apply the evolutionary game-theoretic approach to study *reliability*, *fault tolerance*, and *survivability*. The agreement algorithm of *Byzantine* generals' issue is employed in a dynamic situation to check the *consensus* among game players. In a such circumstance, the number of generals and traitors dynamically evolves.

Shen et al. [2012] evaluate the survivability of WSNs under attack using a *continuous-time Markov chain* and a stochastic game that aims to calculate the *mean time to failure* (MTTF). In the *attack-prediction* stochastic game, the attacked sensor node is classified as healthy, vulnerable, weak, compromised, or failed. While the attacker chooses to attack or not to attack, the system also has two responding actions: to defend or not to defend. Since the transposition of activating actions state is stochastic, a finite set of states of a sensor device's lifespan is described using the continuous-time Markov chain. Then, the authors can derive the availability, reliability, and *survival lifetime* at the system steady state. Using numerical results, the authors show that the prediction of the expected motivation of the attacker has higher priority in the vulnerable state than that in the weak state, which is beneficial in prolonging the MTTF of the attacked device. To increase the survival lifetime of the overall WSN, they recommend increasing total sensor devices in a cluster and/or decreasing total clusters in a path from the sender to the receiver.

The degree of *replication* within a system can be paramount to the system's survivability [Kamhoua et al. 2012a, 2012c, 2013]. In fact, a particular subsystem may fail, but the overall system survives because the functions performed by the failed component are replicated. To reinforce replication, diversity is also taken into account in the survivability of the system. Kamhoua et al. [2012a] developed a scheme that tracks a replica's history leading to the building of that replica's reputation, that is, an estimate of how much a defender can believe in that replica's *genuineness*. This approach uses a mechanism based on a *repeated game*. Specifically, the authors apply a repeated game among replicated nodes to extend the mission survival times in a critical mission. The *replica voting mechanism* consists of three main parts as follows.

(1) The reputation U of the wireless node is continuously revised using an exponential moving average based on updated events. The reputation $U_k(t)$ of a wireless node k's at the t time slot is calculated based on a recursive rule as follows:

$$\begin{cases} U_k(0) = 0.5, & \\ U_k(t) = (1-\gamma)U_k(t-1) + \gamma & \text{if node } j \text{ vote correctly,} \\ U_k(t) = (1-\gamma)U_k(t-1) & \text{if node } j \text{ vote incorrectly,} \end{cases}$$

where $\gamma \in (0, 1)$ is the smoothing factor.

(2) An optimal value w_k is given as

$$w_k = \log \frac{U_k(t)}{1 - U_k(t)}. \qquad (7)$$

The vote weight w_k use the weakness of ambiguous data from malfunction nodes; for example, knowledge from the node that has zero reputation all the time can be put on the opposite side to derive the correct value.

(3) The game decomposition approach discouraging malfunction nodes from accumulating credit. Thus, it can prolong the accumulating-reputation process of malfunction nodes.

Replicas support mission survival; however, replicas should run transparently. A replicated process, for example, will produce replicated outputs that have to be resolved to a single output. Voting among the replicas resolves multiple outputs and can prevent some malicious replicas from corrupting the outcome. *Voting*, which is a strategical mechanism using a node's guess about the fraction of nodes taken over by the attacker, is categorized as a Bayesian Zero-sum game. Replication coupled with voting can, therefore, be a pervasive element of survival. *Binary voting* algorithms are used by Kwiat et al. [2010] with computer replication for providing both security and reliability. Kamhoua et al. [2012c] again apply binary voting games among replicated nodes to extend the mission survival time in a critical mission. The outcomes of the security games help to derive the total mission survival time by both mathematical proofs and simulations. In a similar work [Kamhoua et al. 2013], the defender is always better off when using diverse replicas in an *incomplete information* security game in which the attacker skill level and the success probability of the defender are not common knowledge but private information.

5. PRIVACY

Recently, *privacy* has become a critical issue as mobile applications, networks, and the Internet have rapidly developed. Social networking websites (e.g., Twitter, Facebook)

Table IV. Summary of Privacy Game Models

Privacy issue	Key objective	Game model	Solution
Cryptography	Guarantee that participators keep using the designated service	Two-player static game Dynamic game Extensive form game Repeated game Stochastic two-player zero-sum game	Nash equilibrium Perfect Bayesian equilibrium Bayesian Nash equilibrium Computational Nash equilibrium ϵ-approximate Nash equilibrium Threat-free Nash equilibrium
Anonymity	Aim to participate in the system without being tracked	Perfect and complete sequential game Repeated game Bayesian game	Subgame Perfect Equilibrium Nash equilibrium Bayesian Nash equilibrium
Information sharing	Protect the privacy information in the information sharing process	Cooperative game Evolutionary game Strategic game Two-player zero-sum Markov game	Vickrey-Clarke-Groves mechanism Nash equilibrium Markov equilibrium
Confidentiality	Limit access or place restrictions on certain types of information	Signaling game Two-player static game Repeated game	Bayesian equilibrium Nash equilibrium Subgame perfect equilibrium

and professional networking sites (e.g., LinkedIn) have billions of active user, and online shopping sites have seen exponential growth. Consequently, the amount of stored personal information, such as private pictures and data, financial information, and location, is also increasing exponentially. For example, according to a report from Symantec, more than 8.4 billion email messages are generated by Symantec's clients each month [Symantec 2014]. The more information we put in cyberspace, the greater the chance of a privacy breach. Not only individuals but also enterprise clients are concerned about privacy when engaging in online activities, because there are many methods of compromise that can range from using spyware/key logger to collecting histories of users' activities. Furthermore, modern applications expect nodes to automatically build an autonomous network without a central manager. Protecting privacy without a central manager is challenging (e.g., trust management in autonomous multi-hop networks [Kamhoua et al. 2011]) and to tackle privacy issues in a distributed manner, game theory is a natural and powerful mathematical framework. In this section, we focus on several applications for game theory as follows: cryptography, anonymity, information sharing, integrity, and confidentiality. Reviewed privacy game models in the following subsection are summarized in Table IV.

5.1. Cryptography

Cryptography generally aims to guarantee that participants keep using the designated service, and this is the same objective in the game-theoretic approach. The game-theoretic approach is employed to invent an incentive mechanism aiming to prevent diversion. Katz [2008] provides a survey of the common subject of cryptography and the game-theoretic approach; however, we focus on several new trends in applying game theory to cryptography from recent works. Katz [2008] reported his research several years ago, and as cyberspace rapidly changes, cryptography needs to adapt to those changes. Thus, we briefly review game-theoretic approaches for *multiparty computation*, *secret sharing*, and *steganography*.

5.1.1. Multiparty Computation. Multiparty Computation is classified into the cryptographic literature in which various players jointly compute a function based on the private data they each provide. Then, after *secure computation*, each player has a share of the function value without revealing their private data to everyone.

Asharov et al. [2011] demonstrate how to employ a *two-player static* game into standard cryptographic notions when considering *malicious fail-stop* adversaries. The authors consider privacy, correctness, and fairness as parameters in the game-theoretic simulation-based framework. The players can choose one of two strategies $\{\sigma^{continue}, \sigma^{abort}\}$, that is, the player to follow $\sigma^{continue}$ must precisely follow the protocol specified by the mechanism designer. From this, the authors argue that when a player terminates the computation, the opponent player cannot react. Therefore, a player that terminates cannot be punished.

Although Asharov et al. [2011] show the impossibility of rational fair computation for a particular function and a particular set of utilities, Groce and Katz [2012] demonstrate that *fairness* can be achieved for a much broader class of utility functions than those specified by Asharov et al. [2011]. Furthermore, Groce and Katz [2012] conclude that whenever the strategy (i.e., computing the function) is a strict Nash equilibrium in the ideal world, then it is possible to construct a rational fair protocol in the real world.

Most of the previous works use computational variants of Nash, for example, Asharov et al. [2011], or *correlated* and *Bayesian* equilibrium as the solution concept for security games in multiparty computation [Katz 2008]. However, in real scenarios, players cannot observe the move made by others in cryptographic protocols. Thus, a *dynamic game* of imperfect information is recommended as a natural method for modeling this uncertainty [Wallrabenstein and Clifton 2013]. Then, the *perfect Bayesian equilibrium* is adopted as the solution.

We next consider a secret sharing protocol, which is getting more attention in the modern cryptography.

5.1.2. Secret Sharing Protocol. A secret sharing scheme allows someone to *share a secret message* among a set of players. For instance, a secret α is distributed among n players $P_1, \ldots, P_n$ for subsequent secret recovery such that any t may *reconstruct* secret α. The number t comes from an assumption: There are at most $n - t$ "bad" players who may oppose cooperation, while the "good" players obey the prescribed protocol. Since the two terms "good" and "bad" do not generalize all types of players, researchers recently have focused on studying a rational secret sharing protocol. Note that the players are presumed to be *rational* players aiming to optimize the benefit. Game-theoretic approaches can help the secret sharing protocol to guarantee that malicious players cannot stop normal players from reconstructing the secret.

Fuchsbauer et al. [2010] rely on the *synchronous point-to-point* channel to design an efficient rational secret sharing protocol. They demonstrate how secret sharing notions can be framed in a game-theoretic view when considering *t-out-of-n* secret sharing. It consist of a dealer D distributing the secret sharing of α to participators $P_1, \ldots, P_n$ as follows: (1) It requires only t any participators to rebuild the secret α and does not need support from the dealer, yet (2) there is no group having fewer than t participators can rebuild the secret α. The proposed protocol induces *computational Nash equilibrium* as the solution of the game. However, efficient schemes obtaining the computational equilibrium cannot be functional when any participator is computationally unbounded.

Once there is strict security requirement or *computationally unbounded* participator, a unconditionally secure rational secret sharing mechanism is more reliable. Zhang and Liu [2011] propose a rational secret sharing mechanism that is coalition resilient. However, the proposal only achieves ϵ*-approximate* Nash equilibrium, which means that even a computationally unbounded participator deviate from the prescribed mechanism, he would not obtain more than ϵ-benefit.

Nojoumian and Stinson [2012] introduce *socio-rational* secret sharing, where cryptography, a repeated game, and reputation systems are combined as an integrated secret sharing protocol. Since the secret sharing game is assumed to be repeated an unknown number of times, rational players need to consider future gain or loss. Then the reputation value is updated according to a player's behavior each time the game is played. The authors employ a Nash equilibrium as the game solution that reflects the long-term interactions between players using *reputation*. However, they also assume that there exists a *public trust network* that stores a player's believed honesty based on past protocol interactions.

In cryptography, the *trusted mediator* is proposed to direct the game to a desirable *correlated equilibrium* [Katz 2008]. However, Gradwohl et al. [2013] rely on *threat-free Nash equilibria* to propose a cryptographic protocol but not to use the trusted mediator under some conditions. Unlike the previous work [Gradwohl et al. 2013], Wallrabenstein and Clifton [2014] realize that using *point-to-point communication* resources instead of relying on the trusted mediator also preserves the original equilibrium. The authors transform the classic prisoner's dilemma into extensive form game models and then present a full security proof for rational secret sharing under their proposed framework.

5.1.3. Steganography. Steganography aims to conceal videos, text-files, messages, and images. In a general context, secret messages can be covered by a digital means such as a text-file, an image or a video file, a program, or even a protocol. A multimedia file is a perfect means for *steganographic transmission*, since it is easy to modify. For example, adjusting a few of the pixels in a Joint Photographic Experts Group (JPEG) image is not difficult. Moreover, compared to cryptography, in steganography the intended hidden message gets less attention because it does not look like a secret hidden mechanism. Game theory is employed to address the security of practical steganography in which the defender (*steganographer*) wants to hide a message in a cover object while the attacker (*steganalyst*) wants to distinguish plain covers from those with a hidden message.

The defender and attacker's behaviors related to the security of practical steganography are captured by a *stochastic two-player zero-sum* game. The steganographer tries to increase his or her security by maximizing the attacker's decision error, whereas the attacker tries to minimize it [Johnson et al. 2012; Schottle et al. 2013]. The steganographer aims to attach the concealed message in series randomly using a predefined distribution such that the location in series is not distributed identically but independent. On the opposite side, the steganalyst tries to classify a digital file that may or may not cover the concealed message. The payoff for the steganalyst is the precise categorization probability, and the payoff for the steganographer is the imprecise categorization probability of the steganalyst. Then, Schottle et al. [2013] prove a unique existence of the *mixed strategy* Nash equilibrium.

Since the current steganographic embedding prototype resorts to an additive-distortion minimizer, Denemark and Fridrich [2014] take the *distortion function* into account when employing the game-theoretic approach to enhance the security of steganography. In the proposed game, the strategies of the steganographer and the steganalyst are sets of values, which are the resources for modifying the pixel in a digital file. The authors adopt the minimal total error probability under equal priors as the payoff functions that are used by both the steganographer and the steganalyst. Thus, the solution of this game is a Nash equilibrium, that is, the *saddle point*, which is the minimum payoff for the steganographer and the maximum payoff for the steganalyst.

5.1.4. Summary. One objective of applying game theory in cryptography is to model the malicious behavior of users. The reason for this is not only the fact that a malicious action is more difficult to control than a rational action, but that it is also more realistic and frequent for some of the participants to not honestly follow the cryptographic protocol. To increase the efficiency and security of the cryptographic protocols, researchers propose many approaches and new terminologies such as socio-rational secret sharing [Nojoumian and Stinson 2012], using a point-to-point channel instead of the trusted mediator [Fuchsbauer et al. 2010; Wallrabenstein and Clifton 2014], or employing perfect Bayesian equilibrium [Wallrabenstein and Clifton 2013]. Game-theoretic approaches have recently been employed for steganography and are ideal mechanisms that permit researchers to evaluate certain design options, such as distortion functions [Denemark and Fridrich 2014] in adaptive steganography or payload distribution in batch steganography [Schottle et al. 2013; Johnson et al. 2012; Ker et al. 2013]. All these works demonstrate that the interplay between cryptography and game theory has a huge benefit in the design of defense mechanisms.

5.2. Anonymity

The property *anonymity* expresses a condition in which a player is *anonymous* or basically hidden and able to participate in the system without being tracked. Therefore, a device is anonymous if it is able to present in a system but does not disclose its identification. Anonymity is very important and should be achieved in many areas in cyberspace, including browsing the web, accessing networks (wired or wireless), using a cloud service, and so on. When there is no demand to reveal personal identifiable data, service providers should hide it. On the other hand, users should actively participate in anonymity-preserving mechanisms instead of relying on service providers. Game theory can help both users and service providers analyze and increase anonymity in cyberspace.

The critical issue when personal data are collected, stored, and published is privacy protection. In the anonymization process, choosing an appropriate *level of privacy protection* is a crucial decision determined by answering the question of how to set the privacy parameter and what the optimal value is. Adl et al. [2012] employ a game-theoretic model that finds consensual privacy and utility levels by considering the preferences of three different parties: a *data provider*, who can choose to participate in data collection if they see it as worthwhile; a *data collector*, who collects and provides privacy protected data to data users; and a *data user*, who wants to perform data analysis on a data set and is willing to pay for it. The interaction between the three parties who individually aim to maximize their utility can be modeled using a perfect and complete sequential game. The *subgame perfect equilibrium* is adopted as the solution determined using *backward induction*. When the authors use *k-anonymity*, which was first introduced by Sweeney [2002], as the privacy parameter, the equilibrium value of k represents shared agreements in which none of the players attempts to behave differently.

Mohammed et al. [2011] apply an *infinitely repeated game* in data-integration process to prevent harmful nodes and to guarantee *fair and honest* adhesion of the data provider. To combine the proficiency and to provide more flexible service to customers, data providers resort to the data-integration process. However, during the anonymization process, if malicious providers seek to get out of control from the secure protocol to increase their profit, then the game-theoretic approach is an appropriate model to overcome such problems. In this security game, the provider chooses a strategy (to participate or not participate) to attain the rational participating point. Using a game-theoretic approach, the authors proposed an effective and scalable algorithm based on locally generated information.

Although location-based service provides great advantages to mobile device users, it also introduces significant threats to privacy. A game-theoretic approach is a perfect method for investigating *location privacy* protection issues for self-interested mobile users in a distributed mobile environment [Adl et al. 2012; Freudiger et al. 2009; Shokri et al. 2012; El-Badry and Younis 2012]. Recently, the game-theoretic approach has been employed to increase anonymity in location-based service in wireless networks [Jin et al. 2013; Liu et al. 2013b].

In WSNs, Jin et al. [2013] model cooperation and trust behaviors of autonomous mobile nodes with the existence of selfish and malicious sensor nodes using *Bayesian game* theory. The authors provide equilibrium strategies for users in a *trajectory privacy* preservation game in which there are two neighboring nodes as players. To preserve trajectory privacy, each node needs to cooperate with its neighbor; however, the node does not know whether its neighboring nodes will cooperate, defect, or even attack. Thus, a Bayesian game formulation is applied to model the interactions between two neighboring nodes.

Liu et al. [2013b] propose a distributed *dummy user* generation to design a location privacy-preserving mechanism. In the example scenario, the trajectories of users u_1 and u_2 are obtained from location reports, r, of location-based service that is eavesdropped or concluded by side information associated with u_2's real identity r_2. Without dummy users, an adversary may achieve the correlation between u_2 and r_2 by comparing the footprints in these trajectories. Thus, the adversary can learn r_2's moving trajectory beyond the span of side information. By introducing the dummy users u_2', the risk of r_2's whole trajectory being revealed is reduced. However, generating dummies costs the users resources, thus, the selfish users may not be motivated to generate dummies to preserve the privacy. Using *Bayesian game* models, the authors design an incentive mechanism to help users achieve *k-anonymity* to measure the effectiveness of location privacy protection. In the Dummy User Generation game, the players have two strategies: (1) Cooperate (i.e., generate $k - 1$ dummy users) or (2) Defect (i.e., only report one's own location and wait for others to generate dummy users). Then, the property and existence of the Bayesian Nash equilibrium are analyzed using both theoretical proof and simulation results.

In summary, we have briefly reviewed a game-theoretic approach to analyze anonymity. To achieve anonymity, all participants and infrastructure need to trust each other and cooperate together. The reviewed works demonstrate that game theory is useful for providing incentive schemes in the context of multiple participants [Mohammed et al. 2011; Adl et al. 2012; Franzen and Pointner 2012] or in self-organizing networks [Jin et al. 2013; Liu et al. 2013b], which require distributed mechanisms.

5.3. Information Sharing

Recent works model problems of *information sharing* as security games and apply the incentive mechanism to tackle *malicious* or *dishonest* behavior. Sharing private information or data between individuals or organizations can yield many benefits, such as quickly accessing data or extracting useful knowledge from big data. However, a dishonest/malicious user can undermine others' reputations or cause other types of damage based on others' private information. Protecting the privacy of even one participant is successful only if every partner of the system in possession of the participant's private information also protects it. However, protecting privacy information in the context of information sharing relies on the importance of privacy to participants, the resource consumption to conserve it, and participants' certainty in the secret sharing mechanism. The game-theoretic approach is the most effective for modeling and designing incentive mechanisms to protect privacy in information sharing, especially considering the nature of sharing data that requires distributed protocols.

The classic *Vickrey-Clarke-Groves* (VCG) scheme is adopted to incentivize *truth telling* in the context of distributed data mining, which aims to obtain data and assemble in a model that should be more meaningful than the beginning data [Kantarcioglu and Nix 2010; Nix and Kantarcioуglu 2012]. Each player P_i has x_i, a part of information contributed to compute a certain data-mining function. The VCG mechanism aims to achieve an optimum *social-welfare* of all players in the *cooperative sharing game*. In this game, the player P_i decides whether to participate with an amount x_i' of data. Denote D as the data-mining function and X' as the vector of chosen values x_i' or all players and $m = D(X')$ as the function results all players receive. The utility of each players is given as follows:

$$u_i(x_i, D(X')) = \max\{v_i(m) - v_i(D(x_i)), 0\} - p_i(X', m) - c(D)v_i(m), \tag{8}$$

where $v_i(\cdot)$ is the valuation function, player P_i pays $p_i(\cdot)$ according to the result and input, and consumes a cost $c(D)$ to compute the function D, all of which are defined correspondingly to particular data-mining models. Using real data in different data-mining models, the authors run the proposed mechanism to prove its usefulness in practice. They conclude that the incentive scheme encourages all participators to perform honest behaviors in the data sharing mechanism such that the user do not have to check the data again after the computing process. Following their works, Kantarcioglu and Jiang [2013] propose an incentive privacy-preserving mechanism by modifying a noncooperative computation model that is an ideal application of the game theory in a distributed computation setting. To achieve beneficial data models or analysis results, competing participants having private information might work together to perform *privacy-preserving* distributed information analyzing tasks.

In the work by Wang et al. [2011], the set of strategies for any given users in *Peer-to-Peer* systems, which have sharing mechanisms between peers, includes three actions: always cooperate, always defect, and always reciprocate. According to a strategy, different profit/loss and the corresponding payoff are determined. An evolutionary game is used to design a *reciprocity-based* incentive mechanism and investigates the dynamics of a soft security mechanism, which is defined as a social incentive mechanism to win against peers' self-interested behavior.

Outsourcing complex computation tasks has been proposed and implemented in many applications in which big data have been utilized in parallel in the processors of a huge number of participants. As a result, the *outsourcer* (customer) is relieved from maintaining a dedicated computing infrastructure. However, there is a concern for the outsource about the *correctness* of the returned results. Hence, to guarantee the soundness of the return results, there must be a mechanism to encourage the participant of computation services to perform the computation *completely* and *honestly*. To avoid an expensive cryptographically verifiable computation that aims at defeating malicious agents, many civil purposes of outsourced computation tolerate a weaker notion of security, for example, contractors. The goal of a *contract* for outsourcing computational tasks is to minimize the expense of the outsourcer while guaranteeing correct computation using appropriate *rewards*, *punishments*, and *auditing rates*. Nix and Kantarcioglu [2012] employ a game-theoretic model to design a proper incentive contract that effectively deters selfish or dishonest behavior on the part of the data outsourcing services in cloud computing. The authors use the outcome of the game to prove that the incentive for an outsourcing service to cheat can be reduced to zero. Pham et al. [2014] provide an incentive analysis of outsourced computation with non-malicious but selfish utility-maximizing agents. Differing from the work by Nix and Kantarcioglu [2012], they allow partial outsourcing, direct auditing, and auditing through redundancy, for example, employing multiple agents and comparing the results, and optimize the utility of the outsourcer among all hybrid possibilities. Pham et al. [2014] establish the global optimality of contracts using a Nash equilibrium.

Online Social Networks (OSNs) help people connect and share resources such as video, pictures, and other files. However, an inappropriate sharing mechanism might generate privacy lapses or security violation that would make the user leave an OSN. The game-theoretic approach is used to study privacy for information sharing in OSNs in which users need to determine the optimum *levels of information sharing* [Park et al. 2012a, 2012b; White et al. 2013]. The authors use a *two-player zero-sum Markov* game to capture the interaction of users and attackers under several scenarios: an attacker without knowledge, with limited knowledge, and with full knowledge of attacked systems.

Sharing information between cyber firms not only enhances privacy but also increases their revenue. Tosh et al. [2015a] employ a non-cooperative information sharing game in which the firms (i.e., players) independently choose whether to participate in a *Cyber Security Information Exchange* network and share their information. The authors use *participation cost* dynamically as an incentive pricing mechanism to attract firms toward self-enforced sharing and as a charge to users to increase firms' revenue. Using an evolutionary game model, the ESS is characterized and a distributed learning heuristic is proposed to achieve ESS. However, this work only considers limited scenarios (e.g., fixed investment amount by firms). The extended version of this article is published in Tosh et al. [2017]. Tosh et al. [2015b] proposed a game-theoretic framework to investigate the economic benefits of cyber-threat information sharing and analyze the impacts and consequences of not participating in the game of information exchange. Tosh et al. [2015] study the incentives and costs behind information sharing and security investments made by the firms. Specifically, a non-cooperative game between N-firms is formulated to analyze the participating firms decisions about information sharing and security investments. The authors analyze the probability of successful cyber attack using the famous dose-response immunity model.

All of the models discussed in this subsection are related to the context of privacy information sharing. While a lot of privacy-preserving data-analytical mechanisms are invented based on the cryptographic technique, game theory is employed to guarantee the truthfulness of the participants [Kantarcioglu and Nix 2010; Wang et al. 2011; Nix and Kantarcioglu 2012; Kantarcioglu and Jiang 2013]. However, these works only tackle dishonest but not malicious behavior. In Makovian games [White et al. 2013; Park et al. 2014], investigations on several attack scenarios are based on the assumption that the player can only observe the complete state, but the research can be extended for partially observed scenarios.

5.4. Confidentiality and Integrity

Confidentiality aims to limit access or place restrictions on certain types of digital information that is controlled by the computer or/and delivered through network to the destination. The main difference between confidentiality and other security properties is that the effective defenses for confidentiality are limited to prevention, because once the attacker intrudes the system, every effort of recovery is useless. Lin et al. [2012] study the *multi-step attack-defense* scenarios in which the attack-defense on confidentiality will terminate after a finite number of actions based on an attacking graph. The defender is assumed to know the attack's manner but not the target nodes. To model the uncertainty of the target, the authors use *signaling games* where the defenders can receive alerts and update the belief about the target. Therefore, an adaptive defense strategy is proposed and the defenses are optimized repeatedly. One simple but effective way to protect information or make it more difficult for the attacker to access it is making the password harder to hack. In scarce empirical work on the implications of *password reuse*, Preibusch and Bonneau [2010] analyze password implementations across 150 free websites, explaining the technical means by which password re-use allows low-security sites that are often unmotivated to make the effort or that have experience in securing passwords to compromise high-security sites. There are two players: *security-sensitive* Web site operators that invest in security by forcing the customers to use strong passwords and *security-indifferent* Web site operators that let customers use weak passwords. Using game theory, Preibusch and Bonneau [2010] explore this question, finding that sites with the lowest security needs can endanger those with the highest.

Blocki et al. [2012] propose an *audit mechanism* to encourage the defender to adopt accountable data governance and risk management. They employ a repeated game with imperfect information to investigate how the defense entity react to an inside attacker during the audit process that is used to detect violations. The inside adversaries either gain benefit from violations they commit or suffer punishments imposed for detected violations. The defender needs to decide a level of inspection and punishment based on a budgetary plan that the defense mechanism may spend to perform the inspection process. The adversary, who may deviate to achieve a tiny benefit, can bring huge damage to the defender. Then, the authors adopt an *asymmetric* subgame perfect equilibrium as the solution for this game

Integrity aims to prevent users' information unauthorized changes. Using a legitimate authority, the information can be changed in a legitimate way. The property of integrity aims to permit user information cannot be tampered during its lifecycle. To secure cloud data centers, data integrity and availability are studied by Djebaili et al. [2014]. According to the customers' service agreement, the customers have rights to ensure that data stored in cloud are not modified. However, the storage service provider, who may experience failures occasionally, wants to hide data errors from the customer for his or her own benefit, that is, reputation. Therefore, it requires effective *verification schemes* that verify the data with the appropriate frequency for the minimum cost while maintaining accuracy and consistency of the data. This data verification game consists of two players: the defender (*verifier*) and the attacker (*cloud provider*). Given the customers' data information, the verifier chooses either to check or not to check the data integrity while the cloud provider decides either to modify or delete the data to obtain some benefit. The interaction between the two players is modeled using a static non-cooperative game that yields a Nash equilibrium as the solution.

There are still several privacy and security issues needing further investigation. We present several areas for the future direction of game theory applications in the following section.

6. FUTURE RESEARCH DIRECTIONS AND CONCLUSIONS

6.1. Future Research Directions

In previous sections, some recent security and privacy games in cyberspace are presented. However, cyber attacks evolve through time using new approaches and objectives. Cyber attackers can utilize the advantage of new Internet technologies to reach out to a vast number of victims quickly and efficiently. Possible future research directions of game-theoretic approaches for cyber security and privacy may consist of several emerging areas as follows:

(1) *Social media:* Recently, social media networks, such as Facebook and Twitter, ahave been growing explosively and are becoming the preferred method of communication. Attackers can use these sites as new media for performing insidious attacks. Because of the centralization of massive amounts of user data, *privacy protection* requires increased attention. For example, Carbunar et al. [2013] provide a survey

of privacy vulnerabilities and defensive mechanisms in *GeoSocial* networks (e.g., Foursquare, Yelp, Google Latitude). For OSN, game-theoretic approaches are proposed to enhance security and privacy protection [Park et al. 2014; White et al. 2014]. Kamhoua et al. [2012b] develop a framework that can provide trusted data management in OSN services based on game theory. Zhao et al. [2012] propose a game-theoretic framework to model and analyze colluding attackers in multimedia social networks. Griffin and Squicciarini [2012] apply a game-theoretic approach to analyze the dynamics of social identity verification protocols. There are more scenarios where online social network services are quite vulnerable and more work needs to be done to protect privacy.

(2) *Cloud computing* is arguably one of the most significant technological shifts in recent years. However, moving data to clouds poses various security and privacy challenges. Jebalia et al. [2014] use the game-theoretic approach to offer an incentive to cloud users to cooperate to revoke malicious users. The data integrity, privacy, and availability issues are solved using game theory [Anastasopoulou et al. 2013; Djebaili et al. 2014]. Kamhoua et al. [2014] employ game theory to model security and interdependency in a public cloud. Game theory also is applied to design an incentive mechanism to enforce honesty in cloud outsourcing [Nix and Kantarcioglu 2012] or to secure virtual machine allocation with the effect of negative externalities [Kwiat et al. 2015a]. For cloud computing, game theory can be a promising mathematical framework to analyze the cause and effect of cyber security and privacy issues [Furuncu and Sogukpinar 2015; Kwiat et al. 2015b; Han et al. 2016]. Kamhoua et al. [2015] apply game theory to justify the benefits of a fully Open-Implementation cloud infrastructure, which means that the cloud's implementation and configuration details can be inspected by both the legitimate and malicious cloud users. They conclude that, even though an Open-Implementation cloud may facilitate attacks, vulnerabilities or misconfigurations are easier to discover, which in turn reduces the total security threats and facilitates the cloud's provable trustworthiness. Kamhoua et al. [2015] also apply game theory for cyber-threat information sharing in the cloud. Chung et al. [2016] proposed Q-Learning as a means to react automatically to the adversarial behavior of a suspicious user to secure the system. They compared variations of Q-Learning with a traditional stochastic game. Simulation results show the possibility of Naive Q-Learning as a promising approach when confronted with restricted information on opponents.

(3) *Bitcoin* is a decentralized electronic fiat currency implemented using cryptography and peer-to-peer technology [Nakamoto 2008]. One of the challenges of Bitcoin is to design effective and secure *mining mechanisms*. Game theory can model mining as a game between all miners. To protect Bitcoin against certain adversaries, Kroll et al. [2013] apply the game-theoretic approach to analyze the incentives, stability, and governance of Bitcoin. Vasek and Moore [2014] use game theory to gain some insights into the strategies in the Bitcoin market, in which a mining pool may trigger a costly DDoS attack to a competing mining pool.

(4) *Embedded Security:* Malware attacks can happen at a single point of surface among hardware. This is the most privileged entity and provides the greatest ability to manipulate a computing system. The attacker deliberately and stealthily modifies electronic devices such as integrity circuits to create *hardware Trojans*. Kamhoua et al. [2014] model testing for hardware Trojans as a zero-sum game between malicious manufacturing attackers and the defender that tries to detect the Trojans. In Physical Embedded Systems, Wang et al. [2016] apply a repeated game to find a malicious node. approach. Kamhoua et al. [2016] apply the proposed game-theoretic approach to a real-world scenario such as System on Chip. Walid Saad et al. [2017] expanded the proposed game model based on the robust behavioral

framework of prospect theory, which allows us to capture potential uncertainty, risk, and irrational behavior in the decision making of both attacker and defender.

(5) *Cyber-insurance:* Risk management techniques are promising solutions to improve cyber security with *economic incentives* for users, policy makers, and security software vendors [Pal et al. 2014]. Several works in cyber-insurence use the game-theoretic approach to model the interaction between players in cyber market insurance, in which buying cyber-insurance is considered a defense strategy [Johnson et al. 2011; Pal et al. 2011; Yang and Lui 2012; Hayel and Zhu 2015; Chaisiri et al. 2015]. When a cyber-insurer needs to provide proportional benefits to the users of the network, game theory can derive an optimal self-defense investment strategy for the users [Pal and Hui 2012]. Although game theory can help to design mechanisms that incentivizes the insurer, more techniques are needed to answer the questions cyber-insurance will have to improve cyber security and privacy.

(6) *Internet of things (IoT):* IoT connects a huge number of smart devices that are seamlessly incorporated in networks to provide services in all aspects of human life. Since IoT is vulnerable to various attacks, researchers should focus on security and privacy of IoT applications [Rullo et al. 2016; Kumar et al. 2016; Niyato et al. 2016]. Duan et al. [2014] use a static security game to design an *energy-aware* trust derivation mechanism in WSNs for IoT applications. The authors prove that there exists a mixed Nash equilibrium and present an efficient algorithm to achieve it. Hamdi and Abie [2014] employ a Markov game-theoretic approach to tackle the adaptive security issues under dynamic contexts such as *connection*, *battery lifetime*, and *memory usage* of IoT devices. Because of rapid evolution of the technologies that will make up the IoT, new severe challenges and more serious security problems of IoT will be the prospective areas for game-theoretic approaches.

(7) *Device-to-Device Communications:* Device-to-Device communication has become a hot topic in both the academic and industrial communities, because of high throughput and low energy consumption. However, most works in the literature only focus on node discovery and resource management, for example, while the issue of security is less of concern. Although the game-theoretic approach is well known for security in distributed mobile networks, Panaousis and Alpcan [2014] and Panaousis et al. [2017] recently address three aspects (i.e., *security*, *QoS*, and *energy efficiency*) at the same time for security of packet forwarding in Device-to-Device communication. Since distributed mobile networks and Device-to-Device communication share some common technologies and models, there are several promising topics related to secure Device-to-Device communication for future research such as protecting user privacy, survivability, and security [Yang et al. 2016; Xiao et al. 2016].

6.2. Conclusions

We have been comprehensively reviewed recent applications of game theory for cyber security and privacy. Our goal is to help the reader to have a good familiarity with cutting-edge works and various game-theoretic approaches to investigate cyberspace security and privacy issues. This article differs from previous surveys by focusing on some different recent topics of cyber security and privacy. Moreover, our survey reviews updated articles and identifies current trends of using game-theoretic approaches in cyber security and privacy. Throughout this article, we review the long history of the development of some issues such as survivability, DoS, and packet forwarding, but further investigation is still needed, since communication technology is rapidly changing. We also survey recent security issues such as cyber-physical security, survivability, information sharing, and steganography, which are less reported in the literature but recently have begun to get more attention. Finally, we highlight emerging threats in cyberspace and consider them as potential future research directions for game-theoretic approaches. We realize that combining mainstream knowledge with new developments can provide a new direction of knowledge. For instance, combining network design with programming we now have software-defined networks. For security, integrating cyberspace with physical space results in cyber-physical security, or combining security with economic elements creates cyber-insurance issues. To solve security and privacy problems in a new domain, game-theoretic approaches are the most suitable tools, since they offer a variety of sets of proven mathematical methods for multi-player strategy making and they also use different forms to capture the interaction of players in privacy and security issues.

REFERENCES

Alfssandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1 (Jan. 2005), 26–33.

Rosa Karimi Adl, Mina Askari, Ken Barker, and Reihaneh Safavi-Naini. 2012. Privacy consensus in anonymization systems via game theory. In *Proceedings of the 26th Annual IFIP WG Working Conference on Data and Applications Security and Privacy*, Vol. 7371. 74–89.

Khajonpong Akkarajitsakul, Ekram Hossain, and Dusit Niyato. 2013. Cooperative packet delivery in hybrid wireless mobile networks: A coalitional game approach. *IEEE Trans. Mobile Comput.* 12, 5 (May 2013), 840–854.

Kalliopi Anastasopoulou, Theo Tryfonas, and Spyros Kokolakis. 2013. Strategic interaction analysis of privacy-sensitive end-users of cloud-based mobile apps. In *Proceedings of Human Aspects of Information Security, Privacy, and Trust*. 209–216.

Munnujahan Ara, Hugo Reboredo, Samah a. M. Ghanem, and Miguel R. D. Rodrigues. 2012. A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer. In *Proceeding of the IEEE International Conference on Communication Systems (ICCS)*. 60–64.

Gilad Asharov, Ran Canetti, and Carmit Hazay. 2011. Towards a game theoretic view of secure computation. In *Proceedings of Advances in Cryptology (EUROCRYPT)*. 426–445.

Tamer Basar. 1995. H/sup/ control of large scale jump linear systems via averaging and aggregation. In *Proceedings of the 1995 34th IEEE Conference on Decision and Control*, Vol. 3. 2574–2579.

Tamer Basar and Pierre Bernhard. 2008. *H-infinity Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach*. Springer Science & Business Media.

Harkeerat Singh Bedi, Sankardas Roy, and Sajjan Shiva. 2011. Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. In *Proceeding of IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*. 129–136.

Jeremiah Blocki, Nicolas Christin, Anupam Datta, and Arunesh Sinha. 2012. Audit mechanisms for provable risk management and accountable data governance. In *Proceedings of Decision and Game Theory for Security, GameSec*. Vol. 7638, LNCS. Springer, 38–59.

Stephan Bohacek, Joao Hespanha, Junsoo Lee, Chansook Lim, and Katia Obraczka. 2007. Game theoretic stochastic routing for fault tolerance and security in computer networks. *IEEE Trans. Parallel Distrib. Syst.* 18, 9 (Sep. 2007), 1227–1240.

S. Buchegger and J.-Y. Le Boudec. 2002. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-Based Processing*.

Levente Buttyan and Jean-Pierre Hubaux. 2001. *Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Mobile Ad Hoc Networks*. Technical Report.

Bogdan Carbunar, Mahmudur Rahman, and Niki Pissinou. 2013. A survey of privacy vulnerabilities and defenses in geosocial networks. *IEEE Commun. Mag.* 51, 11 (Nov. 2013), 114–119.

Sivadon Chaisiri, Ryan K. L. Ko, and Dusit Niyato. 2015. A joint optimization approach to security-as-a-service allocation and cyber insurance management. In *Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 426–433.

Pin-yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen. 2012. Smart attacks in smart grid communication networks. *IEEE Commun. Mag.* 50, 8 (Aug 2012), 24–29.

Tingting Chen, Liehuang Wu, Fan Wu, and Sheng Zhong. 2011. Stimulating cooperation in vehicular ad hoc networks: A coalitional game theoretic approach. *IEEE Trans. Vehic. Technol.* 60, 2 (Feb 2011), 566–579.

Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. 2009. Sensor network security: A survey. *IEEE Commun. Surv. Tutor.* 11, 2 (Jun 2009), 52–73.

Keywhan Chung, Charles A. Kamhoua, Kevin A. Kwiat, Zbigniew T. Kalbarczyk, and Ravishankar K. Iyer. 2016. Game theory with learning for cyber security monitoring. In *Proceedings of the 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*. IEEE, 1–8.

CSIS. 2014. *Significant Cyber Incidents Since 2006*. Technical Report. Retrieved from http://csis.org/files/publication/131010.

Tomáš Denemark and Jessica Fridrich. 2014. Detection of content adaptive LSB matching (a game theory approach). In *Proceeding of IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics.

Brahim Djebaili, Christophe Kiennert, Jean Leneutre, and Lin Chen. 2014. Data integrity and availability verification game in untrusted cloud storage. In *Proceedings of the Conference on Decision and Game Theory for Security (GameSec)*. 287–306.

Junqi Duan, Deyun Gao, Dong Yang, Chuan Foh, and Hsiao-Hwa Chen. 2014. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. *IEEE Internet Things J.* 1, 1 (may 2014), 58–69.

Rania El-Badry and Mohamed Younis. 2012. Providing location anonymity in a multi-base station wireless sensor network. In *Proceedings of IEEE International Conference on Communications (ICC)*. 157–161.

AbdelRahman Eldosouky, Walid Saad, Charles Kamhoua, and Kevin Kwiat. 2015. Contract-theoretic resource allocation for critical infrastructure protection. In *Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM'15)*. IEEE, 1–6.

Mark Felegyhazi, J.-P. Hubaux, and Levente Buttyan. 2006. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Trans. Mobile Comput.* 5, 5 (May 2006), 463–476.

Axel Franzen and Sonja Pointner. 2012. Anonymity in the dictator game revisited. *J. Econ. Behav. Organiz.* 81, 1 (Jan 2012), 74–81.

Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux, and David C. Parkes. 2009. On non-cooperative location privacy: A game-theoretic analysis. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*. 324–337.

Georg Fuchsbauer, Jonathan Katz, and David Naccache. 2010. Efficient rational secret sharing in standard communication networks. In *Proceeding of the 7th Theory of Cryptography Conference*, Vol. 5978 LNCS. 419–436.

Neal Fultz and Jens Grossklags. 2009. Blue versus red: Towards a model of distributed security attacks. In *Proceeding of Financial Cryptography and Data Security*. Springer, Berlin, 167–183.

Evrim Furuncu and Ibrahim Sogukpinar. 2015. Scalable risk assessment method for cloud computing using game theory (CCRAM). *Comput. Stand. Interf.* 38 (Feb. 2015), 44–50.

Tirthankar Ghosh, Niki Pissinou, and Kia Makki. 2004. Collaborative trust-based secure routing against colluding malicious nodes in multi-hop ad hoc networks. In *Proceeding of the 29th Annual IEEE International Conference on Local Computer Networks*. 224–231.

Ronen Gradwohl, Noam Livne, and Alon Rosen. 2013. Sequential rationality in cryptographic protocols. *ACM Trans. Econ. Comput.* 1, 1 (Jan. 2013), 1–37.

Christopher Griffin and Anna Squicciarini. 2012. Toward a game theoretic model of information release in social media with experimental results. In *Proceedings of the IEEE Symposium on Security and Privacy Workshops*. 113–116.

Adam Groce and Jonathan Katz. 2012. Fair computation with rational players. In *Proceeding of Advances in Cryptology (EUROCRYPT'12)*, Vol. 7237 LNCS. 81–98.

Abhishek Gupta, Cedric Langbort, and Tamer Basar. 2010. Optimal control in the presence of an intelligent jammer with limited actions. In *Proceeding of the 49th IEEE Conference on Decision and Control (CDC)*. 1096–1101.

Mohamed Hamdi and Habtamu Abie. 2014. Game-based adaptive security in the internet of things for ehealth. In *Proceeding of IEEE International Conference on Communications*. 920–925.

Yi Han, Tansu Alpcan, Jeffrey Chan, Christopher Leckie, and Benjamin I. P. Rubinstein. 2016. A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning. *IEEE Trans. Inf. Forens. Secur.* 11, 3 (Mar. 2016), 556–570.

Yezekael Hayel and Quanyan Zhu. 2015. Attack-aware cyber insurance for risk sharing in computer networks. In *Proceedings of the 6th International Conference, GameSec 2015*. 22–34.

Fei He, Jun Zhuang, Nageswara S. V. Rao, Chris Y. T. Ma, and David K. Y. Yau. 2013. Game-theoretic resilience analysis of cyber-physical systems. In *Proceedings of the 2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA)* (Aug. 2013), 90–95.

Fei He, Jun Zhuang, and United States. 2012. Game-theoretic analysis of attack and defense in cyber-physical network infrastructures. In *Proceedings of the Industrial and Systems Engineering Research Conference*.

Walter Houser. 2015. Could what happened to sony happen to us? *IT Prof.* 17, 2 (2015), 54–57.

IDC and NUS. 2014. *The Link between Pirated Software and Cybersecurity Breaches*. Technical Report. Retrieved from http://news.microsoft.com/download/presskits/dcu/docs/idc.

Anil Jade, Sanjay Kumar Madria, and Mark Linderman. 2009. Incentive based routing protocol for mobile peer to peer networks. In *Proceeding of the 10th International Conference on Mobile Data Management: Systems, Services and Middleware*. 285–292.

Maha Jebalia, Asma Ben Letaifa, Mohamed Hamdi, and Sami Tabbane. 2014. A revocation game model for secure cloud storage. In *Proceeding of IEEE International Conference on High Performance Computing & Simulation (HPCS)*. 1016–1017.

Zhu Ji, Wei Yu, and K. J. Ray Liu. 2006. Cooperation enforcement in autonomous MANETs under noise and imperfect observation. In *Proceeding of the 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*. 460–468.

Zhu Ji, Wei Yu, and K. J. Ray Liu. 2010. A belief evaluation framework in autonomous MANETs under noisy and imperfect observation: Vulnerability analysis and cooperation enforcement. *IEEE Trans. Mobile Comput.* 9, 9 (Sep. 2010), 1242–1254.

Xinyu Jin, Niki Pissinou, Sitthapon Pumpichet, Charles A. Kamhoua, and Kevin A. Kwiat. 2013. Modeling cooperative, selfish and malicious behaviors for trajectory privacy preservation using bayesian game theory. In *Proceeding of the 38th Annual IEEE Conference on Local Computer Networks*. Sydney, 835–842.

Benjamin Johnson, Rainer Bohme, and Jens Grossklags. 2011. Security games with market insurance. In *Proceedings of 2nd International Conference on Decision and Game Theory for Security*. 117–130.

Benjamin Johnson, Pascal Schöttle, and Rainer Böhme. 2012. Where to hide the bits? In *Proceedings of the Decision and Game Theory for Security, GameSec*, Vol. 7638 LNCS. 1–17.

Daniel Kahneman. 2003. Maps of bounded rationality: Psychology for behavioral economics. *Am. Econ. Rev.* 93, 5 (Nov. 2003), 1449–1475.

M. Kaliappan and B. Paramasivan. 2015. Enhancing secure routing in mobile ad hoc networks using a dynamic bayesian signalling game model. *Comput. Electr. Eng.* 41, 1 (Jan. 2015), 301–313.

Charles Kamhoua, Andrew Martin, Deepak K. Tosh, Kevin A. Kwiat, Chad Heitzenrater, and Shamik Sengupta. 2015. Cyber-threats information sharing in cloud computing: A game theoretic approach. In *Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*. IEEE, 382–389.

Charles A. Kamhoua, A. Ruan, A. Martin, and K. A. Kwiat. 2015. On the feasibility of an open-implementation cloud infrastructure: A game theoretic analysis. In *Proceedings of the 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*. 217–226.

Charles A. Kamhoua, Patrick Hurley, Kevin A. Kwiat, and Joon S. Park. 2012a. Resilient voting mechanisms for mission survivability in cyberspace: Combining replication and diversity. *Int. J. Netw. Secur. Appl.* 4, 4 (Jul. 2012), 1–20.

Charles A. Kamhoua, Kevin Kwiat, and Joon S. Park. 2012b. A game theoretic approach for modeling optimal data sharing on online social networks. In *Proceedings of the 9th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*. 1–6.

Charles A. Kamhoua, Kevin A. Kwiat, Mainak Chatterjee, Joon S. Park, and Patrick Hurley. 2013. Survivability in cyberspace using diverse replicas a game theoretic approach. *J. Inf. Warfare* 12, 2 (Jul. 2013), 27–40.

Charles A. Kamhoua, Kevin A. Kwiat, and Joon S. Park. 2012c. Surviving in cyberspace: A game theoretic approach. *J. Commun.* 7, 6 (Jun. 2012), 436–450.

Charles A. Kamhoua, Luke Kwiat, Kevin A. Kwiat, Joon S. Park, Ming Zhao, and Manuel Rodriguez. 2014. Game theoretic modeling of security and interdependency in a public cloud. In *Proceedings of the IEEE 7th International Conference on Cloud Computing*. 514–521.

Charles A. Kamhoua and Niki Pissinou. 2010. Mitigating selfish misbehavior in multi-hop networks using stochastic game theory. In *Proceedings of the IEEE Local Computer Network Conference*. 232–235.

Charles A. Kamhoua, Niki Pissinou, Alan Busovaca, and Kia Makki. 2010. Belief-free equilibrium of packet forwarding game in ad hoc networks under imperfect monitoring. In *Proceedings of the International Performance Computing and Communications Conference*. 315–324.

Charles A. Kamhoua, Niki Pissinou, and Kia Makki. 2011. Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy. In *Proceedings of the IEEE International Conference on Communications (ICC)*. 1–6.

Charles A. Kamhoua, Niki Pissinou, Kia Makki, Kevin Kwiat, and S. Sitharama Iyengar. 2012. Game theoretic analysis of users and providers behavior in network under scarce resources. In *Proceeding of the International Conference on Computing, Networking and Communications (ICNC)*. 1149–1155.

Charles A. Kamhoua, Niki Pissinou, and S. Kami Makki. 2010. Game theoretic analysis of cooperation in autonomous multi hop networks: The consequences of unequal traffic load. In *Proceedings of the IEEE Globecom Workshops*. 1973–1978.

Charles A. Kamhoua, Manuel Rodriguez, and Kevin A. Kwiat. 2014. Testing for hardware trojans: A game-theoretic approach. In *Proceedings of the 5th GameSec (Lecture Notes in Computer Science)*, Vol. 8840. Cham, 360–369.

Charles A. Kamhoua, Hong Zhao, Manuel Rodriguez, and Kevin A. Kwiat. 2016. A game-theoretic approach for testing for hardware trojans. *IEEE Trans. Multi-Scale Comput. Syst.* 2, 3 (Jul. 2016), 199–210.

Rajgopal Kannan and S. Sitharama Iyengar. 2004. Game-theoretic models for reliable path-length and energy-constrained routing with data aggregation in wireless sensor networks. *IEEE J. Select. Areas Commun.* 22, 6 (2004), 1141–1150.

Rajgopal Kannan, Srivatsan Srinivasagopalan, and S. Sitharama Iyengar. 2003. Strategic path reliability in information networks. In *Proceedings of the 14th International Conference on Game Theory*.

Murat Kantarcioglu and Wei Jiang. 2013. Incentive compatible privacy-preserving data analysis. *IEEE Trans. Knowl. Data Eng.* 25, 6 (Jun. 2013), 1323–1335.

Murat Kantarcioglu and Robert Nix. 2010. Incentive compatible distributed data mining. In *Proceedings of the 2010 IEEE 2nd International Conference on Proceeding of Social Computing (SocialCom)*. 735–742.

Jonathan Katz. 2008. Bridging game theory and cryptography: Recent results and future directions. In *Proceedings of the Theory of Cryptography Conference (TCC)*, Vol. 4948. 251–272.

Ad Ker, Patrick Bas, and Rainer Böhme. 2013. Moving steganography and steganalysis from the laboratory into the real world. In *Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security*. 45–58.

Tanmay Khirwadkar, Kien C. Nguyen, David M. Nicol, and Tamer Basar. 2010. Methodologies for evaluating game theoretic defense against DDoS attacks. In *Proceedings of the 2010 Winter Simulation Conference*. 697–707.

Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. 2013. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of the Workshop on the Economics of Information Security*. 1–21.

Sathish Alampalayam Kumar, Tyler Vealey, and Harshit Srivastava. 2016. Security in internet of things: Challenges, solutions and future directions. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 5772–5781.

Kevin Kwiat, Alan Taylor, William Zwicker, Daniel Hill, Sean Wetzonis, and Shangping Ren. 2010. Analysis of binary voting algorithms for use in fault-tolerant and secure computing. In *Proceedings of the International Conference on Computer Engineering and Systems*. 269–273.

Luke Kwiat, Charles A. Kamhoua, Kevin A. Kwiat, Jian Tang, and Andrew Martin. 2015a. Security-aware virtual machine allocation in the cloud: A game theoretic approach. In *Proceedings of IEEE Cloud Computing*.

Luke Kwiat, Charles A. Kamhoua, Kevin A. Kwiat, Jian Tang, and Andrew Martin. 2015b. Security-aware virtual machine allocation in the cloud: A game theoretic approach. In *Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing*. IEEE, 556–563.

Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo. 2013. Jamming attack on cyber-physical systems: A game-theoretic approach. In *Proceedings of the IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*. 252–257.

Xiaohui Liang, Xu Li, Tom H. Luan, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. 2012. Morality-driven data forwarding with privacy preservation in mobile social networks. *IEEE Tran. Vehic. Technol.* 61, 7 (Sep. 2012), 3209–3222.

Jingqiang Lin, Peng Liu, and Jiwu Jing. 2012. Using signaling games to model the multi-step attack-defense scenarios on confidentiality. In *Proceedings of Decision and Game Theory for Security (GameSec)*, Vol. 7638 LNCS. 118–137.

Xinxin Liu, Kaikai Liu, Linke Guo, Xiaolin Li, and Yuguang Fang. 2013b. A game-theoretic approach for achieving k-anonymity in location based services. In *Proceedings of IEEE INFOCOM*. 2985–2993.

Yuling Liu, Dengguo Feng, Yifeng Lian, Kai Chen, and Yingjun Zhang. 2013a. Optimal defense strategies for DDoS defender using bayesian game model. In *Proceedings of Information Security Practice and Experience*. 44–59.

Chris Y. T. Ma, Nageswara S. V. Rao, and David K. Y. Yau. 2011. A game theoretic study of attack and defense in cyber-physical systems. In *Proceeding of 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 708–713.

Chris Y. T. Ma, David K. Y. Yau, Xin Lou, and Nageswara S. V. Rao. 2013b. Markov game analysis for attack-defense of power networks under possible misinformation. *IEEE Trans. Power Syst.* 28, 2 (May 2013), 1676–1686.

Chris Y. T. Ma, David K. Y. Yau, and Nageswara S. V. Rao. 2013a. Scalable solutions of markov games for smart-grid infrastructure protection. *IEEE Trans. Smart Grid* 4, 1 (Mar. 2013), 47–55.

Zhanshan Sam Ma and Axel W. Krings. 2011. Dynamic hybrid fault modeling and extended evolutionary game theory for reliability, survivability and fault tolerance analyses. *IEEE Trans. Reliabil.* 60, 1 (Mar. 2011), 180–196.

George J. Mailath and Larry Samuelson. 2006. *Repeated Games and Reputations: Long-Run Relationships*.

Sonia Martinez. 2011. Stackelberg-game analysis of correlated attacks in cyber-physical systems. In *Proceedings of the 2011 American Control Conference*. 4063–4068.

Richard D. McKelvey and Thomas R. Palfrey. 2015. Erratum to: Quantal response equilibria for extensive form games (Exp Econ, DOI 10.1023/A:1009905800005). (2015).

Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. 2012. Cyber physical security of a smart grid infrastructure. *Proceedings IEEE 100* 100, 1 (Jan 2012), 195–209.

Noman Mohammed, Benjamin C. M. Fung, and Mourad Debbabi. 2011. Anonymity meets game theory: Secure data integration with malicious participants. *Int. J. Very Large Data Bases* 20, 4 (Aug. 2011), 567–588.

Maryam Mohi, Ali Movaghar, and Pooya Moradian Zadeh. 2009. A bayesian game approach for preventing DoS attacks in wireless sensor networks. In *Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing*. 507–511.

Roger B. Myerson. 1991. *Game Theory: Analysis of conict*.

Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Consulted* 1, 2012 (Oct 2008), 28–37.

Robert Nix and Murat Kantarcioglu. 2012. Contractual agreement design for enforcing honesty in cloud outsourcing. In *Proceedings of Decision and Game Theory for Security*, Vol. 7638 LNCS. 296–308.

Robert Nix and Murat Kantarciouglu. 2012. Incentive compatible privacy-preserving distributed classification. *IEEE Transactions on Dependable and Secure Computing* 9, 4 (May 2012), 451–462.

Dusit Niyato, Xiao Lu, Ping Wang, Dong In Kim, and Zhu Han. 2016. Economics of internet of things: An information market approach. *IEEE Wireless Communications* 23, 4 (Aug 2016), 136–145.

Mehrdad Nojoumian and Douglas R. Stinson. 2012. Socio-rational secret sharing as a new direction in rational cryptography. In *Proceedings of Conference on Decision and Game Theory for Security, (GameSec)*, Vol. 7638 LNCS. 1–37.

Martin J. Osborne and Ariel Rubinstein. 1994. *A Course in Game Theory*. MIT press.

Ranjan Pal, Leana Golubchik, and Konstantinos Psounis. 2011. Aegis a novel cyber-insurance model. In *Proceeding of the Second International Conference, GameSec*. 131–150.

Ranjan Pal, Leana Golubchik, Konstantinos Psounis, and Pan Hui. 2014. Will cyber-insurance improve network security? A market analysis. In *Proceedings of IEEE INFOCOM 2014*. 235–243.

Ranjan Pal and Pan Hui. 2012. CyberInsurance for cybersecurity a topological take on modulating insurance premiums. *ACM SIGMETRICS Performance Evaluation Review* 40, 3 (Jan 2012), 86–88.

Emmanouil Panaousis and Tansu Alpcan. 2014. Secure message delivery games for device-to-device communications. In *Proceedings of the Conference on Decision and Game Theory for Security (GameSec)*. 195–215.

Emmanouil Panaousis, Eirini Karapistoli, Hadeer Elsemary, Tansu Alpcan, M.H.R. Khuzani, and Anastasios A Economides. 2017. Game theoretic path selection to support security in device-to-device communications. *Ad Hoc Networks* 56 (2017), 28–42.

Joon S. Park, Sookyung Kim, Charles A. Kamhoua, and Ke A. Kwiat. 2012a. Optimal state management of data sharing in online social network (OSN) services. In *Proceeding of Trust, Security and Privacy in Computing and Communications (TrustCom)*. 648–655.

Joon S. Park, Sookyung Kim, Charles A. Kamhoua, and Kevin A. Kwiat. 2012b. Towards trusted data management in online social network (OSN) services. In *Proceedings of the IEEE World Congress on Internet Security (WorldCIS'12)*. 202–203.

Joon S. Park, Kevin A. Kwiat, Charles A. Kamhoua, Jonathan White, and Sookyung Kim. 2014. Trusted online social network (OSN) services with optimal data management. *Computers and Security* 42, 1 (May 2014), 116–136.

Viet Pham, M.H.R. Khouzani, and Carlos Cid. 2014. Optimal contracts for outsourced computation. In *Proceedings of Conference on Decison and Game Theory for Security, GameSec*. 79–98.

Sören Preibusch and Joseph Bonneau. 2010. The password game: Negative externalities from weak password practices. In *Proceedings of Conference on Decison and Game Theory for Security, GameSec*, Vol. 6442 LNCS. 192–207.

Antonino Rullo, Daniele Midi, Edoardo Serra, and Elisa Bertino. 2016. Strategic security resource allocation for internet of things. In *Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 737–738.

Walid Saad, Zhu Han, Tamer Basar, Merouane Debbah, and Are Hjorungnes. 2009. Physical layer security: Coalitional games for distributed cooperation. In *Proceeding of the 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*. 1–8.

Pascal Schottle, Aron Laszka, Benjamin Johnson, Jens Grossklags, and Rainer Bohme. 2013. A game-theoretic analysis of content-adaptive steganography with independent embedding. In *Proceedings of the 21st European Signal Processing Conference (EUSIPCO)*. Marrakech, 1–5.

Dan Shen, Genshe Chen, Erik Blasch, and George Tadda. 2007a. Adaptive markov game theoretic data fusion approach for cyber network defense. In *Proceeding of IEEE Military Communications Conference (MILCOM)*. 1–7.

Dan Shen, Genshe Chen, Jose B. Cruz, Jr., Leonard Haynes, Martin Kruger, and Erik Blasch. 2007b. A markov game theoretic data fusion approach for cyber situational awareness. In *Proceeding of SPIE Defense+ Security*, Vol. 3. 65710F–65710F.

Shigen Shen, Risheng Han, Lizheng Guo, Wei Li, and Qiying Cao. 2012. Survivability evaluation towards attacked WSNs based on stochastic game and continuous-time Markov chain. *Applied Soft Computing Journal* 12 (May 2012), 1467–1476.

Smitha Shivshankar and Abbas Jamalipour. 2014. An evolutionary game theory based approach for cooperation in VANETs under different network conditions. *IEEE Transactions on Vehicular Technology* PP, 99 (Jul 2014), 1–8.

Reza Shokri, George Theodorakopoulos, Carmela Troncoso, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. 2012. Protecting location privacy. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. 617–627.

Yasser Shoukry, Jose Araujo, Paulo Tabuada, Mani Srivastava, and Karl H. Johansson. 2013. Minimax control for cyber-physical systems under network packet scheduling attacks. In *Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems*. 93–100.

Theodoros Spyridopoulos, G. Karanikas, Theodore Tryfonas, and Georgios Oikonomou. 2013. A game theoretic defence framework against DoS/DDoS cyber attacks. *Computers & Security* 38 (Oct 2013), 39–50.

Vikram Srinivasan, Pavan Nuggehalli, Carla-Fabiana Chiasserini, and Ramesh R. Rao. 2003. Cooperation in wireless ad hoc networks. In *Proceedings of INFOCOM*, Vol. 2. IEEE, 808–817.

Vivek Srivastava and Luiz DaSilva. 2006. Equilibria for node participation in Ad Hoc networks - An imperfect monitoring approach. In *Proceedings of IEEE International Conference on Communications*. 3850–3855.

Vivek Srivastava, James Neel, A. B. Mackenzie, Rekha Menon, L. A. Dasilva, J. E. Hicks, J. H. Reed, and R. P. Gilles. 2005. Using game theory to analyze wireless ad hoc networks. *IEEE Commun. SurvTutor.* 7, 4 (Jan 2005), 46–56.

Surendran Subbaraj and Prakash Sabarimuthu. 2014. EigenTrust-based non-cooperative game model assisting ACO look-ahead secure routing against selfishness. *EURASIP J. Wireless Commun. Netw.* 78, 1 (May 2014), 1–20.

Latanya Sweeney. 2002. k-anonymity: A model for protecting privacy. *Int. J. Uncert. Fuzz. Knowl.-Based Syst.* 10, 5 (Oct. 2002), 557–570.

Symantec. 2014. *Internet Security Threats Report*. Technical Report. Symantec. Retrieved from http://www.symantec.com/threatreport/.

Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, and Ahmed Helmy. 2004. Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks. In *Proceeding of IEEE International Conference on Performance, Computing, and Communications*. 463–469.

Deepak Tosh, Shamik Sengupta, Charles A. Kamhoua, Kevin Kwiat, and Andrew Martin. 2015a. An evolutionary game-theoretic framework for cyber-threat information sharing. In *Proceeding of IEEE International Conference on Communications*.

Deepak Tosh, Shamik Sengupta, Charles A. Kamhoua, and Kevin A. Kwiat. 2017. Establishing evolutionary game models for CYBer security information EXchange (CYBEX). *J. Comput. System Sci.* (Accepted Oct. 2017).

Deepak K. Tosh, Matthew Molloy, Shamik Sengupta, Charles A. Kamhoua, and Kevin A. Kwiat. 2015. Cyber-investment and cyber-information exchange decision modeling. In *Proceedings of the 2015 IEEE 7th International Symposium on Cyberspace Safety and Security*. IEEE, 1219–1224.

Deepak K. Tosh, Shamik Sengupta, Sankar Mukhopadhyay, Charles A. Kamhoua, and Kevin A. Kwiat. 2015b. Game theoretic modeling to enforce security information sharing among firms. In *Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*. IEEE, 7–12.

Marie Vasek and Tyler Moore. 2014. Game-theoretic analysis of DDoS attacks against bitcoin mining pools. In *Financial Cryptography and Data Security*. 72–86.

Walid Saad, Anibal Sanjab, Yunpeng Wang, Charles A. Kamhoua, and Kevin Kwiat. 2017. Hardware trojan detection game: A prospect-theoretic approach. *IEEE Trans. Vehic. Technol.* (2017).

John Ross Wallrabenstein and Chris Clifton. 2013. For rational multiparty computation. In *Proceeding of Decison and Game Theory for Security (GameSec)*. 226–245.

John Ross Wallrabenstein and Chris Clifton. 2014. Realizable rational multiparty cryptographic protocols. In *Proceedings of Conference on Decison and Game Theory for Security (GameSec)*, Vol. 2014. 134–154.

Kun Wang, Miao Du, Dejun Yang, Chunsheng Zhu, Jian Shen, and Yan Zhang. 2016. Game-theory-based active defense for intrusion detection in cyber-physical embedded systems. *ACM Trans. Embed. Comput. Syst.* 16, 1 (Oct. 2016), 1–21.

Wenjing Wang, Mainak Chatterjee, and Kevin A. Kwiat. 2009. Coexistence with malicious nodes: A game theoretic approach. In *Proceedings of the 2009 International Conference on Game Theory for Networks (GameNets)*. 277–286.

Wenbo Wang, Andres Kwasinski, and Zhu Han. 2014. A routing game in cognitive radio networks against routing-toward-primary-user attacks. In *Proceeding of IEEE Wireless Communications and Networking Conference (WCNC)*, Vol. 3. 2510–2515.

Yufeng Wang, Akihiro Nakao, Athanasios V. Vasilakos, and Jianhua Ma. 2011. P2P soft security: On evolutionary dynamics of P2P incentive mechanism. *Comput. Commun.* 34, 3 (2011), 241–249.

Jonathan White, Joon S. Park, Charles A. Kamhoua, and Kevin A. Kwiat. 2013. Game theoretic attack analysis in online social network (OSN) services. In *Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. Best Paper Award, 1012–1019.

Jonathan White, Joon S. Park, Charles A. Kamhoua, and Kevin A. Kwiat. 2014. Social network attack simulation with honeytokens. *Soc. Netw. Anal. Min.* 4, 1 (Jul. 2014), 1–14.

Qishi Wu, Sajjan Shiva, Sankardas Roy, Charles Ellis, and Vivek Datla. 2010. On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks. In *Proceedings of the Spring Simulation Multiconference*. 1–8.

Yong Xiao, Dusit Niyato, Kwang-Cheng Chen, and Zhu Han. 2016. Enhance device-to-device communication with social awareness: A belief-based stable marriage game framework. *IEEE Wireless Commun.* 23, 4 (Aug 2016), 36–44.

Guanhua Yan, Ritchie Lee, Alex Kent, and David Wolpert. 2012. Towards a bayesian network game framework for evaluating DDoS attacks and defense. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS'12)*. 553–566.

Qing Yang, Kejie Lu, Vincenzo Mancuso, and Chan-Hyun Youn. 2016. Device-to-device communications with social awareness. *IEEE Wireless Commun.* 23, 4 (Aug. 2016), 10–11.

Rong Yang, Christopher Kiekintveld, Fernando Ordóñez, Milind Tambe, and Richard John. 2013. Improving resource allocation strategies against human adversaries in security games: An extended study. *Artif. Intell.* 195 (2013), 440–469.

Zichao Yang and John C. S. Lui. 2012. Security adoption in heterogeneous networks: The influence of cyber-insurance market. In *11th International IFIP TC 6 Networking Conference*. 172–183.

S. T. Zargar, James Joshi, and David Tipper. 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Commun. Surv. Tutor.* 15, 4 (Mar. 2013), 2046–2069.

Zhifang Zhang and Mulan Liu. 2011. Unconditionally secure rational secret sharing in standard communication networks. In *Proceedings of Information Security and Cryptology-ICISC*, Vol. 6829 LNCS. 355–369.

H. Vicky Zhao, W. Sabrina Lin, and K. J. Ray Liu. 2012. Cooperation and coalition in multimedia fingerprinting colluder social networks. *IEEE Trans. Multimedia* 14, 3 (Jun. 2012), 717–733.

Sheng Zhong, Jiang Chen, and Yang Richard Yang. 2003. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *Proceedings of IEEE INFOCOM*, Vol. 3. 1987–1997.

Jie Zhou and Jiannong Cao. 2012. OSR: Optimal and secure routing protocol in multi-hop wireless networks. In *Proceeding of 32nd International Conference on Distributed Computing Systems Workshops*. 187–193.

Quanyan Zhu and Tamer Basar. 2011. Robust and resilient control design for cyber-physical systems with an application to power systems. In *Proceedings of IEEE Conference on Decision and Control and European Control Conference*. 4066–4071.

Quanyan Zhu and Tamer Basar. 2012. A dynamic game-theoretic approach to resilient control system design for cascading failures. In *Proceedings of the 1st International Conference on High Confidence Networked Systems*. 41–46.

Quanyan Zhu, Ju Bin Song, and Tamer Basar. 2011. Dynamic secure routing game in distributed cognitive radio networks. In *Proceeding of IEEE Global Telecommunications Conference (GLOBECOM'11)*. 1–6.

Saman Zonouz and Parisa Haghani. 2013. Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior. *Comput. Secur.* 39 (Nov. 2013), 190–200.

Received August 2015; revised January 2017; accepted February 2017