2016 IEEE First International Conference on Data Science in Cyberspace

A Survey of Game Theoretic Methods for Cyber Security

Yuan Wang, Yongjun Wang, Jing Liu, Zhijian Huang and Peidai Xie
College of Computer
National University of Defense Technology
Changsha, China
{wangyuan, wangyongjun, liujing0111, zjhuang, xiepeidai}@nudt.edu.cn

Abstract—**Cyber security has been heavily studied in both industry and academia, but the traditional security technology is still facing unprecedented challenges in the background of massive and complicated network traffic. Game theory as a mathematical model of conflict and cooperation between intelligent rational decision-makers has great potential to improve cyber security. This paper describes a focused literature survey of game theoretic methods for cyber security applications. The methods are classified according to their security application scenarios, and we also present their advantages and limitations respectively. Then we discuss the difficulties and challenges confronting researchers, and in addition, we propose some directions for further research on game theory as applied to cyber security from both the mathematics perspective and security perspective.**

Keywords-cyber security; game theory; cyber attack and defense; security assessment; Nash equilibrium

I. Introduction

Computer networks have profoundly changed people's daily life in many areas, such as business, entertainment, healthcare and education, etc. The network, especially the Internet, has brought great convenience to people, and also increasingly serious security threats. A variety of cyber security incidents in recent years, causing serious consequences, demonstrates the importance of cyber security, especially with the expansion of network forms and network convergence. As cyber-crime seriously threatens national security and the economy of many industries, how to understand and solve the cyber security problem is an important issue in the process of social informationization.

Traditional cyber security technology, which depends on the firewall, intrusion detection and anti-virus software, is more for a specific attack scenario or method. These static and unilateral passive security defense tend to lag behind to attacks. Additionally, the traditional cyber security solutions are lack of quantitative analysis and decision framework. In response to this problem, game theoretic methods has been applied to cyber security issues by a growing number of researches in recent years [1]-[4]. Game theory shares many common concerns with the cyber security problem. In game theory, game player's payoff depends on both his own decisions and other player's behaviors. Similarly, the cyber security situation depends not only on the security strategies and defense implementations, but also on the attacker's strategies and even other network users' behaviors in the system. Based on this similarity, game theory has provided a mathematical tool to strictly descript and analyze these complex multi-agent competitive behaviors. At present, the game theory has been applied to the analysis of cyber attack-defense, the cyber security assessment, the network reliability measurement and the security policy [2].

In this paper we present a survey of game theoretic methods that have been applied to improve cyber security. These different game theory methods are classified according to their security application scenarios, and compared to discuss their advantages and limitations. In addition, we also propose some recommended directions for further research on cyber security from both the mathematics perspective and security perspective. This survey is differs from the existing surveys such as [3] and [4] in the following ways. First, our survey is not restricted to only computer communication networks but all forms of cyberspace. Second, we survey the methods both from the mathematical theory perspective and the security application perspective.

The remainder of the paper is structured as follows. Section II gives some background of game theory. Section III introduces the relationship between game theory and cyber security while Section IV discusses different game theory methods applied to cyber security. Conclusion and discussion for future research are given in Section V.

II. Overview of Game Theory

Game theory is a mathematical discipline which studies situations and models of competition and cooperation between several involved individuals or entities. Game theory was developed based on the assumption that the players are rational, and for whatever circumstance, or for whatever game, there exists a strategy that will make one player to win the game. Game theory is wildly used in social science such as economics, politics and psychology, as well as nature science such as logic, biology, and computer science. Game theory is one of the best mathematical tool for the science of logical decision making in humans, animals and computers, especially when dealing with a situation that involves several entities whose decisions are influenced by what decisions they expect from other entities [5], [6].

A. Basic Difinitions

There are several essential elements exist in any game at least including: players, actions, strategies and payoff functions. With these elements we can describe a game [6].

978-1-5090-1192-6/16 $31.00 © 2016 IEEE
DOI 10.1109/DSC.2016.90

Players: The game players are the individuals or entities who make decisions having their own goals and preferences involved in a game. These entities can be people, institutions, animals, or any other things that can interact with each other. The players are rational, that is to say, the players know well about their own goal and interests, and each player's goal is to maximize his utility by choice of actions.

Actions: An action by a player is a choice he can make. In each move of a player, he takes an action. Game theory assumes that each player knows the possible actions of every other player.

Payoff Functions: Payoff is a concept that refers to the amount of satisfaction that a player derives from an object or an event. At the end of the game, all players have taken actions, and each one will get either a negative or a positive return. This return of each player is his payoff.

Strategies: A player's strategy is simply a predetermined plan of actions that guides a player as to what actions to take specifically in response to past and expected actions from other players in the game.

If above four elements have been identified, a game is described by a set of rational players, the strategies associated with the players, and the payoffs for the players, and then the basic framework of the game is formed. An equilibrium in a game is a set of mixed strategies, one for each player, and each player's strategy is the best response to the strategies of the other players so that no player can change his strategy and get a better payoff. Nash equilibrium was proposed by John Nash in 1950s, and Nash proved that every normal-form game has a Nash equilibrium, which laid the foundation of modern non-cooperative game theory.

B. Classification of Games

There are many kinds of games, and from the different perspective, games can be classified into categories in different ways [5], [6].

Non-cooperative and cooperative games. A game is called non-cooperative, if the actions of each individual player are considered and each player is assumed to be selfish, just for improve its own payoff and not taken into account other players involved in the game. Alternatively, a cooperative game is a game where groups of players may enforce cooperative behavior, hence the game is a competition between coalitions of players, rather than between individual players. Non-cooperative game emphasizes individual rationality and individual optimal decision, while cooperative game emphasizes the group rationality, efficiency and equity. Non-cooperative game is the research focus of modern game theory, many cyber security problems in reality is a non-cooperative game.

Static games and dynamic games. In static game (or strategic game) the players make their own decisions simultaneously at the beginning of the game, and it is a one-shot game that the players have no information about the actions of the other players in the game. The prisoner's dilemma and the battle of the sexes are both classic static games. The dynamic game (or extensive game) is a game consisting of multiple stages or moves, in this form players have some information about the decision of other players and the players can make decisions during the game and they can react to other players' actions too.

Perfect information games and imperfect information games. A game is a perfect information game if each player knows all of the previous actions of all other players when he takes his move. Alternatively, if at least one player does not know all information about other players' actions when it is her turn to decide, it is imperfect information game. As it is hardly ever any user knows the exact actions of the others in the complicated cyberspace, the imperfect information game seems like the more suitable framework for cyber security.

Complete information games and incomplete information games. In a complete information game all elements of the game are public knowledge to all players, so each individual player is fully aware of all other players, their strategy spaces and all the payoff functions of each player. Otherwise, in the incomplete information games, at least one player does not know all players' payoff functions, which made him not able to predict the effect of their actions on others.

III. Game Theory Meets Cyber Security

Game theory has been developed in the framework of mathematical economics at first, and as a powerful analysis tool has been used in microeconomics. Then it has been widely applied in various disciplines as mathematical model to solve the competition and conflict problems.

A. Game Theory and Cyberspace

As strategic decision making model, game theory techniques were adopted to solve a lot of protocol design issues in communication networks, especially to analysis of resource allocation among heterogeneous agents in networks. Routing involves multiple agents' competition, so in wired network, game theory is widely used to research selfish routing, and to optimize the routing algorithm for better routing protocol design [7]. As the network congestion problem is essentially about competition and interaction, game theory is also a powerful tool on this issue. With the emergence of wireless network and its wide applications, game theory get the more extensive and in-depth application compared to the wired network, such as the communications channel contention, the abolition of the network nodes and the optimization of network resource allocation[7]. Because of the usually homogeneous architecture of the wireless network and its fixed configuration to some extent, the network behaviors tend to be "rational", and the application of game theory in wireless network can achieve better result.

B. Game Theory and Cyber Security

The network, especially the Internet has become an important part of daily life and an essential tool today. At the same time, cyber security has become a serious problem, and game theory has been applied to network security by security analysts [2]. The application of game theory in cyber security can be generally divided into two categories: the cyber attack-defense analysis and the cyber security assessment. Cyber attack-defense analysis predicts the actions of the cyber attackers through modeling the attack and defense behaviors as games, and analyzes the possible states of

TABLE I. GAME THEORETIC METHODS FOR CYBER SECURITY

Game models			Security issues
Cooperative game models	Static game models		mobile ad hoc networks security
Non-cooperative game models	Static game models		intrusion detection
			security investment optimization
	Dynamic game models	Complete information game models	security investment optimization
			security incentive mechanism
		Incomplete information game models	cyber attack-defense analysis

attack-defense equilibrium. Based on the ideal state of equilibrium, the responding defense strategy can be determined. The analysis to the equilibrium state of cyber attack-defense and the predication of the attack and defense strategies can be also used as the basis of cyber security and reliability assessment. Due to the quantitative characteristic of game analysis, the security and reliability assessment is a quantitative evaluation and such assessment also gives a measurement of cyber security and reliability.

The game models that has been applied to cyber security are briefly described in Table I. From the game model perspective, the game applications for cyber security mainly adopt a non-cooperative game model, which is determined by the attack-defense competitive feature of cyber security. Earlier researches on non-cooperative game are almost all based on static models. Due to the dynamic characteristic of the network, for behavior analysis the static model is very difficult to achieve the ideal effect. However, for the economic problems of cyber security such as security protection investment and defense resource allocation can be analyzed by static game models. The game theoretic researches on cyber security mainly adopts dynamic game models at present, closer to the reality of cyber security. More specifically, complete information game models are more used in security investment optimization and incentive mechanism, while incomplete information game models are more applied in cyber attack-defense analysis.

IV. GAME THEORETIC METHODS FOR CYBER SECURITY APPLICATIONS

From the security application scenario perspective, the applications of game theory in cyber security can be divided into following six categories.

A. *Physical Layer Security*

Physical layer security is an emerging security area. Communication channels of the network may suffer from jamming and eavesdropping attacks. In particular, compared to wired networks these attacks are of a greater concern for the wireless networks.

Han et al. [8] introduce a game theoretic approach to investigate the interaction between the source that transmits the useful data and some friendly jammers who give assistance to the source by confusing the eavesdropper. The friendly jammers charge the source with a certain price for the jamming service, and so there is a tradeoff for the price. A Stackelburg type of game is proposed and a distributed algorithm is constructed to analyze the game outcome to show the effectiveness of friendly jamming and the tradeoff for setting the jamming service price.

In [9] the authors investigate the problem of secure communication between secondary users (SUs) and their serving base station in the presence of multiple eavesdroppers and multiple primary users. They use the non-cooperative game to model and analyze the interactions between the SUs and eavesdroppers. A novel algorithm of secure channel selection is proposed to make sure that the SUs and eavesdroppers take distributed decisions so as to reach a Nash equilibrium point. Simulation results show that this approach yields significant improvements of at least 32.7% relative to a classical spectrum sharing scheme and enables the SUs to reach Nash equilibrium with up to 86.5% less computation than other standard learning algorithms.

B. *Self-Organized Network Security*

The typical application of game theory for security in self-organized networks (SON) is using game-theoretic approaches to design security protocols for SONs such as vehicular networks, wireless sensor networks, or mobile ad hoc networks (MANETs). Because of the homogeneous architecture of the SONs and its fixed configuration to some extent, the network behaviors mode tend to be more like a rational economic man and a rational decision maker, thus more in line with the requirements of game theory.

Many previous researches on applying game theories to security only consider two players in the security game model: an attacker and a defender, while unfortunately this assumption may be not realistic in MANETs without centralized administration. For problems with a large number of players, the mean field game theory provides a powerful mathematical tool. Wang et al. [10] use recent advances in mean field game theory to propose a novel game theoretic distributed approach with multiple players for security in MANETs. The proposed fully distributed approach enable an individual node in MANETs to make strategic defense decisions without centralized administration and each node only needs to know its own state information and the aggregate effect of the other nodes in the MANET.

In wireless mobile networks, to ensure the authenticity of messages and the identity of network nodes, digital signature has been widely employed. But signature verification tend to cause increase of verification delay and adverse the network QoS. The batch cryptography technology would somehow mitigate this negatively impact. In [11], the authors propose a Game-theory-based Batch Identification Model (GBIM), which enables nodes to discover invalid signatures with the optimal delay under heterogeneous and dynamic attack scenarios. An incomplete information game model is designed between a verifier and its attackers, and the existence of Nash Equilibrium has been proved. In addition, an auto-match protocol to optimize the identification algorithm selection is proposed, when the attack strategies can be estimated based on history information.

C. Intrusion Detection and Prevention

In terms of game theory, intrusion detection is one of the most extensively applied research areas in security because of its attack-defense interactive characteristic. With the game model analysis, the security configuration and distributed design of intrusion detection systems can be optimized.

Puzzle-based defense mechanisms have been proposed against flooding attacks. In [12], game theory is utilized to propose a series of optimal client puzzle-based strategies for defense against sophisticated flooding attack scenarios. The interactions between a flooding attacker and a defender using a puzzle-based defense can be modeled as an infinitely repeated game of discounted payoffs, and the solutions of the game are used to find the defense solutions, then the optimal puzzle-based defense strategies are developed and four defense mechanisms are proposed.

In [13] a Bayesian game model based evaluation framework for Distributed Denial-of-Service (DDoS) attack and defense is presented. Previous methods has been mostly conducted in a static environment and previous game-theoretic models typically formulated DDoS attacks and defense as a static game. The authors use random variables and Bayesian networks to describe the state of attack and defense, which greatly improves the complexity of the scenario. The Level-K thinking theory in economics is introduced to analyze attack and defense entities with different level reasoning ability. Simulation shows that defense parameters seemingly unrelated with the attacker will ultimately affect the attacker's strategy choice and different levels of defense approach can be replaced with each other, that is to say, the deployments of all available defense approaches against DDoS attacks is not necessary.

In [14] an automated intrusion response engine is proposed, called the response and recovery engine (RRE). The RRE employs a game-theoretic response strategy against intruders modeled as opponents in a two-player Stackelberg stochastic game in which the attacker and RRE try to maximize their own benefits by taking optimal adversary and response actions, respectively. Using Snort's alerts, RRE efficiently takes appropriate countermeasure actions against ongoing attacks and can protect large networks for which attack-response trees have more than 500 nodes.

There are lots of other works which employ game theory for intrusion detection or prevention, such as in [15] a collaborative game-theoretic incentive-based mechanism for intrusion detection is designed, in [16] a game theoretic model to detect cooperative intrusion over multiple packets is proposed, in [17] an extended game theoretic Dirichlet based collaborative IDS is presented, and in [18] Punithan et al. employ a game theoretic model for dynamic configuration of large-scale intrusion detection signatures.

D. Privacy Perservation and Anonymity

Prom the game theory perspective, users should evaluate their privacy and inspect different strategies to set their privacy at their desired level. Game theory can be helpful to economic analysis of privacy preservation, and to find the best compromise between the privacy and the performance.

A variety of successful location-based services (LBSs) has brought a lot of convenience to us, but come with a cost of users' privacy. In [19], the authors propose the first methodology that enables a designer to find the optimal location-privacy preserving mechanism for a LBS. The mutual optimization of location privacy vs. correctness of localization is modeled by using the Stackelberg Bayesian games, and it is proved that this optimal mechanism is better than a straightforward obfuscation method.

Anonymous networking is an effective way to preserve network users' privacy. Providing anonymity in a network is hard to avoid reducing the achievable network performance. Therefore it is necessary to find the optimal set of nodes to modify transmission schedules so that anonymity is maximized without reducing too much QoS. In [20], the problem of optimizing anonymity is posed as a two-player zero-sum game between the network designer and the adversary. The authors present a game-theoretic formulation and proved the existence of saddle-point equilibria, and prove that this approach can be used to obtain optimal strategies for the two players, as well as provide insights into anonymity–throughput tradeoffs in large networks.

To protect data providers' privacy, the data collector usually performs anonymization on the data, usually causing a decline of data utility. So how to make a trade-off between privacy protection and data utility is important. In [21], the interactions among data providers/collector/user are modeled as a game, and a general approach to find the Nash equilibriums of the game is proposed.

E. Economics of Cyber Security

As game theory has been developed in the theoretical framework of economics at first, game theory has been most prominently applied to the economics of cyber security. Many classic economics theories and models can be applied to some economical problem of security such as security investment, security incentives and security policy making.

It is important to protect the network infrastructure from attacks, since the attack on the high speed data link will lead to the loss or delay of large scale data. In [22], it is investigated that for ISP, by pre allocating limited security resources, how to protect the network infrastructure from attacks, no matter where the attacker will launch them. The game model is a two-player zero-sum game, and the payoff function are measured by the maximum network flow. It is proved that a global Nash equilibrium (NE) exists when there is only one critical region, but when more than one, there is no global NE. To solve this problem, a mixed-strategy solution has been designed. Final results show that, when there are multiple min-cut sets, to dedicate all defending resources to one of the min-cut sets will not be an optimal solution; nevertheless, when the defending resource is limited, min-cut strategies will have higher probabilities to be selected in the mixed-strategy solution.

Both in [23] and [24] the authors by analyzing the externality of the network caused by the selfish investment behaviors in security and the price of anarchy (POA), study the incentive mechanism of network security, and prove that improving the incentive mechanism of cyber security investment can enhance the security of the network more effectively compared with the improving cyber security preservation techniques. In [23], the author employ both strategic game and repeated game to study how users' preference and mutual dependency affect network security in a non-cooperative setting. Finally it is shown that technology improvement alone may not offset the POA due to the lack of incentives. Xiao et al. [24] study the question of incentive alignment for agents of a large scale network towards a better security. It is shown that risk-neutral agent do not invest more than 37% of the expected loss under log-convex security breach probability functions. If a security game where agents anticipate the effect of their actions on the security level of the network, in all cases, the fulfilled equilibrium is not socially efficient, and alignment of incentives typically leads to a coordination problem.

F. Cloud Computing Security

Cloud computing is very popular information processing concepts and thriving industry and its security issue is complicated because each service model uses different infrastructure elements. Traditional security models are not suitable to cloud computing. The new concepts introduced by clouds such as multi-tenancy, resource sharing and outsourcing pose new challenges to the security researchers. But on this issue, game theory can make some difference.

Different public cloud users share a common platform such as the hypervisor, this common platform intensifies the well-known problem of cyber security interdependency, and a user who does not invest in cyber security 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. In [25] the authors use the game theory framework to analyze the cause and effect of interdependency in a public cloud platform. They shows that although there are multiple possible Nash equilibria of the public cloud security game, the players use a specific Nash equilibrium profile depending on the probability that the hypervisor is compromised given a successful attack on a user and the total expense required to invest in security. There is no Nash equilibrium in which all the users in a public cloud will fully invest in security. In [26] the authors propose a security-aware virtual machine (VM) allocation approach in the public cloud using game theory. They show that there are multiple Nash equilibria for the public cloud security game and we can allow the players' Nash equilibrium profile to not be dependent on the probability that the hyper visor is compromised, reducing the factor externality plays in calculating the equilibrium. It is proved that using this allocation method, the negative externality imposed onto other players can be brought to a minimum compared to other common VM allocation methods.

In [27], the authors present a framework, called FlipIt game, for the cloud systems security that specifies when a device should trust commands from the cloud hypervisor which may be compromised. This interaction is considered as a game of three players: a defender, an attacker, and a device. In [28] a scalable security risk assessment model is proposed for cloud computing using game theory, so it can be evaluated that whether the risk in the system should be fixed by cloud provider or tenant of the system. In [29] the cloud security transparency problem is modeled as a dynamic non-cooperative game theoretic problem, whereby the provider and client are modelled as the players in the game. Finally a theoretical analysis through which the provider or client can compute his best strategy to reach the Nash equilibrium is presented.

V. Conclusion and Discussion

As has been described in this paper game theory has been widely and extensively researched for cyber security and the application of game theory to cyber security is being an active and promising research field. However, in order to make game theory a viable and practicable approach for analyzing and solving cyber security problems, there are still a lot of challenges need to be addressed. The most prominent challenge is the gap between the fantastic results of theoretic analysis versus the lack of actionable security solutions.

A. Problems and Challenges

First of all, in the game modeling and analysis, defining the payoff function is the key procedure, but unfortunately it is usually the most difficult procedure. The definition of payoff function must be reasonable according to practical security situation; meanwhile, in mathematics it is not only needed to ensure the existence of the equilibrium point, but also to satisfy the convex condition and other more tough conditions [6]. So how to construct the payoff function both to accurately express the realistic situation and to strictly meet the mathematical condition requirements is still a big challenge in game modeling for cyber security.

Secondly, most of the existing game models are based on the assumption of finite state space [5]. Nevertheless, the strategy spaces of many cyber security problem is infinite. In this situation, researchers have to reluctantly use a series of finite state spaces as the approximations and substitutions of finite ones, and get the unsatisfied results. The same goes for unperfected information problem and the incomplete information problem. These problems thirst for not only the new techniques and skills of applications but also the developments and improvements of the game theory itself.

Thirdly, game modeling as a quantitative analysis method need to quantify some security parameters such as risk, privacy and reputation, and it is necessary for the game theoretic method to define payoff functions for both attackers and defenders [2]. But computing an exact quantification of these security parameters is sometimes impossible. More efforts are needed to be spent to understanding and quantification the economics of the cyber security.

At last, computing an equilibrium of a game is generally not a cakewalk, and the computational complexity of the Nash equilibrium of a security game is yet a big challenge. The proof of existence of Nash equilibrium is logical rather than constructive, and there is not a standard method for the computing a Nash equilibrium of a game. However, if we want the game model to be instructive for security practice, it is needed to know what exactly the Nash equilibrium is. In

[30] it is shown that computing a Nash equilibrium is a PPAD-complete problem, still an intractable problem.

B. Recommendations for Further Research

Although many game theoretic methods have been developed and applied to cyber security by the research community, there are still a number of open research issues and challenges. Besides the further research on the challenges mentioned before, the followings are some recommendations one needs to be mindful of when developing a game theoretic methods for cyber security.

The Nash equilibrium is essentially a Brouwer fixed point in mathematics, and the stability of fixed points is a crucial issue [31]. Stability means that the system's stable state do not change too much under small perturbations of the system initial state or the system parameters. As applied to cyber security scenario, only the stable Nash equilibrium is significant. In the game model for cyber security, network status and parameters could not be completely accurate, but a specific approximation of the practical state to some extent. Relatedly, in a game model the Nash equilibrium is not unique, on the contrary, there is a set of fixed points. Therefore, we are facing with serious problems: based on the practical security scenario, how to analyze the stability of these fixed points and how to make the choice of one or more Nash equilibriums from these fixed points as the solution of the model? Nevertheless, the relevant research results are still very few as far as we can see.

In addition, the game theoretic methods in cyber security often use the existing economic models, which are usually classic and old, sometimes naive. How to introduce the latest developments and findings in the economics especially in the game theory into the research of cyber security is an interesting issue that deserves more attention.

Acknowledgment

This work is partially supported by the National Natural Science Foundation of China (Nos. 61472439, 61271252).

References

[1] S. Roy and C. Ellis, "A Survey of game theory as applied to network security," Proc. 43rd Hawaii Int'l Conf. on System Sciences, 2010.

[2] T. Alpcan and T. Basar, Network Security: A Decision and Game-Theoretic Approach, Cambridge: Cambridge University Press, 2011.

[3] X. Liang and Y. Xiao, "Game theory for network security," IEEE Commun. Surveys Tutorials, 15(1): 472-486, 2013.

[4] M. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J. Hubaux, "Game theory meets network security and privacy," ACM Computing Surveys, 45(3): 1-39, 2013.

[5] R. Gibbons, Game Theory for Applied Economists, Princeton: Princeton University Press, 1992.

[6] G. Owen, Game Theory, New York: Academic Press, 3rd ed., 2001.

[7] I. Menache and A. Ozdaglar, "Network Games: Theory, Models, and Dynamics," Synthesis Lectures on Communication Networks, 2011.

[8] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," EURASIP J. Wirel. Commun. Netw., 2009.

[9] A. Houjeij, W. Saad, and T. Bascar, "A game-theoretic view on the physical layer security of cognitive radio networks," Proc. IEEE ICC, 2013.

[10] 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., 13(3): 1616-1627, 2014.

[11] J. Chen, Q. Yuan, G. Xue and R. Du, "Game-theory-based batch identification of invalid signatures in wireless mobile networks," Proc. IEEE Conference on Computer Communications, 2015.

[12] M. Fallah, "A puzzle-based defense strategy against flooding attacks using game theory." IEEE Trans. on Dependable and Secure Computing 7(1): 5-19, 2010.

[13] G. Yan and R. Lee, "Towards a bayesian network game framework for evaluating DDoS attacks and defense," Proc. ACM CCS, 2012.

[14] 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, 25(2): 395-406, 2014

[15] 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., 30(11): 2220-2230, 2012

[16] P. Chakraborty, K. Majumder and A. Dasgupta, "A game theoretic model to detect cooperative intrusion over multiple packets," Proc. ICAIECES, Springer India: 895-907, 2016.

[17] S. Paul et al., "Extended game theoretic Dirichlet based collaborative intrusion detection systems," Proc. Computational Intelligence, Cyber Security and Computational Models, Springer, 2016.

[18] 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: 1-17, 2015

[19] R. Shokri et al., "Protecting location privacy Optimal strategy against localization attacks," Proc. ACM CCS, 2012.

[20] P. Venkitasubramaniam and L. Tong, "A game-theoretic approach to anonymous networking," IEEE/ACM Trans. on Netw., 20(3), 2012.

[21] L. Xu et al. "Game theoretic data privacy preservation: Equilibrium and pricing," Proc. IEEE ICC, 2015.

[22] X. Xiao, M. Li, J. Wang, and C. Qiao, "Optimal resource allocation to defend against deliberate attacks in networking infrastructures," Proc. IEEE INFOCOM, pp. 639-647, 2012.

[23] L. Jiang et al., "How bad are selfish investments in network security," IEEE/ACM Trans. on Networking, Vol.19, No.2, April 2011.

[24] M. Lelarge, "Coordination in network security games: a monotone comparative statics approach," IEEE Journal of Selected Areas in Commun., December 2012.

[25] C. Kamhoua et al., "Game theoretic modeling of security and interdependency in a public cloud," Proc. IEEE 7th Int'l Conf. on Cloud Computing, 2014.

[26] L. Kwiat et al., "Security-aware virtual machine allocation in the cloud: a game theoretic approach," Proc. IEEE 8th Int'l Conf. on Cloud Computing, 2015.

[27] J. Pawlick et al., "Flip the cloud: cyber-physical signaling games in the presence of advanced persistent threats," Proc. 6th Int'l Conf. on Decision and Game Theory for Security, November, 2015.

[28] E. Furuncu and I. Sogukpinar (2015). "Scalable risk assessment method for cloud computing using game theory," Computer Standards & Interfaces, 38: 44-50, 2015.

[29] A. Aldribi and I. Traore, "A game theoretic framework for cloud security transparency," Network and System Security, Springer: 488-500, 2015.

[30] C. Daskalakis, P. Goldberg, and C. Papadimitriou, "The complexity of computing a Nash equilibrium," SIAM Journal on Computing, 39(1): 195-259, 2009.

[31] V. Chepyzhov and M. Vishik, Attractors for Equations of Mathematical Physics. Providence, RI: AMS, 2002.