Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 8, No. 1, March 2020, pp. 189~203
ISSN: 2089-3272, DOI: 10.11591/ijeei.v8i1.1810

A Comprehensive Insight into Game Theory in relevance to Cyber Security

Farhat Anwar[1], Burhan Ul Islam Khan[2], Rashidah F. Olanrewaju[3], Bisma Rasool Pampori[4] and Roohie Naaz Mir[5]
[1,2,3]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, IIUM Malaysia
[4]Department of Information Technology, CUK Srinagar, Kashmir, India
[5]Department of Computer Science & Engineering, NIT Srinagar, Kashmir, India

Article Info

Article history:

Received Nov 10, 2019
Revised Feb 27, 2020
Accepted Mar 4, 2020

Keywords:

Cybersecurity
Game theory
Security games
Game theory vs. cryptography

ABSTRACT

The progressively ubiquitous connectivity in the present information systems pose newer challenges to security. The conventional security mechanisms have come a long way in securing the well-defined objectives of confidentiality, integrity, authenticity and availability. Nevertheless, with the growth in the system complexities and attack sophistication, providing security via traditional means are increasingly becoming unachievable. A novel theoretical perspective and an innovative approach are thus required for understanding security from a decision-making and strategic viewpoint. One of the analytical tools which may assist the researchers in designing security protocols for computer networks is game theory. The game-theoretic concept finds extensive applications in security at different levels, including the cyberspace and is generally categorized under security games. It can be utilized as a robust mathematical tool for modelling and analyzing contemporary security issues. Game theory offers a natural framework for capturing the defensive as well as adversarial interactions between the defenders and the attackers. Furthermore, defenders can attain a deep understanding of the potential attack threats and the strategies of attackers by equilibrium evaluation of the security games. In this paper, the concept of game theory has been presented, followed by game-theoretic applications in cybersecurity, including cryptography. Different types of games, particularly those focused on securing the cyberspace, have been analysed and varied game-theoretic methodologies including mechanism design theories have been outlined for offering a modern foundation of the science of cybersecurity.

Corresponding Author:

Burhan Ul Islam Khan,
Department of Electrical and Computer Engineering,
Kulliyyah of Engineering,
International Islamic University Malaysia, Gombak, Selangor, Malaysia
Email: burhan.iium@gmail.com

1. INTRODUCTION

Modern-day communication technology, as well as information, are progressing rapidly in terms of diversity and its sophistication level. The growing connectivity, pervasiveness and complexity in the current information systems pose novel challenges to security, with the cyberspace becoming a playground for people with varying skill levels and intentions – positive or negative. Thus, the protection of assets, identities and information is gaining more and more importance since constant connectivity has become an essential part of the daily life of people [1]. Besides, the social well-being and the economic progress of a nation are increasingly becoming reliant on cyberspace. The increasing interconnectivity, as well as the rise in the computational resource availability for attackers, offers them provision for sophisticated, unpredictable and distributed attacks [2]. Attackers can, therefore, cause disruptions to critical infrastructures, including financial networks,

telecommunications, energy pipelines, electrical power, refineries, etc. [3]. Recent events reveal the damage cyber-attacks can cause to private enterprises, governments and the public in general, in terms of reputation, data confidentiality and money [4]. For more than twenty years, the research community has been paying attention to the field of cyberspace security. Nevertheless, the cybersecurity issue has still not been solved completely. In this paper, the applicability of game-theoretic methods in solving cybersecurity issues has been explored.

Contineours advancements have been accomplished by traditional security methods in the protection of well-defined goals viz. confidentiality, integrity and availability (CIA). Cryptography is one such strong theoretic security foundation that depends on the cryptographic key secrecy. But as in social engineering attacks or Advanced Persistent Threats (APTs) where attackers steal the whole cryptographic keys, the assumption of confidentiality of keys gets violated and thus leading to the penetration of the systems [1]. A novel theoretical foundation and an innovative perspective are required for capturing the scenarios where attackers can compromise systems thoroughly, and defenders can secure the systems without the fundamental key secrecy assumption.

The limitation of conventional security solutions is the non-existence of a quantitative decision framework. As such, many research groups have begun encouraging the employment of game-theoretic methods. Since game theory handles the problems where several players with opposing goals compete with one another, it can offer a mathematical framework for the modelling and analysis of network security issues.

The models based on game theory are natural frameworks for capturing the defensive as well as adversarial interaction among players [5, 6]. Game theory can offer a quantitative measure of the security quality provided using the Nash equilibrium concept where defender, as well as attacker, look for optimal strategies and none has the incentive for unilateral deviation from their equilibrium strategy regardless of their opposing security goals. This equilibrium concept further, quantitatively, predicts the security outcome of the scenario being captured by the game model. Game theory, thus, provides manageable security with its quantitative security measure, unlike the qualitative measure assured by cryptographic security. Furthermore, the game-theoretic approach can be extended to mechanism designing, allowing the system designers to shift the equilibrium as well as the predicted outcome in favour of the defender utilizing an intricate game design.

The interest in the field of game and decision theory has grown for more than a decade, and it has become a well-proven, systematic, strong theoretical foundation of the present-day security research. Game theory espouses a distinct and economic perspective of security, not the same as the standard definition, i.e., security is not the nonexistence of threats, but the stage where attacking a system is more expensive than not attacking. Therefore, beginning from the game-theoretic base attains the most sophisticated self-enforcing protection by evaluating and generating incentives for encouraging honest behaviour instead of thwarting maliciousness. Simultaneously, the economic approach to security is essential as well since it is analogous to the progression of attackers in the present day. Cybercrime has developed into a fully-featured economy with the maintenance of supply chains, black marketing and mostly resembles an illicit counterpart of the legal software market [1]. Although conventional security forms a significant base for dealing with the problem from below, game theory provides a top-down approach by the adoption of strategic and economic perspectives of the attackers as well and thus complements technological security methods. The ideal stage is attained when the two routes taken up converge towards the middle, and this is the goal of game theory.

From the survey conducted in this study, a link between various types of games and different kinds of security issues was observed. Examples include dynamic games for adaptive network security defence [7-11], multiple-layered and Stackelberg games for proactive protection [12-14], investigation of resource allocation methods using mechanism design theory for network security economics [15-19], game-theoretic examination of the concepts of cryptography – authentication and confidentiality [20, 21], network provisioning and design [22-25], quantitative management of security risks [26-30], and network games for cyber-physical protection dealing with information assurance and critical infrastructure security [31-35].

From a cybersecurity viewpoint, the latest game theory applications to various evolving topics include critical infrastructure security [8, 31, 36-38], cyber-risk management [39-42], defense of moving target [43, 44], insider threat [45, 46], cross-layer cyber physical security [32, 34, 47], adversarial machine learning [12, 48, 49] and cyber deception [11, 50, 51].

The rest of the paper is organised into various sections with Section 2 discussing the cybersecurity in detail, followed by the discussion on game theory aspects in Section 3. The relation between game theory and cybersecurity has been presented in Section 4, and the various categories of games have been elucidated in Section 5. Section 6 comprises of the illustration of varied game models that are applied in cybersecurity and Section 7 discusses the bridging of game theory and cryptography. Finally, the future research directions and concluding remarks have been given in Section 8 and 9, respectively.

2. CYBER SECURITY

Before defining cybersecurity, cyberspace needs to be determined. As per National Security Presidential Directive 54, "Cyberspace is the interdependent network of information technology infrastructures including the Internet, embedded processors, computer systems, controllers in critical industries and telecommunication networks" [52]. The social well-being and economic development of a nation are now becoming reliant on cyberspace.

Furthermore, the term ‘cyber' is also linked with various other genres such as cybergoth is associated with music; cyberpunk is a kind of novel based on fiction; cybercrime involves crimes done using computers, and cyberbullying is bullying anyone on social media or internet [53].

Cybersecurity has been defined in the Oxford English Dictionary [54] as, "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". Practically, it implies that any criminal-based or unauthorized use of electronic devices or data is regarded as a cyber threat. Manipulation of physical assets is also considered as threat to cybersecurity. Nevertheless, the connecting line between information security and cybersecurity is very thin since the issues in cybersecurity can be transformed into those of information security and vice versa in several instances. Some public sources even consider both as synonymous terms. However, cybersecurity involves human factors like people as cyber-attack targets, unlike information security [55].

European Union Agency for Network and Information Security (ENISA) considers cybersecurity as a collective term of various realms that include communication security, operation security, information security, military security and physical security [56]. The relation between the domains is shown in Figure 1.

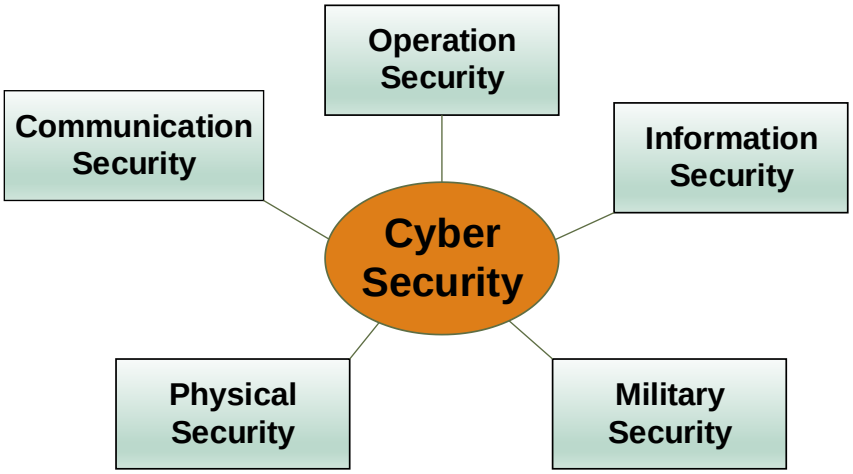

Figure 1. The connection among cybersecurity domains

The function of each of these domains is the security in respective areas. Table 1 discusses the various domains, along with their objectives in a detailed manner.

Table 1. Cybersecurity domains.

Domain	Definition
Communication Security	Security against a threat that attempts to affect the technical setup and influence specific values in a way not anticipated by the designer or owner
Operation Security	Securing against the threat that attempts to influence workflows or processes into undesirable outcomes
Information Security	Securing data saved in cyber systems against risks of deletion, manipulation or theft
Physical Security	Security against illicit use and securing physical assets of cyber systems like network components, storages or servers
Military Security	Protection against threats against physical assets but have flavours of strategic, military or political aspects

As is evident from Table 1 and Figure 1, each security domain focusses on its forte; nevertheless, in the end, all of them are linked to cybersecurity. From this perspective, cybersecurity can be understood as the umbrella term for all the security domains.

The definition of cybersecurity given in Table 1 depicts the relationship between various components. Notably, cybersecurity is not limited to technical security of the environment, but it also includes potential threat sources, assets and the fundamental elements associated with organizations such as the CIA.

Confidentiality, Integrity and Availability or CIA is a significant definition associated with cybersecurity. While defining cybersecurity policies and information security on an organizational level, the CIA is considered as a fundamental element[53].

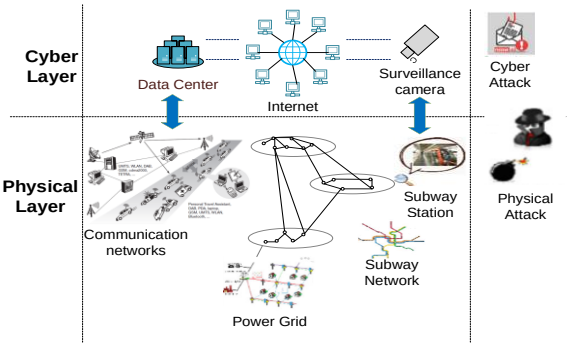

Figure 2. Interdependence of cyber network and physical systems

Figure 2 shows how cyber networks are interconnected with physical systems that comprise of crucial infrastructures like the communication network, subway and power grid. The physical system components such as subway stations can function properly only if the cross-layer nodes (like surveillance cameras and power substations) and other subway stations work correctly. This interdependent nature of the cyber-physical infrastructure paves the way for coordinated attack exploitation leveraging the susceptibilities in cyber networks and physical systems and increasing the attack probability as well as infrastructure failure rate [57]. For instance, cyberattacks can be used by a terrorist for compromising surveillance cameras of a government building, public place or an airport and planting a bomb stealthily without being sensed physically. The physical loss inflicted on the infrastructure systems may also aid the attackers in intruding into the cyber systems like control rooms and data centres. Therefore, both physical as well as cyberinfrastructure failures might lead to detrimental outcomes. Furthermore, the physical, logical and cyber connectivity of the setups leads to interdependencies and dependencies between components and nodes within and across the infrastructures. Consequently, the failure of an element might cause cascading failures in several arrangements. For mitigating these cyber-physical threats, designing effective design mechanisms is essential for hardening the physical and cybersecurity at the infrastructure nodes to secure them from failures.

Together with the development in cyberinfrastructure, cyber risks are growing at a rapid pace. The conventional cybersecurity technologies are focussed on common threats but are not meant for the infrastructures with heavy traffic. Game theory provides a better approach for dealing with cybersecurity issues than traditional security solutions.

3. ASPECTS OF GAME THEORY

Nowadays, the research community is making all the efforts possible to bring effective network security solutions to organizations; and one such resolution is the utilization of theories suitable for real-life situations for developing mitigation methods. The game theory falls in the category of one such approach that is being explored by the researchers. Over the years, researchers have been investigating the applicability of game-theoretic methods for dealing with cybersecurity; and many of those methods have been successful. Game theory helps in understanding scenarios where there is an interaction among the decision-makers in some way. In the regular sense, a game can be considered as a competitive activity in which the players compete with one another based on a distinct rule-set or the moves that have already been laid down [58].

With growing distributed and infrastructure-less systems, game theory has also found applicability in the security of decentralized communication systems viz. wireless sensor networks (WSN) [59]. Such a security scenario, involving the interaction of attacker and defender, can be precisely mapped to a game among the players where every player tries their best to increase their profit. Most importantly, game theory is perfectly suitable for such a security model since the action taken by the attacker or defender relies on the behaviour of the opposite party [60-62].

Lately, the extensive application of game theory in the field of security is categorized into security games. Besides cybersecurity, game theory has applications in many other spheres such as politics, sciences, economics, auction, finance, etc. This paper reviews the game theory applications in cybersecurity.

3.1. Definition of a game

Applying mathematical analysis of cooperative and/or individual behaviours among players selecting a specific action/strategy to fulfil their self-interests can be understood as game theory [63].

The definitions of the basic parameters of a game have been given below:

1. A *game* is defined as the strategic interaction among cooperating or opposing interests taking into account the payoffs for the actions taken by the players and constraints without revealing anything about the actual steps carried out [58].

2. A *player* is the fundamental game entity involved in a game with a finite player set (depicted by N) that take logical actions (illustrated by A_i), for every player i. A player can be a machine, a group of people or an individual in the game.
3. The *payoff/utility* is the negative or positive reward given to players for their actions in the game. It is signified as $u_i: A \rightarrow \mathbb{R}$, that measures the result for the player i based on the actions of other players $A = \times_{i \in N} A_i$, where $\mathbb{R}$ is the set of real numbers, and × indicates Cartesian product.
4. A *strategy* implies the plan of action that can be adopted by a player in the game that can be represented in the strategic/extensive form as

$$\text{Game} = \langle N, (A), (u_i) \rangle \quad (1)$$

Game theory is a description of a multi-person decision scenario as a game where every player selects an action that leads to the best reward for their ownselves while expecting logical actions from the rest of the players. A typical game, when applied to game theory, is characterized by four fundamental features, which are:

a) Two or more players
b) Competing nature
c) Rules governing each game
d) Payoffs for every player

3.2. Nash equilibrium

An important game-theoretic concept is the Nash Equilibrium that is defined as the intersection point of best responses, i.e., every player plays their best response against the actions of the rest of the players [58]. In general, Nash equilibrium is an intelligent solution to social problems that have become a favourable concept for wireless sensor network security [64, 65].

Nash equilibrium is a solution concept describing the steady-state game condition; no player would desire to modify its strategy since it may decrease their payoffs provided the rest of the players are following the stipulated policy.

However, this solution concept indicates the steady-state in the game without specifying how to reach such a state. Although various other solution concepts are utilized occasionally, Nash equilibrium is the most prominent. This information shall be employed for defining games having relevant characteristics to represent network security issues [58].

Let us assume the strategy profile for an N player game is

$$a_1, a_2, a_3, \ldots \ldots \ldots a_N^* \quad (2)$$

Where a_N^* denotes Nash equilibrium, if every player i has a payoff value u_i, then

$$u_i(a_i^*, a_{-i}^*) \geq u_i(a_i, a_{-i}^*) \quad (3)$$

Must be valid for every player i with a_i^* denoting the action profile of player i and a_{-i}^* indicating the equilibrium action of the rest of the players.

For each game, two significant concepts hold, viz. common knowledge and rationality. Common knowledge comprises of the earliest comprehension of results as well as the mutual knowledge of every player about the results. Rationality, on the other hand, specifies the consistency in decisions without taking into account the likes/dislikes of the players within the game [66].

Take into consideration a simple game – Prisoner's dilemma that involves only two players. The matrix representation of the game is given in Figure 3.

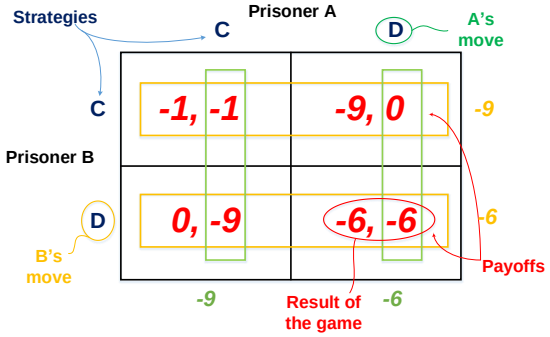

Figure 3. Matrix representation of a game

The police have arrested two people who have been accused of the possession of guns. They are suspected of having committed a crime; they both shall be put behind bars for a 6-year term if neither of them admits. But if only one of them confesses, he/she shall be freed, and the other one shall be imprisoned for nine years. Now, if both of them admit to the crime, each of them shall be jailed for a year. In such a game, the Nash

equilibrium shall be reached when both of them refuse the crime because neither has prior knowledge about their partner's action. The result of this game is depicted in Figure 3 as (-6, -6).

4. GAME THEORY AND CYBER SECURITY

The recent proliferation in cyber-attacks, as well as identity thefts, have turned the Internet into a daunting place. Cyber-attacks have generated a global threat, in securing global as well as local networks [4]. They are also threatening society since communication, and economic infrastructures primarily rely on information technology and computer networks [63].

Therefore, more effective defence strategies are a must for countering the threats caused by the rising cybersecurity concerns. In cybersecurity, game theory can help in knowing the response of the defender to the attacker and vice versa. A two-player game can be used to capture the strategic interaction between the attacker and defender in which both players try to maximize their interests. The strategy of the attacker is determined by the actions of the defender and vice versa. Therefore, a defence mechanism can be said to be valid on the basis of the strategic behaviours of the attacker and the defender. A tactical analysis can be performed by employing game theory for investigating the attacks from multiple nodes or a single node. As a result, game theory is essential for studying the strategic decision-making scenarios of defenders and analysing the attackers' incentives.

There are several aspects in which game-theoretic methods are better than the traditional approaches to cybersecurity and privacy, which have been discussed below [63]:

(1) Well-timed action: Owing to the absence of incentives for the participants, traditional security solutions are adopted rather slowly. However, game-theoretic methods back the defenders by the employment of fundamental incentive mechanisms for allocating restricted resources to even out the risks perceived.

(2) Proven mathematics: Majority of the traditional security approaches that are implemented in reactive devices like anti-virus programs or preventive tools like firewalls are dependent only on heuristics. Nonetheless, game-theoretic approaches analyse the security decisions methodically with proven mathematics.

(3) Distributed solution: The decision-making in conventional security solutions is centralized and not distributed (or individualized) in nature. Because of the absence of coordinators in autonomous systems, the centralized decision-making process is almost impossible in network security games. Thus, security solutions can be realized in a distributed way by making use of game theory.

(4) Reliable defence: The researchers can design defence strategies for robust and dependable cybersecurity systems against attacks (or selfish behaviours) based on the analytical results provided from game theory.

All the reasons as mentioned above, make game theory a suitable solution for cybersecurity problems. Nevertheless, the following issues need to be kept in mind while using game-theoretical methods for implementation in cyber systems:

(1) Multi-layer protection: In the previous works reviewed, it is observed that the defender targets a particular defence mechanism and attempts to maximize its utility by adjusting suitable parameters. Nevertheless, the presence of multiple layers of defenders providing security against the attack, that is frequently realized in the current cyber systems, is overlooked. Thus, a fitting game-theoretic approach is needed to resolve how multiple-layer defenders can offer security against attacks while implementing the defending layers simultaneously and how the other layers can be enhanced.

(2) Rationality: Most of the game-theoretic methods utilized in cybersecurity emphasize on equilibrium strategies in the action profiles of the attackers and defenders. But it is not easy for the attacker or the defender to provide the best-response actions owing to constrained rationality (in terms of restricted resources or information) in real cyber systems [67]. Thus, suitable models like Quantal Response Equilibrium and Prospect Theory are essential for predicting the behaviour of the players [68, 69]. Moreover, in the scenarios with multiple equilibria, it is not clear what the players shall select or if at all they agree to choose one.

(3) Implementation: When the defenders and attackers make decisions in real cyber systems, they take into account several factors that are real but uncertain like signal-to-noise ratio, the traffic produced in a typical network and/or the node power in wireless networks. Nevertheless, the defenders may not perceive the entire information accurately in realistic situations. Consequently, they should be able to study the environment and understand it. Besides, there are several game-theoretic methods that model security games as two-player games with multiple defenders or attackers being taken as a single entity. Two-player games are realistic models if multiple defenders or attackers have the same payoffs and strategies but might not be reasonable in a real system owing to the variety in the payoffs and strategies of defenders and attackers.

The game theory thus plays an integral part in acquiring an equilibrium strategy for surviving from unpredicted interruptions and attacks because of the interaction among users in cyber communication. Furthermore, in connection with cyber privacy, the game theory also finds applications in information sharing, anonymity, confidentiality and cryptography.

5. CLASSIFICATION OF GAMES WITH THEIR APPICATIONS IN NETWORK SECURITY

On the basis of perspectives, games can be categorized into several classes. The varied types of games have been discussed in this section below: Figure 4 represents the classification of various game models plus the security issues each class of games handles [70].

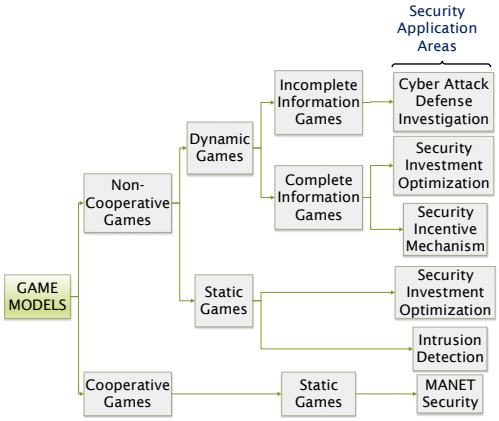

Figure 4. Classification of game models

Co-operative games: In a cooperative game, every player enforces cooperative behaviour. Such games are between the coalitions of players rather than between two players only. Cooperative games thus accentuate group efficiency, equity and rationality [71].

Non Co-operative games: In non-cooperative games, every player exhibits selfish behaviour without taking into consideration the opponents. The chief goal of every player is gain in payoffs. Non-cooperative games accentuate individual optimal decisions and individual rationality. This game type is the research goal of contemporary game theory; notably, several cybersecurity issues are non-cooperative games [71].

Strategic/Static Games: In this type of game, every player makes a one-time decision before the game begins. No player keeps the information about any other player's behaviour. Static games are one-shot games in which every player selects their plan of action, and the decisions of all the players are made at the same time [58]. This implies that whenever a plan of action is chosen by a player, no other player is informed about it.

Extensive/Dynamic Games: In dynamic games, every player has some knowledge about the behaviours of the rest of the players, unlike static games; besides, these are multi-stage games. The players in this game make decisions on the basis of the opponent's behaviour. Such games are sequential structures of the decision-making problems that the players of static games come across. The game sequences can be finite or infinite [58].

Complete Information Games: The games in which every player within the game has comprehensive knowledge about the opponents' behaviour are said to be complete information games. Every player is completely aware of all the opponents' strategies.

Incomplete Information Games: The game in which any one of the players has zero information about the opponent players. As a result, the players may not be able to make perfect strategies for winning the game.

Perfect Information Games: In this type of game, every player has the perfect knowledge of all the previous actions of the opponent player before making a move. Chess, go, and tic-tac-toe are examples of perfect information games [58].

Imperfect Information Games: In such games, there is at least one player who does not know about the past actions of the opponent player, thus making it tough for the player to make a move. Cybersecurity falls in this type of game category.

Bayesian Game: It is well-known that every outcome is valuable to every player in recreational games since the game rules quantify this. On the contrary, when real-world strategic scenarios are modelled, every player might be uncertain about the value of various outcomes to the rest of the players. Such uncertainty can be modelled naturally using Bayesian games. In Bayesian games, every player selects one 'type' from distribution

at the beginning of the game. That type determines the value of every outcome to the player. Every player has knowledge about its type but does not have any comprehension about the kind chosen by other players. Moreover, Bayesian games may be transformed into standard form, but there shall be an exponential growth in size [72]. This type of game is referred to as Bayesian, owing to the employment of Bayesian analysis in anticipating the outcome [73].

Stochastic Game: These games are multi-player generalizations of Markov decision processes. In every state, an action is chosen by all the players and the profile of actions chosen govern the instant reward to all of them together with their probabilistic transitions [72]. Thus, such games progress as a series of states beginning from a start state. Then, the players acquire a payoff after selecting their actions based on the present game state. This is followed by the transition of the game into a different state with a probability determined by the current state and actions of the players [74]. Stochastic games having just one state are referred to as repeated games in which the same normal-form game is played by the players repeatedly.

Repeated Game: As defined already, repeated games are an interaction of two players that play the game repeatedly [64]. Also known as iterative games, this game comprises of many repetitive stages, and at every step, the present action determines the next action of the players. Repeated games can be either finitely repeated or infinitely repeated. There is a fixed and known time-period in infinitely repeated games. However, it has a limitation that makes the player behave selfishly, and Nash Equilibrium is used to equal minmax payoff. The most popular type is the infinitely repeated game in which the game continues for an infinite period [59].

Zero-sum Game: It is a kind of non-cooperative game played between two players. One of the players is the maximizer since it attempts to raise its gain to the maximum and the other player is the minimizer since it tries to keep its losses to the minimum. As a result, the zero-sum game can be assumed to be a one-side win game or two-side conflict game in which the overall payoff/utility of the players stays constant throughout the game, $\sum_{i=1}^{2} u_i(s) = 0 \; \forall \; \boldsymbol{s} \in S, \boldsymbol{s}$ being the strategy profile [59].

Non-zero-sum Game: This type of game can be played by multiple players, and the sum of the payoff values of the players does not remain constant during the game [59]. So, all the game players are either maximizers or minimizers without having any constraints on the overall payoff value as is the case with zero-sum games. Thus, all the players in the game can lose or gain together [64].

Evolutionary Game: Evolutionary games are basically applied to biological networks in which pure and mixed strategies might be merged by the players with logical behaviour for enhancing the population characteristics [64]. Notably, evolutionary games have been utilized in the past to model various wireless sensor network applications [59].

Stackelberg Game: Stackelberg games are used for modelling two competing players where one of the players is the initiator (or leader) of the game who opts an action from a specific set A_1, and the other player follows the action of the leader to choose later a move from a different set A_2[59]. Such a situation is prevalent for protecting various wireless sensor networks where the attacker acts as the follower, and the defender plays the role of the leader [75, 76].

A distinctive category of games called security games analyse the interaction between defenders and malicious attackers. These games, along with their solutions, form the base of algorithm development and formal decision-making besides the prediction of the behaviour of the attackers. Moreover, security games find vast applications to security issues like intrusion detection and privacy in computer, wireless and vehicular networks [77].

6. GAME-THEORETICAL METHODS FOR CYBER SECURITY APPLICATIONS

From the perspective of game-theoretic applications in cybersecurity, there are six categories of security applications:

6.1. Physical layer security

It is an evolving area of security. Eavesdropping and jamming attacks are commonplace on the communication channel of networks [70]. Notably, these attacks are more alarming for wireless networks in comparison to wired networks.

In this regard, a game-theoretic model was introduced by authors in [78] for examining the communication between the source transmitting valuable data and some available jammers who aid the source in puzzling the eavesdroppers. Those jammers charge some cost from the source for their service and then there is a price trade-off. Stackelberg game has been put forward by the authors plus a distributed algorithm for investigating the result of the game to display the effectiveness of the price trade-off and the friendly jamming service.

6.2. Self-organized network security

A specific application of game theory is the design of security protocols for self-organized networks like mobile adhoc networks (MANETs), wireless sensor networks or vehicular networks. Due to the relatively static configuration and homogenous architecture of self-organized networks, the behaviour of the network tends to be like that of a reasonable decision-maker or a logical economic man, therefore making it consistent with the game theory requirements.

Several previous works take into account only two players in their game models when applying game theory to security. But it might not be practical in case of MANETs that have no centralized administration. In the scenarios with multiple players, a robust mathematical tool is mean-field game theory. In [79], authors have employed the contemporary developments in mean-field game theory for proposing a new game theory-based distributed approach for MANET security with multiple players. Such an approach allows a distinct MANET node to make decisions of strategic defence, and every node needs the knowledge of its state together with the cumulative effect of the rest of the nodes in the MANET.

6.3. Intrusion detection and prevention

Intrusion detection is considered to be one of the most broadly applied security research areas in terms of game theory owing to its attack and defence characteristic [70]. With the study of game models, it is possible to optimize the distributed design as well as security configuration of intrusion detection systems. In this regard, defence strategies based on puzzles have been put forth against flooding attacks

An automated intrusion response engine has been introduced by authors in [80] that is referred to as Response and Recovery Engine (RRE). This engine makes use of game-theory based response strategies to ward off intruders that are displayed as opponents in a two-player stochastic Stackelberg game with RRE and the attacker attempting to raise their benefits to the maximum by considering the response actions and the optimal opponent respectively. There are many research-works that utilize game theory for intrusion detection as well as prevention. For instance, a collaborative incentive-based game-theoretic method has been designed for intrusion detection in [81], another game theory model has been proposed in [82] for the detection of cooperative intrusion over multiple packets, a protracted Dirichlet based collaborative IDS based on game theory has been given in [83], and authors in [84] present a game-theoretic approach to configure large scale intrusion detection signature dynamically.

6.4. Privacy preservation and anonymity

From the perspective of game theory, privacy can be evaluated by the users, and various strategies can be inspected for their desired privacy level setting. Game theory can prove beneficial in analysing the privacy preservation economically and in finding the best compromise between performance and privacy. Several effective location-based services bring convenience to the users but at the cost of the privacy of users. Authors in [85] have been the first to put forward an optimal mechanism that finds the location besides preserving user privacy in location-based service. The Stackelberg Bayesian games are used for modelling the mutual optimization of localization accuracy vs location privacy, and it has been proven that this methodology showed better results in comparison to a direct obfuscation mechanism. Furthermore, the interaction among data collectors, data users and data providers have been modelled in [86] using a game and a general methodology for finding Nash equilibrium.

6.5. Economics of cyber security

Since the game theory was set up initially in the theoretical framework of economics, it can be applied chiefly to cybersecurity economics. Various standard economic models and theories find applications to the economic perspective of security like security policy making, security incentive and security investment. Securing the network infrastructure against attacks is a must because the attacks on high-speed data links could cause a delay or loss of large-scale data.

In the works [87, 88], authors have studied the incentive mechanism in network security by investigating the network externality that is produced by the price of anarchy (POA) and selfish investment behaviour. They have proved that network security can be improved dramatically by enhancing incentive mechanisms of cybersecurity investment rather than by the enhancement in security preservation methods.

6.6. Cloud computing security

Cloud computing is a thriving industry and a well-known concept of information processing. Still, its security problem is complicated due to the use of varied infrastructure elements in every service model [70]. The conventional security mechanisms are not apt for cloud computing because novel cloud concepts like

outsourcing, resource-sharing and multi-tenancy are challenging to the security research community. But game theory can make a difference in this issue.

Different public cloud users share a common platform such as the hypervisor. This universal platform intensifies the well-known problem of cybersecurity interdependency, and a user who does not invest in cybersecurity imposes a negative externality on others. This is one of the reasons that many large organizations with sensitive information have been reluctant to join a public cloud.

A framework has been put forward by authors in [10] known as FlipIt game for cloud security that provides details about when devices should trust the cloud hypervisor's commands. This communication is modelled as a game with the device, attacker and the defender as the players. A game theoretic-security risk assessment model has been proposed in [89] for cloud computing that is scalable such that it is assessed if the system risks should be fixed by tenant or cloud provider. Authors in [90] have modelled the problem of cloud security transparency as a non-cooperative dynamic game in which the client and provider are modelled as the game players. Consequently, authors have presented a theoretical examination for the client or provider to compute the best strategy for reaching the Nash equilibrium.

7. BLENDING GAME THEORY AND CRYPTOGRAPHY

Both game theory and cryptographic protocols deal with the analysis of interactions among mutually suspecting parties. Historically, both the fields have evolved independently of each other within diverse research communities and thus are likely to have different flavours. Nevertheless, there has been growing interest in merging the approaches and techniques of these fields that were inspired by the desire for developing more pragmatic protocols and models of such an interaction. The present research at the relation of cryptography and game theory can be divided into two categories: applying game-theoretic models to cryptographic protocol design and applying cryptographic protocols to the problems based on game theory.

Conventionally, the protocols in cryptography are devised, assuming that a few participants are authentic and follow the protocols faithfully while other participants are malicious and act haphazardly. However, the game-theoretic perception is that every participant is rational and acts according to its best interest. Such a perspective is different from the cryptographic one, according to which the protocol need not avert to irrational behaviour although no one can be trusted to follow the protocol unless it acts in the participant’s best interests.

In general, cryptography focusses on guaranteeing that the parties continue to use the authorized service and game-theoretic approach has the same goal. Game-theoretic methods are used for devising incentive mechanisms that aim to avert diversion. An important motive to apply the game-theoretic method in cryptography is the modelling of malicious behaviour of the user. The rationale behind this is that malicious actions are not only more challenging to control than rational actions, but it is also more common and practical for some parties to follow the cryptographic protocol dishonestly. For enhancing the security and efficiency of cryptographic protocols, many new terminologies and approaches have been proposed by researchers. For instance, socio-rational secret sharing, employment of Perfect Bayesian Equilibrium (PBE) or utilization of point-to-point channels rather than trusted mediators. Also, game-theoretic methods have been used in steganography and have proved to be ideal in allowing researchers to assess several design choices like distribution of payload in batch steganography or distortion functions in adaptive steganography. All these approaches exhibit the huge benefit that blending of cryptography and game theory brings in designing defence mechanisms.

8. FUTURE RESEARCH DIRECTIONS

Possible future research directions of game-theoretic approaches for cybersecurity and privacy may consist of several emerging areas as follows:

8.1. Social media

In recent times, social media sites, for instance, Twitter and Facebook, have been emerging as excellent ways of communication. These sites can be used by attackers as novel media for conducting insidious attacks. Owing to the massive centralized user data, increased attention should be paid to privacy protection. The application of game theory to social media can help us identify the objectives of social media users and how they work to achieve them. Based on formalized utilities of security policies and security rules, the choice of security policies in content access is described as a game between the content provider and the content requester.

8.2. Cloud computing

Debatably, cloud computing is assumed to be one of the essential technological shifts in recent times. Nevertheless, while shifting data to clouds, various challenges to security and privacy are posed. Game theory is a potential mathematical framework for analyzing the effects and causes of privacy and integrity issues for

cloud computing [89]. Authors in [91] have put forward methods for reacting automatically to the opponent's behaviour for securing the system through Q-Learning. The researchers, after comparing Q-Learning with the conventional stochastic game, presented simulation results that affirm Naive Q-Learning as a potential approach on confrontation with limited information about adversaries.

8.3. Bitcoin

Bitcoin is an electronic decentralized fiat currency that is implemented through peer-to-peer technology and cryptography. The designing of secure and effective mining methods is one of the challenges faced by bitcoins. Minigas, a game, can be modelled among all users through game theory.

8.4. Embedded security

At a single point, attacks of malware can occur in the hardware. It's the most beneficial entity which provides the ability for manipulating a computing system. The attackers secretly and deliberately bring modification to electronic devices like integrity circuits for creating hardware Trojans. Game theory is the mathematical treatment of conflict, thus could be utilised for strategically guiding microcircuit testing to balance the risk posed by hardware Trojans.

8.5. Cyber-insurance

Techniques of risk management for improving cybersecurity are promising solutions with economic benefits for security software vendors, users and policymakers. The game-theoretic approaches have been employed in various cyber insurance research works for modelling the interactions among the players of cyber market insurance where the retail of cyber-insurance is taken as a defence mechanism. Though game theory may assist in designing mechanisms incentivizing the insurers, more methods are required for answering the questions that cyber insurance poses for improving cybersecurity and privacy.

8.6. Internet-of-Things (IoT)

IoT provides connection among numerous smart devices integrated in networks seamlessly for offering services in every aspect of human life. Being susceptible to varied attacks, the research community needs to emphasize on the privacy as well as the security of IoT applications. Due to the speedy development in technology making up the IoT, several new crucial problems and significant security issues in IoT shall be the potential topics for game-theoretic methods.

8.7. Device-to-Device communications

Device-to-Device (D2D) is emerging as a new trend in industrial as well as academic communities due to the economic energy consumption and high throughput. It is expected to be a key feature supported by next-generation cellular networks. D2D can extend the cellular coverage allowing users to communicate when telecommunications infrastructure is highly congested or absent. Various potential topics in relevance to D2D communication such as secure transmission, enhanced quality-of-service and energy efficiency can be considered utilizing the utility function maximization game frameworks.

9. CONCLUSION

Game theory has been found to play a vital role in numerous security situations and has been extensively applied in cybersecurity. The latest research works conducted reveal the effective use of game theory in web security, network security, etc. Game theory allows the defender to assess the security quantitatively and predict the security outcome in addition to offering a mechanism design tool for enabling security-by-design and reversing the advantage of the attacker. Games can be analysed and designed; players' optimal moves can be utilized for determining how effectively security can be approached in the cyber world. However, an essential game-theoretic issue is the ability to find a feasible mathematical solution to the game problem. More systematic solutions that solve the problem of cybersecurity utilizing game theory are recommended which involve practical mathematical solutions. One such approach that is presently being studied by the research community is the employment of linear programming. Furthermore, integer programming can be delved into for offering a more pragmatic solution to distributed denial of service attacks in the cyber world.

ACKNOWLEDGMENTS

This work was supported by the Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under the Fundamental Research Grant Scheme (FRGS) number FRGS19-137-0746 (Ministry Project ID: FRGS/1/2019/ICT03/UIAM/01/2). The authors express their personal appreciation for the effort of Saiyara Shehnaz in proof-reading and editing the paper.

REFERENCES

[1] Q. Zhu and S. Rass, "Game Theory Meets Network Security: A Tutorial", in *CCS '18: 2018 ACM SIGSAC Conference on Computer & Communications Security*, October 15-19, 2018, Toronto, ON, Canada, J. B. Sartor, T. D'Hondt, and W. De Meuter (Eds.), ACM, New York, NY, USA, Article 4, p. 4, 2018.

[2] B. Gourley, "Cloud Computing and Cyber Defense", Crucial Point LLC, March 2009.

[3] D.C. Blair, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence: Testimony Before the Committee*. DIANE Publishing, 2009.

[4] S. Shiva, D. Dasgupta and Q. Wu, "Game Theoretic Approaches to Protect Cyberspace", Final Technical Report, Department of Computer Science University of Memphis, Memphis, TN, USA, p. 86, 2010.

[5] B.U.I. Khan, R.F. Olanrewaju, M.M.U.I. Mattoo, A.A. Aziz and S.A. Lone, "Modeling Malicious Multi-Attacker Node Collusion in Manets via Game Theory", *Middle-East Journal of Scientific Research*, vol. 25, no. 3, pp. 568-579, 2017.

[6] B.U.I. Khan, R.F. Olanrewaju, F. Anwar, A.R. Najeeb and M. Yaacob, "A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 832-842, November 2018.

[7] S. Farhang, M.H. Manshaei, M. N. Esfahani, and Q. Zhu, "A Dynamic Bayesian Security Game Framework for Strategic Defense Mechanism Design", in *Decision and Game Theory for Security*, Springer, 2014, pp. 319–328.

[8] L. Huang, and Q. Zhu, "Adaptive Strategic Cyber Defense for Advanced Persistent Threats in Critical Infrastructure Networks", *ACM SIGMETRICS Performance Evaluation Review*, vol. 46, no. 2, pp. 52-56, 2019.

[9] L. Huang, and Q. Zhu, "Analysis and Computation of Adaptive Defense Strategies Against Advanced Persistent Threats for Cyber-Physical Systems", in *International Conference on Decision and Game Theory for Security*, Springer, Cham, 2018, pp. 205-226.

[10] J. Pawlick, S. Farhang, and Q. Zhu, "Flip the Cloud: Cyber-physical Signaling Games in the Presence of Advanced Persistent Threats", in *Decision and Game Theory for Security*, Springer, 2015, pp. 289–308.

[11] T. Zhang, and Q. Zhu, "Strategic Defense Against Deceptive Civilian GPS Spoofing Of Unmanned Aerial Vehicles", in *International Conference on Decision and Game Theory for Security*, Springer, 2017, pp. 213–233.

[12] J. Pawlick, and Q. Zhu, "A Stackelberg Game Perspective on the Conflict Between Machine Learning and Data Obfuscation", in *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on*, IEEE, 2016, pp. 1–6.

[13] Q. Zhu, H. Tembine, and T. Basar, "Hybrid learning in stochastic games and its applications in network security", *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control*, pp. 305–329, 2013.

[14] Q. Zhu, Z. Yuan, J.B. Song, Z. Han, and T. Başar, "Interference aware routing game for cognitive radio multi-hop networks", *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 2006–2015, 2012.

[15] W.A. Casey, Q. Zhu, J.A. Morales, and B. Mishra, "Compliance control: Managed vulnerability surface in social-technological systems via signaling games", in *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*, ACM, 2015, pp. 53–62.

[16] J. Chen and Q. Zhu, "Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach", *IEEE Transactions on Information Forensics and Security*, 2017.

[17] Y. Hayel and Q. Zhu, "Attack-aware Cyber Insurance for Risk Sharing in Computer Networks", in *Decision and Game Theory for Security*. Springer, 2015, pp. 22–34.

[18] Y. Hayel, and Q. Zhu, "Epidemic protection over heterogeneous networks using evolutionary poisson games", *IEEE Transactions on Information Forensics and Security 12*, no. 8, pp. 1786–1800, 2017.

[19] R. Zhang, Q. Zhu, and Y. Hayel, "A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks", *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 779–794, 2017.

[20] S. Rass and P. Schartner, "A Unified Framework for the Analysis of Availability, Reliability and Security, With Applications to Quantum Networks", *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews 41*, no. 1, pp. 107–119, 2011.

[21] S. Rass and P. Schartner, "Information-Leakage in Hybrid Randomized Protocols", in *Proceedings of the International Conference on Security and Cryptography (SECRYPT)*, J. Lopez and P. Samarati, Eds., SciTePress – Science and Technology Publications, 2011, pp. 134–143.

[22] S. Rass, "On Game-Theoretic Network Security Provisioning", *Springer Journal of Network and Systems Management*, vol. 21, no. 1, pp. 47–64, 2013.

[23] S. Rass, "Complexity of Network Design for Private Communication and the P-vs-NP question", *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 2, 2014, pp. 148–157.

[24] S. Rass, B. Rainer, M. Vavti, and S. Schauer, "A Network Modeling and Analysis Tool for Perfectly Secure Communication", in *Proceedings of the 27th IEEE International Conference on Advanced Information Networking and Applications (2013)*, IEEE Computer Society Press, pp. 267–275.

[25] S. Rass, B. Rainer, M. Vavti, J. Göllner, A. Peer and S. Schauer, "Secure Communication over Software-Defined Networks. Mobile Networks and Applications", vol. 20, no. 1, 2015, pp. 105-110.

[26] S. Rass and S. Schauer, (Eds.), Game Theory for Security and Risk Management: From Theory to Practice, Springer: Birkhäuser, 2018.

[27] S. Rass, and B. Rainer, "Numerical Computation of Multi-Goal Security Strategies", in *Decision and Game Theory for Security*, R. Poovendran and W. Saad, Eds., LNCS 8840, Springer, 2014, pp. 118–133.

[28] S. Rass, S. König and S. Schauer, "On the Cost of Game Playing: How to Control the Expenses in Mixed Strategies", in *Decision and Game Theory for Security*, Springer, [S.l.], 2017, pp. 494–505.
[29] S. Rass, S. König, and S. Schauer, "Uncertainty in Games: Using Probability Distributions as Payoffs: 346–357", in *Decision and Game Theory for Security, 6th International Conference, GameSec 2015*, M. H. Khouzani, E. Panaousis, and G. Theodorakopoulos, Eds., LNCS 9406, Springer, 2015.
[30] S. Rass, and S. König, "Password Security as a Game of Entropies", *Entropy,* vol. 20, no. 5, pp. 312, 2018.
[31] L. Huang, J. Chen, and Q. Zhu, "A Large-Scale Markov Game Approach to Dynamic Protection of Interdependent Infrastructure Networks", in *International Conference on Decision and Game Theory for Security*, Springer, 2017, pp. 357–376.
[32] F. Miao, Q. Zhu, M. Pajic and G.J. Pappas, "A Hybrid Stochastic Game for Secure Control of Cyber-Physical Systems", *Automatica,* vol. 93, pp. 55–63, 2018.
[33] S. Rass, S. Alshawish, A. Abid, M. A. Schauer, S. Zhu, and H. de Meer, "Physical Intrusion Games - Optimizing Surveillance by Simulation and Game Theory", *IEEE Access 1*, 2017.
[34] Z. Xu, and Q. Zhu, "Secure and Practical Output Feedback Control for Cloudenabled Cyber-Physical Systems", in *Communications and Network Security (CNS), 2017 IEEE Conference on*, IEEE, 2017, pp. 416–420.
[35] Z. Xu, and Q. Zhu, "A Game-Theoretic Approach to Secure Control of Communication-Based Train Control Systems Under Jamming Attacks", in *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*, ACM, 2017, pp. 27–34.
[36] J. Chen, C. Touati, and Q. Zhu, "A dynamic game analysis and design of infrastructure network protection and recovery", *ACM SIGMETRICS Performance Evaluation Review*, vol. 45, no. 2, 128, 2017.
[37] J. Pawlick, and Q. Zhu, "Proactive Defense Against Physical Denial of Service Attacks Using Poisson Signaling Games", in *International Conference on Decision and Game Theory for Security*, Springer, 2017, pp. 336–356.
[38] S. Rass, A. Alshawish, M.A. Abid, S. Schauer, Q. Zhu, and H. De Meer, "Physical Intrusion Games–Optimizing Surveillance By Simulation And Game Theory", *IEEE Access 5*, pp. 8394–8407, 2017.
[39] J. Chen, and Q. Zhu, "Security Investment Under Cognitive Constraints: A Gestalt Nash Equilibrium Approach", in *Information Sciences and Systems (CISS), 2018 52nd Annual Conference on*, IEEE, 2018, pp. 1–6.
[40] C.J. Fung and Q. Zhu, "Facid: A Trust-Based Collaborative Decision Framework for Intrusion Detection Networks", *Ad Hoc Networks 53*, pp. 17–31, 2016.
[41] Y. Hayel, and Q. Zhu, "Epidemic Protection Over Heterogeneous Networks Using Evolutionary Poisson Games", *IEEE Transactions on Information Forensics and Security 12*, no. 8, pp. 1786–1800, 2017.
[42] R. Zhang, Q. Zhu, and Y. Hayel, "A bi-level game approach to attack-aware cyber insurance of computer networks", *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 779–794, 2017.
[43] H. Maleki, S. Valizadeh, W. Koch, A. Bestavros, and M. van Dijk, "Markov Modeling of Moving Target Defense Games", in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, ACM, 2016, pp. 81–92.
[44] Q. Zhu, and T. Başar, "Game-theoretic Approach to Feedback-Driven Multi-Stage Moving Target Defense", in *International Conference on Decision and Game Theory for Security*, Springer, 2013, pp. 246–263.
[45] W. A. Casey, Q. Zhu, J.A. Morales and B. Mishra, "Compliance Control: Managed Vulnerability Surface in Social-Technological Systems Via Signaling Games", in *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*, ACM, 2015, pp. 53–62.
[46] W. Casey, J.A. Morales, E. Wright, Q. Zhu, and B. Mishra, "Compliance Signaling Games: Toward Modeling the Deterrence of Insider Threats", *Computational and Mathematical Organization Theory*, vol. 22, no. 3, pp. 318–349, 2016.
[47] Q. Zhu, and S. Rass, "On Multi-Phase and Multi-Stage Game-Theoretic Modeling of Advanced Persistent Threats", *IEEE Access 6*, pp. 13958–13971, 2018.
[48] R. Zhang, and Q. Zhu, "A Game-Theoretic Approach to Design Secure and Resilient Distributed Support Vector Machines", *IEEE transactions on neural networks and learning systems,* vol. 29, no. 11, pp. 5512-5527, 2018.
[49] W. Wang and Q. Zhu, "On the Detection Of Adversarial Attacks Against Deep Neural Networks", in *Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense*, ACM, 2017, pp. 27–30.
[50] K. Horák, Q. Zhu, and B. Bošansk`y, "Manipulating Adversary's Belief: A Dynamic Game Approach to Deception By Design For Proactive Network Security", in *International Conference on Decision and Game Theory for Security*, Springer, 2017, pp. 273–294.
[51] J. Pawlick, E. Colbert, and Q. Zhu, "Modeling and Analysis of Leaky Deception Using Signaling Games with Evidence", *IEEE Transactions on Information Forensics and Security,* vol. 14, no. 7, pp. 1871-1886, 2018.
[52] G. Bush, "National Security Presidential Directive 54: Cybersecurity Policy", 2008.
[53] V. Sulkamo, "IoT from Cyber Security Perspective Case Study JYVSECTEC", Master's thesis, Master's Degree Programme in Cyber Security, June 2018.
[54] English Oxford Living Dictionaries. N.d. Accessed 27 August 2019. Retrieved from https://en.oxforddictionaries.com/definition/cybersecurity.
[55] R. Von Solms, and J.V. Niekerk, "From Information Security to Cyber Security", *Computers & Security,* vol. 38, no. 2013, pp. 97-102, 2013.
[56] European Union Agency for Network and Information Security (ENISA). 2015. Definition of Cybersecurity. Gaps and overlaps in standardisation. Accessed 23 August 2018. Retrieved from https://www.enisa.europa.eu/publications/definition-of-cybersecurity.
[57] L. Huang, J. Chen, and Q. Zhu, "Factored Markov Game Theory for Secure Interdependent Infrastructure Networks", Springer International Publishing AG, part of Springer Nature, S. Rass, S. Schauer (eds.), *Game Theory for Security and Risk Management*, Static & Dynamic Game Theory: Foundations & Applications, 2018, pp. 99-126.

[58] A.E. Chukwudi, E. Udoka and I. Charles, "Game Theory Basics and Its Application in Cyber Security", *Advances in Wireless Communications and Networks,* vol. 3, no. 4, pp. 45-49, 2017.
[59] M.S. Abdalzaher, K. Seddik, M. Elsabrouty, O. Muta, H. Furukawa, and A. Abdel-Rahman, "Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey", *Sensors,* vol. 16, no. 7, pp. 1003, 2016.
[60] P. Guan, and J. Zhuang, "Modeling Resources Allocation in Attacker-Defender Games with "Warm Up" CSF", *Risk Analysis,* vol. 36, no. 4, pp. 776-791, 2016.
[61] N.S.V. Rao, S.W. Poole, C.Y.T. Ma, F. He, J. Zhuang, and D.K.Y. Yau, "Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models", *Risk Analysis,* vol. 36, no. 4, pp. 694-710, 2016.
[62] J. Xu, and J. Zhuang, "Modeling Costly Learning and Counter-Learning in a Defender-Attacker Game with Private Defender Information", *Annals of Operations Research,* vol. 236, no. 1, pp. 271-289, 2016.
[63] C.T. Do, N.H. Tran, C. Hong, C.A. Kamhoua, K.A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S.S. Iyengar, "Game Theory for Cyber Security and Privacy", *ACM Computing Surveys (CSUR),* vol. 50, no. 2, pp. 30, 2017.
[64] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge university press, 2012.
[65] H.Y. Shi, W.L. Wang, N.M. Kwok, and S.Y. Chen, "Game Theory for Wireless Sensor Networks: A Survey", *Sensors,* vol. 12, no. 7, pp. 9055-9097, 2012.
[66] M.J. Osborne, *An introduction to game theory*, vol. 3, no. 3. New York: Oxford university press, 2004.
[67] A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making", *IEEE Security & Privacy* 3, no. 1, pp. 26–33, 2005.
[68] R.D. McKelvey, and T.R. Palfrey, "Erratum to: Quantal Response Equilibria for Extensive Form Games", *Experimental Economics,* vol. 18, no. 4, pp. 762-763, 2015.
[69] R. Yang, C. Kiekintveld, F. OrdóñEz, M. Tambe, and R. John, "Improving Resource Allocation Strategies Against Human Adversaries in Security Games: An Extended Study", *Artificial Intelligence,* vol. 195, pp. 440-469, 2013.
[70] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A Survey of Game Theoretic Methods for Cyber Security", in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, IEEE, 2016, pp. 631-636.
[71] A. P. Patil, S. Bharath, N. M. Annigeri, "Applications of Game Theory for Cyber Security System: A Survey", *International Journal of Applied Engineering Research,* vol. 13, no. 17, pp. 12987-12990, 2018.
[72] V. Conitzer, "Computing Game-Theoretic Solutions and Applications to Security", in *Twenty-Sixth AAAI Conference on Artificial Intelligence*. 2012.
[73] R.F. Olanrewaju, B.U.I. Khan, F. Anwar, R.N. Mir, M. Yaacob and T. Mehraj, "Bayesian Signaling Game Based Efficient Security Model for MANETs", *Advances in Information and Communication,* Springer Nature Switzerland AG, pp. 1-17, 2019.
[74] A. Gueye, "A Game Theoretical Approach to Communication Security." PhD diss., UC Berkeley, 2011.
[75] X. Tang, P. Ren, Y. Wang, Q. Du and L. Sun, "Securing Wireless Transmission Against Reactive Jamming: A Stackelberg Game Framework", in *Proceedings of the Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, 6–10 December 2015, pp. 1–6.
[76] E. Karapistoli and A.A. Economides, "Defending Jamming Attacks In Wireless Sensor Networks Using Stackelberg Monitoring Strategies", in *Proceedings of the IEEE/CIC International Conference on Communications in China (ICCC)*, Shanghai, China, 13–15 October 2014; pp. 161–165.
[77] M.H. Manshaei, Q. Zhu, T. Alpcan, T. Basar and J.P. Hubaux, "Game Theory Meets Network Security and Privacy", *ACM Comput. Surv.,* vol. 45, no. 3, Article 25, June 2013, p. 39.
[78] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical Layer Security Game: Interaction Between Source, Eavesdropper, and Friendly Jammer", *EURASIP Journal on Wireless Communications and Networking* 2009, pp. 1-10, 2009.
[79] Y. Wang, F. Yu, H. Tang, and M. Huang, "A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad Hoc Networks." *IEEE Trans. on Wirel. Commun*., vol. 13, no. 3, pp. 1616-1627, 2014.
[80] S. Zonouz, H. Khurana, W. Sanders, and T. Yardley, "RRE: A Game-Theoretic Intrusion Response and Recovery Engine", *IEEE Trans. On Parallel and Distributed Systems,* vol. 25, no. 2, pp. 395-406, 2014.
[81] Q. Zhu, R. Boutaba and T. Basar, "GUIDEX: A Game-Theoretic Incentive-Based Mechanism for Intrusion Detection Networks," *IEEE J. on Selected Areas in Commun.*, vol. 30, no. 11, pp. 2220-2230, 2012.
[82] P. Chakraborty, K. Majumder and A. Dasgupta, "A Game Theoretic Model to Detect Cooperative Intrusion Over Multiple Packets," *Proc. ICAIECES*, Springer: India 2016, pp. 895-907.
[83] S. Paul et al., "Extended Game Theoretic Dirichlet Based Collaborative Intrusion Detection Systems," *Proc. Computational Intelligence, Cyber Security and Computational Models,* Springer, 2016.
[84] X. Punithan, J. Kim, D. Kim, and Y. Choi, "A Game Theoretic Model for Dynamic Configuration of Large-Scale Intrusion Detection Signatures," *Multimedia Tools and Applications,* pp. 1-17, 2015.
[85] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.P. Hubaux, and J.Y.L. Boudec, "Protecting Location Privacy: Optimal Strategy Against Localization Attacks", in *Proceedings of the 2012 ACM conference on Computer and communications security,* ACM, 2012, pp. 617-627.
[86] L. Xu, C. Jiang, J. Wang, Y. Ren, J. Yuan, and M. Guizani, "Game Theoretic Data Privacy Preservation: Equilibrium and Pricing", in *2015 IEEE International Conference on Communications (ICC)*, IEEE, 2015, pp. 7071-7076.
[87] L. Jiang, V. Anantharam, and J. Walrand, "How Bad are Selfish Investments in Network Security?", *IEEE/ACM Transactions on Networking,* vol. 19, no. 2, pp. 549-560, 2010.

[88] M. Lelarge, "Coordination in Network Security Games: A Monotone Comparative Statics Approach", *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2210-2219, 2012.
[89] E. Furuncu, and I. Sogukpinar, "Scalable Risk Assessment Method for Cloud Computing Using Game Theory (CCRAM)", *Computer Standards & Interfaces*, vol. 38, pp. 44-50, 2015.
[90] A. Aldribi, and I. Traore, "A Game Theoretic Framework for Cloud Security Transparency", in *International Conference on Network and System Security*, Springer, Cham, 2015, pp. 488-500.
[91] K. Chung, C. A. Kamhoua, K. A. Kwiat, Z. T. Kalbarczyk and R. K. Iyer, "Game Theory with Learning for Cyber Security Monitoring", in *Proceedings of the 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, IEEE, 2016, pp. 1–8.

BIOGRAPHY OF AUTHORS

Dr. Farhat Anwar received a PhD degree in Electronic and Electrical Engineering from the University of Strathclyde UK in 1996. His research interest includes QoS in IP networks, routing in ah-hoc and sensor networks, computer and network security, network simulation and performance analysis, IoT, and biometrics. He has published extensively in international journals and conferences. He has been with IIUM since 1999 and currently working as a Professor in the Department of Electrical and Computer Engineering.

Burhan Ul Islam Khan is a Ph.D. Scholar and Teaching Assistant at the Department of Electrical & Computer Engineering, International Islamic University Malaysia. He received B.Tech. in CSE from IUST, Kashmir, and MS in CIE from IIUM, Kuala Lumpur during 2011 and 2014 respectively. Before commencing his Ph.D., he has been involved in varying roles as that of Software Engineer, Research Analyst and Assistant Professor. His current research interests include Formulation of Bio-Inspired optimization models in IoT, Designing One Time Password Schemes, Employing Mechanism Design and Game theory to protect ad-hoc networks.

Rashidah Funke Olanrewaju is a Nigerian citizen, born in Kaduna, Nigeria. She received the BSc. Hons degree in Software Engineering from the University of Putra Malaysia, in 2002, and the MSc and PhD degrees in Computer & Information Engineering from the International Islamic University Malaysia (IIUM) Kuala Lumpur, in 2007 and 2011, respectively. She is currently an Associate Professor at the Department of Electrical and Computer Engineering, International Islamic University Malaysia where she is leading the Software Engineering Research Group (SERG). She is an executive committee member of technical associations like IEEE Women in Engineering, Arab Research Institute of Science and Engineers, etc. She represents her university, IIUM, at Malaysian Society for Cryptology Research. Her current in hand projects revolve around: MapReduce Optimization Techniques, Compromising Secure Authentication and Authorization Mechanisms, Secure Routing for ad-hoc networks, Formulating Bio-Inspired Optimization Techniques.

Bisma Rasool Pampori completed her M. Tech in Information Technology and B. Tech in Computer Science & Engineering from Islamic University of Science & Technology, Kashmir and Central University of Kashmir, Kashmir respectively.

Roohie Naaz Mir is a Professor & HoD in the Department of Computer Science & Engineering at NIT Srinagar, India. She received B.E. (Hons) in Electrical Engineering from University of Kashmir (India) in 1985, M.E. in Computer Science & Engineering from IISc Bangalore (India) in 1990 and PhD from University of Kashmir, (India) in 2005. She is a Fellow of IEI and IETE India, senior member of IEEE and a member of IACSIT and IAENG. She is the author of many scientific publications in international journals and conferences. Her current research interests include reconfigurable computing and architecture, mobile and pervasive computing, blockchain technology, security and routing in wireless ad-hoc and sensor networks.