COMP534 - Term Paper
Game Theory Applications within Cyber Security

Erhan Tezcan
Department of Computer Engineering
Koç University
Istanbul, Turkey
etezcan19@ku.edu.tr

Mandana Bagheri Marzijarani
Department of Computer Engineering
Koç University
Istanbul, Turkey
mmarzijarani20@ku.edu.tr

***Abstract*—Cyber security is a well-studied area, yet complex decision making strategies of both attacker and defender have it's own challenges. Game theory has been an intriguing approach to tackle such problems. In this work we cover several such applications of game theory, and group them under classes of games. We focus on 3 particular studies: an intrusion detection network resource allocation model, a detection manipulation game, and a moving target defense for intrusion detection system placement on cloud. For each of them, we further provide a comparison against cryptographical approaches, in terms of similarities and differences.**

***Index Terms*—Game Theory, Cyber Security, Cryptography**

I. Introduction

Cyber security is a collective term that denotes technologies, processes and controls aimed to protect systems, network, and data from attackers. [1]. The number of incidents in cyberspace is constantly growing, especially with the increasing number of network users. Most defense methods can be considered ad hoc, where the attacker then finds ways to circumvent the patches to establish an attack; in some form a race among countermeasures and attacks [2]. However, this patches-on-patches approach is not the most desired method of defense, as one successful attack would suffice for the attacker; whereas the defender has to win each and everytime. In other words, defending against well-defined attack scheme's are remedial to those attack schemes indeed, but it does not count for the dynamic interaction between attacker and defender, nor their decision making strategies.

The complex decision making process may regard countermeasures, recoveries, or even predictions in cyber security; and demands a robust approach that can process the vast number of possible strategies. This is where game theory comes in: it is a branch of mathematics that studies the optimal decision making of independent players. It is tempting to treat several cyber security use-cases as a game of attack-and-defend [3]. The mathematical tools provided by game theory such as equilibrium points, with most widely known being Nash equilibrium, can provide a different perspective for the security of a system. It can also can examine a substantial amount of strategies before yielding the best course of action, both for the attacker and defender parties [1], [2], [4].

TABLE I
Classes of games and their applications in cyber security, as in [1], [5].

Classificiation		Information	Application
Cooperative	Static	Imperfect	[6]
Non-Cooperative	Static	Complete Imperfect	[7], [8]
		Incomplete Imperfect	[9], [10]
	Dynamic	Complete Perfect	[11]–[14]
		Complete Imperfect	[15]
		Incomplete Perfect	[16]–[19]
		Incomplete Imperfect	[20]–[23]

A. Game Theory Terminology

It is required to revisit game theory terminology that is used within the context of this paper, as also described in [1], [2]. First we describe the basic components within a game:

Player: An entity that makes choices for *actions*, which result in *payoffs*. This player can be a single person, machine, or a group of these.
Action: A move in the *game*.
Payoff: A reward given to a *player* for their *action*. This can be positive, negative, or zero.
Strategy: Plan of *actions* within the *game* that a *player* can follow.

When these elements are defined, the basic framework of a game is described by a set of rational players, the strategies of them and their payoffs [24]. There are several classes of games. It is useful to respect to this classification in application of game theory, as each class have their own set of properties and assumptions.

Cooperative: A game in which players can enforce cooperative behaviour, and make agreements over their actions.
Non-Cooperative: A game in which all the players are selfish, and do not take their opponents into account. The main objective of players here is to increase their payoffs.

Static (Strategic): A game in which all players choose the plan of action and all decisions are made simultaneously. This is a *one-shot game*, only one move is made by everyone all at once.

Dynamic (Extensive): A multi-stage game, where in every stage the players can consider their actions.

Depending on the amount of information players have regarding each other, the games are further classified as:

Complete Information: A *game* in which every *player* knows both the *strategies* and *payoffs* of all *players* in the *game*, but not necessarily the *actions*.

Incomplete Information: A *game* in which at least one *player* is unaware of the possible *strategies* and *payoffs* of at least one other *player*. Such games are also known as *Bayesian* games [24].

Perfect Information: A *game* in which each *player* is aware of the *actions* of all other *players* that have already taken place.

Imperfect Information: A *game* in which at least one *player* is not aware of the *actions* of at least one other *player*. Thus by definition, all *static games* are in this category.

In many of the applications of game theory, the information about Nash Equilibrium for the game is a key point. A Nash equilibrium is a steady state condition of the game, where each player is following the best strategy such that all players have the most possible payoff. [2]. The aim is to see whether the equilibrium exists or not, and if it does, how it can be attained [8]. It is a particular challenge that one can prove the existence of Nash equilibrium but still not know how to practically reach that point, as also pointed out in [1]. In the context of 2 players: "Players A and B are in Nash equilibrium if A is making the best decision it can with respect to B's decision, and B is making the best decision it can with respect to A's decision" [4].

The early applications of game theory to cyber security was still related to economics, as in: what is the best resource allocation one must do to secure the system, how to efficiently recover from an attack, and so on. As also mentioned in [5], early applications are static games used in security investment optimization and incentive mechanism. The more realistic game applications are non-cooperative dynamic games. It is natural that the general game theoretic approach in cyber security begs non-cooperative games, as the attacker and defender do not necessarily cooperate. Instead, they tend to act selfishly: the attacker would like to engage in malicious activity, and the defender would like to prevent that from happening; there is no clear point of cooperation in such a scenario. In particular, incomplete information game models are applied in cyber-attack-defense analysis [5].

II. Literature Review

Though there are numerous applications of game theory within cyber security as we have shown in table I, we will be focusing on 3 studies in particular for this paper:

1) **GUIDEX: A Game-Theoretic Incentive-Based Mechanism for Intrusion Detection Networks** [22]. A *dynamic* N-player game with *incomplete* and *imperfect* information. For each peer among these N players, there is also a dynamic game.
2) **Manipulating Adversary's Belief: A Dynamic Game Approach to Deception by Design for Proactive Network Security** [23]. A *dynamic*, *incomplete* 2-player game. Only one of the players have *perfect* information, hence overall the game model is *imperfect*.
3) **Moving target defense for the placement of intrusion detection systems in the cloud** [25]. A two-player general-sum Stackelberg Game between the cloud administrator and an attacker.

We describe these papers with 6 subsections for each: *Motivation*, *Problem*, *Solution*, *Evaluation* and for our comments *Remarks*. We also compare the game theoretic approach to cryptographical approaches within each of these studies, under *Comparison* subsection. For this, we would like to state several remarks that apply to all of the selected studies.

We can seize a similarity among the *reduction proofs in cryptography* and *equilibrium proofs in game theory*. In cryptography, we have assumptions about the computational capabilities of the adversary and the complexity of certain algorithms. Building upon those, we create a cryptographical tool (such as encryption, hashing, signing, etc.) and we prove that with the given assumptions there is a reduction from our problem to an already proven problem [26]. In game theoretical applications of security, the researchers are tasked with formalizing the setting to fit into a game model, which then utilizes the mathematical properties of such game models. We can see this in the prior survey papers [1], [2], [5]. Afterwards, several mathematical techniques are put to use in aim of proving the existence of equilibrium points. We provide further detail on the mathematical methods used in these studies, under their respective subsections.

Looking at both of these domains at once, we see the similarity of robust mathematical definitions and proofs based on those. However, the applications are rather different. In cryptography, the proof is to usually state that some assumption holds [26], but in game theoretical applications the proof is mostly about the existence of equilibrium points. This leaves developing practical algorithms to obtain that equilibrium as a challenge to the respective researcher. Notice that in terms of the "players", there is a difference: in game theory these entities are defined mostly by their decision making strategies, and these can be human, machine, or a group of these. In cryptography however, the players are mostly defined by their computational capabilities and power of the attack.

GUIDEX: A Game-Theoretic Incentive-Based Mechanism for Intrusion Detection Networks [22].

Motivation: Internet intrusion is a major problem in cyber security. Network intruders can obtain private information, and further infect the machine to be a part of botnet and use them in distributed denial of service attacks [27], [28]. To defend

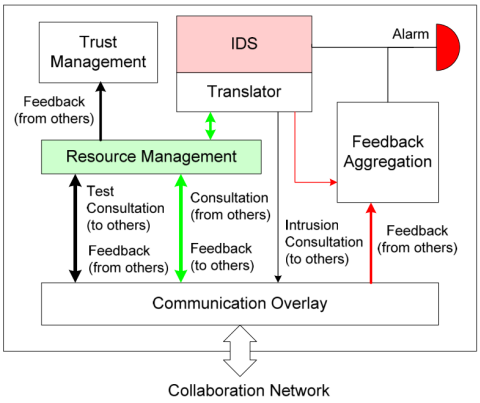

Fig. 1. An IDS Collaboration System within the GUIDEX IDN. (Figure 2 in [22]) Every IDS within the network is assumed to employ this system.

against intrusion, one often employs an Intrusion Detection System (IDS). These systems are remedial on many cases, tasked with alarming the administrators in case of an intrusion. Notwithstanding, attackers can still succeed, especially if the system is compromised via an unknown or unprecedented way [22]. To further improve the defense, a network of IDS' are formed, resulting in an Intrusion Detection Network (IDN). This network is more robust, and different IDS' within the network can have different policies, and different capabilities, which all take part in improving the aggregate defense.

Problem: As is the case in most security systems, IDN's too are vulnerable to *insider attacks*. A malicious member of the network can provide false information, or overload the system via spam. There is also a case called "free riders": members that do not contribute to the network but still use it's capabilities [29], [30]. The trust management and resource allocation within the network then becomes a critical part, which GUIDEX attempts to improve via game theory.

Solution: In figure 1, the IDS Collaboration System within a GUIDEX network is given. It has many components, each described in detail in their work; however, the application of game theory is on the 2 major components of the system: resource and trust management. They construct a *game problem* (GP) for each *peer* in the network. The objective of each peer is to optimize their resource allocation within the IDN. They model the altruistic behaviour among peers as a non-cooperative game. They prove that for each GP there exists a Nash equilibrium and is unique. Furthermore, this equilibrium solution of GP is *reciprocal incentive compatible*. To describe this term, consider the peers: u and v. Suppose the helping resource from v to u is shown as p_{vu}, and p_{uv} for vice versa. The reciprocal incentive compatibility assures that if p_{uv} increases then so does p_{vu} and that if say u trusts v more, then p_{uv} increases too. The latter is especially a good property, because we would want the resource sharing to increase among more trusted peers. We had previously noted that although the equilibrium can be proven to exist, it may be hard to practically compute [1]. In this work they provide a dynamic algorithm using a Lagrangian approach, and they are able to compute this unique equilibrium in a reasonable amount of time. This is described in their section 4, where they describe their "Primal / Dual Iterative Algorithm". Note that this is an iterative method: it approximates to the actual Nash equilibrium, rather than directly computing it; which is often rewarded with better performance with slight loss in accuracy.

Evaluation: Their iterative algorithm is proved to converge to the Nash equilibrium at a geometric rate. In practice, even just 2-3 iterations are enough for convergence, as shown in their Figure 3. They run both centralized and decentralized simulations with the number of nodes ranging from 2-3 to 100 with varying trust values; and in each the resulting resource sharing strategies from the Nash equilibrium is compliant to the expected values. In all cases, they show that when a peer is less trusted, it will have less resources. Furthermore, the practical results are consistent with their theoretical findings. Their results show that GUIDEX can optimize the resource and trust management problems, which in effect prevents free-riders and dishonest insiders. Furthermore, a denial-of-service where a peer spams a large amount of information to overload others [31] is dealt with, because the resource sharing in-advance disallows such overloads.

Remarks: We had mentioned in prior sections that early applications of game theory were more inclined towards the economical aspects of cyber security, such as resource allocation and optimization. Indeed we see such an application in this paper, where the resource allocation is of in particular interest to the members of an IDN. This work is also built on mathematical grounds, and to see it applied in a network setting with promising results in practical simulations, shall intrigue further research to take place; perhaps, in various other network settings or different intrusion detection systems.

Comparison: Though there are many mathematical details in the work of Zhu et al., one part particularly resembles cryptographical methods. They obtain two equations from the game among peers u and v (every peer in the network plays this game), which they then *represent* as a 2×2 matrix within a linear system of equations. They prove that this is an M-matrix [32], which indicates that it has a unique solution; and, they have implemented an iterative solver to find it. It can be said that this is similar to reducing a problem to a known one in cryptography.

Manipulating Adversary's Belief: A Dynamic Game Approach to Deception by Design for Proactive Network Security [23]

Motivation: In the past decades, cyber-attacks have targeted databases and critical public infrastructures. Due to the sophistication of these attacks, traditional defense measures such as IDS, firewalls and malware scanners have fallen short because the attackers can identify these defense mechanisms, study them and find their vulnerabilities and exploit them. [33]

In recent years, defense engineers have proposed a more proactive mechanism to engage with the attacker dynamically and influence their actions by strategically manipulating their perception of the guarded system. This defense technique

called defensive deception, is a way to alleviate the information asymmetry -typically enjoyed by attackers- in favor of defenders. Defense deception is applied in network security but analyzing its impact is done in a quantitative framework of game theory to provide credible predictability and rigor.

Problem: Even though cyber defense technologies such as firewalls, IDS, access control etc. exist within cybersecurity, they fall short in addressing new security and privacy attacks. These mechanisms are not proactive and were not designed to engage the attackers, nor they gather information about the attacker to better understand the future threats.

Solution: Manipulating attacker's belief of system can be an effective counteract to information asymmetry between defender and attacker. Cyber deception can be defined as strategic confrontations between rational parties and since game theory mathematically studies models of conflict and cooperation between intelligent rational decision-makers, it can be an appropriate quantitative method to understand cyber deception. Horak et al., specifically focused on the class of dynamic games of incomplete information which allows modeling the multi-stage interactions between an attacker and a defender as well as the information asymmetry.

The authors employed competitive Markov models with imperfect information, or partially observable stochastic games to model penetration of an attacker into a network; and, they consider defender the player with perfect information. Figure 2 depicts states and network layers to capture the interactions between defender and attacker using a transition system. In the states at the top of the figure, the attacker is not detected yet. When the IDS detects the attacker, the state moves to the bottom of the figure. The defender does not immediately eject the attacker; instead, it decides when to engage the attacker and gathers information about it until ejection. Horak et al. argued that immediate ejection after detection is not optimal, as this may lead to the attacker starting over from another undetected state with useful information on the defender's capabilities. So it would be in the defender's advantage to allow the attacker to stay in the system for now, while being fed disinformation. The attacker compromises the network in layers and chooses when to exfiltrate data without knowing if she has been detected. In equilibrium, the defender's optimal strategy is to keep the attacker inside the network while the attacker believes she has not yet been detected; otherwise, to eject the attacker from the network.

Evaluation: The authors evaluated their work using an experimental evaluation of their game theoretic strategy to determine the average time between the first IDS detecting the attacker and the time the defense system decided to block them. They evaluated their strategy against an advanced attacker who plays the best response to this strategy. They found out that on average it takes 4.577 steps between detection and ejection. In this time window, the defender can make sure of the credibility of the IDS alert and minimize the chance of blocking a benign user.

Remarks: This paper studies a simplified network structure relative to the real scenarios but it offers a good analysis of

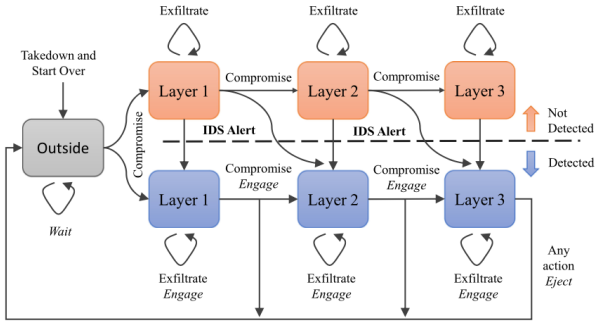

Fig. 2. Transition system of a partially observable stochastic game representing attack on the network. From left to right the states correspond to layers of a network. (Figure 10 in [34])

the optimal strategies for an informed defender. Most game-theoretic models of deception are either static games (such as simultaneous move Nash games) or single-shot dynamic games (such as Stackelberg games or signaling games) [34]. This study uses deception in a multi-stage setting, where both players take sequences of actions to either deceive the adversary, or attempt to find out whether they have been detected or not.

Comparison: This work had less theoretical rigor compared to the other two [22], [25]; however, it is still based on application of one-sided partially observable stochastic games [35]. This again resembles the reduction proofs in cryptography: a cyber-security setting is reduced to an already-studied game model.

Moving target defense for the placement of intrusion detection systems in the cloud [25]

Motivation: Moving Target Defense (MTD) is a defense strategy that utilizes changing the static configuration of systems and networks into a dynamic, fluid configuration. The end goal of MTD is to make the system parameters appear random to attackers. Sengupta et al. propose a new approach for placement of Intrusion Detection Systems (IDS) in a cloud environment based on MTD principles. The aim is to place a few strategic IDS nodes in a large cloud so that attacks are detected effectively. Different IDS configurations are switched between using MTD, to reduce overhead of having one IDS per node while maintaining effectiveness [36].

Problem: Placement of one IDS per node on a cloud provider results in significant performance loss. At the same time, random placement of IDS on a subset of nodes statically will result in discovery of the IDSs by attackers, and consequently targeting of unprotected nodes. [25]. The problem is further compound as there are two general types of IDS, Network IDS which inspects network traffics and patterns, and Host IDS which inspects node resources and behavior.

Solution: A generalization of MTD is provided. Traditional MTD approaches change the attack surface. The approach in this work however, uses MTD for defense purposes and

widens the defense net using dynamic configurations, rather than changing the attack surface.

The problem is formulated as a two-player general-sum Stackelberg Game. The equilibrium of the game provides the optimum strategy for the defender. Utility values of players are calculated by a combination of the CVSS [37] score, a common impact score associated to attacks, and the centrality of the protected node. Several optimizations are used to calculate the equilibrium, such as using custom reward functions and incorporating the cost of deploying an IDS, resulting in a polynomial time algorithm. The Birkhoff Von-Neumann Theorem [38] guarantees that the marginal probabilities will result into probability values that correspond to deployment strategies. Additionally, the most critical vulnerability of such a system is identified using the same infrastructure, showing that the highest CVSS is not necessarily the most critical vulnerability in a protected cloud environment.

Evaluation: `snort` [39], a popular Network IDS and `auditd` [40], a popular Host IDS are used for evaluations. A dynamic MTD approach turns IDS on and off on each of the compute nodes. Comparison is first done against Deterministic Pure Strategy (DPS), Uniform Random Strategy (URS) and Centrality Based Strategy (CBS), using simulations. The proposed system has low cost. It performs on par or slightly worse than URS but better than the other two in average utilities, and outperforms all three approaches on utilities near 1.

Secondly, an evaluation using a cloud network is performed. 15 virtual machines and 42 CVEs scattered throughout these machines uniformly on a flat network are used. Throughput of the services in presence of NIDS/HIDS is measured. As IDSs go from 1 to 15, throughput is reduced from 18 Gbps to 6 Gbps, establishing the motivation of the research. The experimental results show that utility does not grow linearly with the number of IDSs. Rather, from 1 to 18 IDSs, utility grows slowly and linearly, but from 18 to 30 it grows exponentially, and beyond 30 the utility drops. Experimental results in a real-world large-scale cloud are also provided.

Remarks: The paper assumes that the attacker is rational, but does not have unlimited time to recon the behavior of the dynamic strategy. Additionally, most of the paper's effort is put towards optimizing the equilibrium problem so that it is solvable. Evaluation is a bit lacking as only 15 nodes with 42 vulnerabilities are assessed. The results are not immediately scalable to larger systems, especially with respect to the complexity of solving the equation.

Comparison: We see that time complexity of calculating the equilibrium point comes into play in this study. Furthermore, to prove the validity of their algorithm, they make use of Birkhoff Von-Neumann Theorem [38]. In cryptography too, we observe theorems coming into play for validity, for example the Miller-Rabin Primality test [41] are used by other prime generator algorithms [26].

III. Related Work

There have been numerous surveys about the usage of game theory within cyber security. Roy et al. [2] made an extensive coverage of the game theoretic applications within network security. They have proposed a taxonomy of game theoretic approaches, with the aims of aiding further research under that classification. In later survey papers we can relate to this taxonomy [1], [5]. With this taxonomy at hand, they have provided studies from the literature for each sub-class and they have noted several further research directions with respect to each application of game theory.

Wang et al. [5] covered the later works, proposed within the 6 year gap from the previous paper, and they have grouped the domain of applications with respect to game theoretical classifications. Our Table I is motivated by their table, though ours indicate the specific studies under the game classes rather than providing the subject name. They have shed light on the impending challenges of the game theoretical models in cyber security applications, and gave recommendations for the further research. Patil et al. [1] further covered the cyber security applications under the topics that appear in Table I of Wang et al. [5]. They too briefly mentioned the challenges in designing a game theoretical model for cyber security.

Wilczyński et al. [42] surveyed applications of Stackelberg games in security. In such a game, one user acts a leader and the rest of the players are it's followers [43]. This game setting has applications in security aspects of high performance computing telecommunication and transportation systems, with several options for the game model. They discuss both the computational and implementation aspects of each model, and present realistic use-cases for them in their survey.

IV. Conclusion

We have covered a selection of 3 works, that apply game theory under intrusion detection [22], [25] and decision manipulation [23]. In Table I we have provided a general overview of studies with respect to the classifications done in [2] and [5]. For each of the selected studies, we have also provided a general comparison to cryptographical approaches.

It is clear that game theory applications are well-established in the domain of cyber security by now. With clever remodeling of the attacks and finding a suitable game model, one can analyze the system using the mathematical tools provided by game theory. However, it is still a major challenge to decide the assumptions formally such as payoff functions, the information of players regarding each other; albeit having a system modeled after practical settings. The practicality of equilibrium points is also a major concern for game theory applications. For this challenge in particular, we have seen how iterative methods could be used in [22].

Remarks: We had not seen the applications of game theory in cyber security before, and we are fascinated by it. We have seen how some systems covered in class were approached in a game theoretical way, which allowed mathematically robust methods to be employed to improve them. Though the field is already established, we believe there is still more clever game models yet to come, on many different security systems.

REFERENCES

[1] A. P. Patil, S. Bharath, and 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.

[2] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," *Proceedings of the Annual Hawaii International Conference on System Sciences*, no. February 2010, 2010.

[3] A. Attiah, M. Chatterjee, and C. C. Zou, "A Game Theoretic Approach to Model Cyber Attack and Defense Strategies," *IEEE International Conference on Communications*, vol. 2018-May, 2018.

[4] A. Pătraşcu and E. Simion, "Game theory in cyber security defence," *2013 International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2013*, no. June, 2013.

[5] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A survey of game theoretic methods for cyber security," *Proceedings - 2016 IEEE 1st International Conference on Data Science in Cyberspace, DSC 2016*, pp. 631–636, 2016.

[6] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1616–1627, 2014.

[7] L. Carin, G. Cybenko, and J. Hughes, "Quantitative evaluation of risk for investment efficient strategies in cybersecurity: The queries methodology," 2008.

[8] J. Jormakka and J. V. E. Mölsä, "Modelling Information Warfare as a Game," *Journal of Information Warfare*, vol. 4, no. 2, pp. 12 – 25, 2005.

[9] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Trans. Inf. Syst. Secur.*, vol. 8, p. 78–118, Feb. 2005.

[10] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," *ACM International Conference Proceeding Series*, vol. 199, no. January 2006, 2006.

[11] K.-W. Lye and J. M. Wing, "Game strategies in network security," *Int. J. Inf. Secur.*, vol. 4, p. 71–86, Feb. 2005.

[12] C. Xiaolin, X. Tan, Z. Yong, and H. Xi, "A markov game theory-based risk assessment model for network information system," pp. 1057–1061, 01 2008.

[13] T. Alpcan and T. Başar, "An intrusion detection game with limited observations," 01 2006.

[14] K. Nguyen, T. Alpcan, and T. Başar, "Stochastic games for security in networks with interdependent nodes," in *Proceedings of the 2009 International Conference on Game Theory for Networks, GameNets '09*, Proceedings of the 2009 International Conference on Game Theory for Networks, GameNets '09, pp. 697–703, 2009.

[15] K. C. Nguyen, T. Alpcan, and T. Basar, "Security games with incomplete information," in *2009 IEEE International Conference on Communications*, pp. 1–6, 2009.

[16] Z. Chen, *Modeling and defending against internet worm attacks*. dissertation, Georgia Institute of Technology, 2007.

[17] A. Patcha and J.-M. Park, "A game theoretic approach to modeling intrusion detection in mobile ad hoc networks," in *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.*, pp. 280–284, 2004.

[18] T. Alpcan and L. Pavel, "Nash equilibrium design and optimization," in *2009 International Conference on Game Theory for Networks*, pp. 164–170, 2009.

[19] M. Bloem, T. Alpcan, and T. Basar, "Intrusion response as a resource allocation problem," in *Proceedings of the 45th IEEE Conference on Decision and Control*, pp. 6283–6288, 2006.

[20] T. Alpcan and T. Basar, "A game theoretic analysis of intrusion detection in access control systems," in *2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601)*, vol. 2, pp. 1568–1573 Vol.2, 2004.

[21] X. Z. You and Z. Shiyong, "A kind of network security behavior model based on game theory," in *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*, pp. 950–954, 2003.

[22] Q. Zhu, C. Fung, R. Boutaba, and T. Basar, "GUIDEX: A game-theoretic incentive-based mechanism for intrusion detection networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2220–2230, 2012.

[23] K. Horák, Q. Zhu, and B. Bošanský, "Manipulating Adversary's Belief: A Dynamic Game Approach to Deception by Design for Proactive Network Security," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10575 LNCS, pp. 273–294, 2017.

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

[25] S. Sengupta, A. Chowdhary, D. Huang, and S. Kambhampati, "Moving target defense for the placement of intrusion detection systems in the cloud," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11199 LNCS, no. August, pp. 326–345, 2018.

[26] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC, 3rd ed., 2021.

[27] R. Vogt, J. Aycock, and M. Jacobson, Jr, "Army of botnets.," 01 2007.

[28] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, 05 2004.

[29] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Free-riding and whitewashing in peer-to-peer systems," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 5, pp. 1010–1019, 2006.

[30] S. J. Grossman and O. D. Hart, "Takeover bids, the free-rider problem, and the theory of the corporation," *The Bell Journal of Economics*, vol. 11, no. 1, pp. 42–64, 1980.

[31] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Trans. Comput. Syst.*, vol. 24, p. 115–139, May 2006.

[32] A. Berman and R. J. Plemmons, *Nonnegative Matrices in the Mathematical Sciences*. Academic Press, 1st ed., 1979.

[33] K. Horák, Q. Zhu, and B. Bošanskỳ, "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*, pp. 273–294, Springer, 2017.

[34] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–28, 2019.

[35] K. Horák, B. Bošanský, and M. Péchouček, "Heuristic search value iteration for one-sided partially observable stochastic games," in *Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence*, AAAI'17, p. 558–564, AAAI Press, 2017.

[36] S. Sengupta, S. G. Vadlamudi, S. Kambhampati, A. Doupé, Z. Zhao, M. Taguinod, and G.-J. Ahn, "A game theoretic approach to strategy generation for moving target defense in web applications.," in *AAMAS*, pp. 178–186, 2017.

[37] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, and H. Debar, "A service dependency model for cost-sensitive intrusion response," in *European Symposium on Research in Computer Security*, pp. 626–642, Springer, 2010.

[38] D. Korzhyk, V. Conitzer, and R. Parr, "Complexity of computing optimal stackelberg strategies in security resource allocation games," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 24, 2010.

[39] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks.," in *Lisa*, vol. 99, pp. 229–238, 1999.

[40] K. Ilgun and A. USTAT, "A real-time intrusion detection system for unix," *University of California Santa Barbara Master Thesis*, 1992.

[41] M. O. Rabin, "Probabilistic algorithm for testing primality," *Journal of Number Theory*, vol. 12, no. 1, pp. 128–138, 1980.

[42] A. Wilczyński, A. Jakóbik, and J. Kołodziej, "Stackelberg security games: Models, applications and computational aspects," *Journal of Telecommunications and Information Technology*, vol. 3, pp. 70–79, 09 2016.

[43] B. von Stengel and S. Zamir, "Leadership with commitment to mixed strategies," tech. rep., 2004.