Game Theory on Attack Graph for Cyber Deception

Ahmed H. Anwar [0000-0001-8907-3043] and Charles Kamhoua [0000-0003-2169-5975]

[1] US Army Research Laboratory, MD 20783, USA
charles.a.kamhoua.civ@mail.mil

Abstract. Game Theory provides a set of tools and a framework suitable to study security problems. In this paper, a class of games is developed to study cyber deception and the interactions between the network defender who is deceiving an adversary to mitigate the damage of the attack. In order to capture network topology, each game is played over an attack graph that can be generated according to the vulnerabilities associated with each node. The defender's goal is to take deceptive actions to prevent the attacker from taking control over the network resources exploiting the incomplete information of the attacker regarding the deceptive network gained through the attack reconnaissance stage. To this end, we present several games such as normal form static, dynamic, hypergame, and a partially observable stochastic game (POSG) to study the game dynamics at different information structures. For the most general class of games, (i.e., POSG), we provide multiple solution approaches to overcome the intractability of the game model and finally present numerical result samples to show the effectiveness of each solution approach.

Keywords: Game Theory, Cyber Deception, Network Security, Attack Graph, Hypergame, Partial Observable Stochastic Game.

1 Introduction

Cyber deception refers to a set of techniques that can be implemented to give attackers false beliefs. Such set includes information masking, dazzling, hiding, decoying, false information, and camouflaging [2, 5]. In fact, cyber deception is used from both sides, the attacker implements deception techniques to hide his true identity, strategy, and payoff and let the defender believe that the attacker is a legitimate user. However, the focus of this paper is to study cyber deception as a defense technique implemented by network admin [1]. In a real threat scenario, the identities of adversaries are unknown to the defender, which is a huge advantage to the attackers that allows them to collect information about the network until an intrusion detection system (IDS) catches them [17]. Therefore, to suppress this advantage from attackers, a defender needs to implement cyber deception techniques to misrepresent the network and alter its true state, and hence the outcome of the attackers' reconnaissance will be useless and misleading. To this end, deception techniques such as honeynets [7, 4, 16], data, and file obfuscation techniques [11, 21, 25, 12], and moving target defense (MTD) [8, 44, 45] have been proposed. Although, MTD and cyber deception techniques aim to thwart the attackers' attempts to collect the system information via changing the attack space and the true state of the network, however, MTD techniques do not introduce any false

information that can actively mislead attackers. On the other hand, cyber deception may use false objects or information for the attackers to form false beliefs that affect the decision of the attackers.

Security games literature studied strategic decision-making problems in a game-theoretic framework between two players, specifically, the network defender and the attacker [14, 3, 43, 46]. Security games applications includes the protection of critical infrastructures, [22, 14, 23], computer networks [24, 10, 15, 6, 19, 44, 45]. The success of strategic deception hinges on the information observed by both players. The defender may strategically leak or let the attacker access manipulated information about the network that lures the attacker to behave in a certain way that may or may not be observed by the defender. How information observability is classified leads to different classes of the game as discussed in detail in Section 2.

In this paper, we present the state-of-the-art game-theoretic models to address cyber deception and develop a partially observable stochastic game as a generalized framework to study this problem. Secondly, we discuss the complexities and intractability of POSG games and present several approaches and relaxations to overcome the game model complexities. Finally, numerical results are presented to validate the proposed approaches to solve the game.

The rest of the paper is organized as follows: In section 2, we present a line of related cyber deception work on attack graphs and game theory. After that, in Section 3, we discuss different game classes. In Section 4, several approaches are presented to solve the game. We present numerical results in Section 5 and conclude our work in Section 6.

2 Related work

2.1 Attack Graph

An attack graph is a tool used to model network security by capturing network connectivity and vulnerabilities. Attack graphs could be generated in several ways. For instance, Kamdem et al. [30] generated a vulnerability multi-graph in which node are vulnerable hosts, and edges represent the vulnerabilities between nodes. Authors in [31] used attack graphs to model the causal relationship of different vulnerabilities and proposed a probabilistic metric for network security. Stochastic games played on attack graphs facilitate cyber deception automation and deception policy implementation on networks. However, the dimension of strategy space explodes for attack graph games in the size of the attack graph. Moreover, partial observability regarding attacker dynamics is a struggle against developing deception policy.

A defender can model the behavior of a partially observable attacker using one of two approaches. A simple but naïve approach is to model the actions of the attacker as exogenous noise. The second approach is to take into account the attacker's actions as observations that are induced given her actions. Finally, the defender can assume that the attacker is also monitoring the system partially and is maximizing his long-term

reward symmetrically. The latest model is known as POSG and is the most general framework.

Attack graph is adopted extensively to study cybersecurity problems [32, 33, 34, 35, 36]. More specifically, it is used to study cyber deception using different game-theoretic models. These models include normal form games, Stackelberg games, hypergames, and partially observable stochastic games.

In [32], a full information normal form game is played on an attack graph to study the effect of software diversity to deceive adversaries and enhance network security. The goal of the defender is to diversify the network attack graph to prevent the attacker from launching a full-scale zero-day attack exploiting a single vulnerability. Moreover, a diversified network requires a larger number of probes to collect information. Hence the attacker interacts more with the network which leads to early detection. The attack graph captures the network topology and the relation between the set of vulnerabilities associated with each node. Our results show that diversity limited the attacker's ability to control the network.

In a social network, a malicious user attacks the network through influencing its node. Therefore, one way to counter his negative influence is by blocking a subset of edges (i.e., a subgraph) [33]. We formulated the interaction between the defender and the attacker as a Stackelberg game where the defender first chooses a set of nodes to block in order to minimize the attacker's influence. After observing the modified network, the attacker selects a set of seeds to spread negative information from. To avoid the computational complexity of this bi-level game theoretic optimization problem, an approximate method models the attacker’s problem as the maximum node domination problem. To solve this problem, we first develop a method to formulate the problem as an integer programming combined with constraint generation. Also, proposed an approximate solution to enhance scalability [33]. Considering a Stackelberg game, the defender in [34] is assumed to allocate defensive resources and manipulate the attack graph. We provided techniques for efficiently solving the problem as a mixed-integer linear program.

In a more sophisticated attack scenario, the network suffers an outbreak of a spreading virus. An epidemic game-theoretic model is developed in [36] to study these types of attacks. Epidemic models are used in cybersecurity to model the change of nodes' states over time. In other words, at each time slot, a node could be infected, vulnerable, or recovered. The epidemic model captures the transition of nodes between the mentioned three states. In [36], we proposed a POSG game with one-sided information where players don’t observe the actions of each other. In this epidemic-game model, the attacker at any time-slot selects a subset of neighbors of infected nodes to propagate the malware from via connecting edges. On the other hand, the defender distributes a limited number of honeypots over selected edges of the network. We show that the heuristic search value iteration (HSVI) algorithm developed initially to solve partially observable Markov decision process (POMDP) [40], can be used to efficiently solve this class of POSGs. To this end, we show that the value function operator of the epidemic game model has the necessary properties such that it can be solved using an HSVI-like algorithm.

2.2 Hypergame

Another approach to handle uncertainty is the hypergame framework [35, 37, 41]. Hypergame theory studies the case where the game players have different views of the game model including the strategies of their opponents therefore it fits perfectly to study cyberdeception. Although Hypergame theory can be used to study multiple players, we restrict our discussion for the two-player Hypergame for cyber deception.
A Hypergame G= (V_1, V_2) consists of two preference vectors for each player. Each vector represents the player's perspective of the game. In a fully observed game, each player knows his opponent's preference vector. On the other hand, practically player p can perceive player q's preferences partially, in terms of V_{21} and V_{12} as the perspective of player 1 of player 2 preference and vice versa. In hypergame, players play two different games according to how each player perceives the game. Therefore, a player makes his own decision based on his perceived game. In cyber deception, the attacker is unaware of the induced network state after the deceptive actions have been implemented by the network defender. To solve for an equilibrium of hypergame with a first-level perception, each player plays their own perceived game. First, the attacker solves his perceived game and find the equilibrium of the adversary perceived game as denoted by (a^e(A),d^e(A)). Similarly, the defender solves his perceived game, and find the equilibrium (a^e(D),d^e(D)) of the game. Finally, the hypergame equilibrium is (a^e(A),d^e(D)).

In [37], we developed a hypergame model that examines how attacks spread inside the network using attack graphs. In this mode, the defender installs honeypots on well-selected nodes to thwart the attack. Based on the formulated hypergame, the defender decides where to place honeypots. The game is repeated after players receive the payoff of their actions. According to her payoff, the attacker could choose to cover the maximum number of nodes to increase his reward at the current stage. However, the attacker could also decide to explore other unvisited nodes. We estimate the amount of time needed for an attacker to reach the target nodes through experiments, which provides a quantitative measure to determine when it is necessary to disable all the connections to the target nodes.

In [35], we focused on the problem of joint designing a decoy placement strategy and a deceptive defense strategy that maximally exploits the fact that decoy locations are partially observable by the attacker to ensure that the defender can satisfy his/her goal in temporal logic. Given the large space searching for optimal decoy placement policy, we use formal methods to show that the utility function is non-decreasing and monotone. We formulated a deception hypergame to place decoy devices. In this game, the defender allocates decoys to deceive and trap the attacker. We have also synthesized stealthy deceptive strategies with temporal logic specifications using hypergame theory in [41] to develop sure winning and almost-sure winning strategies for the defender.

3 Information model and Game formulation

3.1 On the complexity of POSG

Information monitoring determines the class of the game to be played between the attacker and the defender. In a complete information game, the game reward function, possible actions, and player identity is common knowledge. However, if players don't know all the information about their opponent, then we are dealing with an incomplete information game. This arises if, for example, the defender does not know the reward function or the possible strategies of the attacker. In a game of perfect monitoring, each player fully observes the actions taken by the other players. This is different from a class of game of imperfect monitoring in which, a player does not know what specific action is played by his/her opponent after any stage. Therefore, poker is studied under the latter class of games. A stochastic game is played in a sequence of stages with the game dynamically evolving from one state to another depending on the actions taken by all players. The most general framework that combines an evolving game, with imperfect monitoring is the partially observable stochastic game (POSG). In this class, the game information is known to both players, however, each player observes the game evolution and/or his opponent's actions partially. POSGs are the most general framework in game theory literature. A single-agent dynamic game resort to a Markov decision process (MDP). The optimal policy of an MDP can be obtained efficiently in polynomial time as shown in [20]. On the other side, Conitzer and Sandholm have shown that hardness of determining whether a pure-strategy Nash equilibrium exists in a Markov (stochastic) game is PSPACE-hard [9]. Adding uncertainty to an MDP results in a partially observable MDP (POMDP) where an optimal policy cannot be obtained in polynomial time anymore. Eventually, the complexity of solving a POMDP is known to be PSPACE-complete [20]. A POMDP is considered a single-agent POSG. Goldsmith and Mundhenk [13] have shown that extending a POMDP to a noncooperative multi-agent scenario (i.e., POSG) results in a NEXPNP-complete problem to determine whether there is a "good" strategy for that game and optimal policy existence problem associated with POSGs is undecidable [18].

3.2 Game Model

A zero-sum partially observable stochastic game is a tuple (S, A_1, A_2, O_1, O_2, T, R, b^{init}) where S is a finite set of states, A_1, A_2 are finite sets of actions of player 1 and player 2, respectively. O_1, O_2 denote observation sets of player 1 and player 2, respectively. $T(o_1, o_2, s \mid s_0, a_1, a_2)$ is the probability of transition from s_0 to s, while observing (o_1, o_2), under action profile (a_1, a_2). $R(s, a_1, a_2)$ denotes the reward of player 1 under (a_1, a_2) at state s, and $b^{init} \in \Delta(S)$ is some initial state-belief vector. To study cyber deception within a POSG we need to define the game components regarding our system model.

Let the defender be player 1 and the attacker be player 2. Assuming that the game is played over an attack graph $G(V, E)$, where V is the set of nodes and E is the set of edges. A node represents a vulnerability that can be exploited by the attacker, while an

edge connecting two nodes v_1 and v_2 means that a vulnerability v_2 can be exploited only if the attacker can reach it through exploiting v_1. In other words, the set of edges manifests the dependencies between the network vulnerabilities based on the network topology. The attacker decides which vulnerability or a subset of vulnerabilities to exploit. The defender, on the other side, inserts fake vulnerabilities along the graph edges such as honeypots to deceive the attacker. The defender decides the locations of the honeypots to maximize his long-term expected reward. The attacker does not observe the actions of the defender and vice versa. The state of the game, s, represents the current location of the attacker as well as the locations of the honeypots. In other words, the state captures the joint history of actions taken by the players. However, each player observes the state partially through observing (o_1,o_2) instead. As mentioned above, for the general stochastic game, a no-regret policy is not tractable [13], set aside the partially observable case. Therefore, in the next section, we discuss solution approaches for POSG under some natural assumptions and relaxations.

4 Game Solving Techniques

In this section, we propose different techniques and approaches to solve POSG formulations for cyber deception. This includes solving POMDP+embedded game approach [42], and One-sided POSG [29].

4.1 POMDP embedded game:

In the first approach, we adopt the POMDP game model and leverage the rich literature of efficient solving algorithms [26]. In this approach, we solely focus on the defender's cyber deception strategy to maximize his long-term discounted reward. The attacker is assumed to have local knowledge about the network structure, and hence she can only reason about her immediate reward.

$$V^*(b) = max_{a_1 \in A_1} \left[R(a_1, b) + \gamma \sum_{b' \in B} \tau(b', a_1, b) V^*(b') \right] \quad (1)$$

Adopting the conventional POMDP notations, equation (1) represents the value function under the optimal policy that maps the belief space to action space. A key component of the above equation is the belief update function, $\tau(b', a_1, b)$. In order to calculate that function, one needs to know the state transition dynamic as well as the observation associated with each transition. The state transition model, $T(s', a_1, s)$, is known by the defender.

On the other hand, observations are directly related to the action played by the attacker. Let $O(o, s', a_1) = Pr(o|s', a_1, b)$ denote the probability of observing observation o with the system transitioning from state belief b under action a to state belief b(s'). Using game-theoretic reasoning, the defender can exploit Nash equilibrium strategies adopted by the attacker to estimate the probability that the attacker has played a specific action given any state, s$\in S$. The defender can then calculate the belief update function as follows:

$$P(o|s', a_1, b) = \sum_{s \in S} P(o|s', a_1, s) b(s)$$

Where,

$$P(o|s', a_1, s) = \sum_{a_2 \in A_2} P(o|a_2, s', s) P(a_2|s', s)$$

$$\tau(b', a_1, b) = \sum\nolimits_{\{o \in O | SE(b, a_1, o) = b\prime\}} P(o|a_1, b)$$

for every possible future belief, b', where $SE(b, a_1, o)$, denotes the state estimate computed as the probability $P(s'|a_1, o, b)$.

4.2 One-sided POSG

In the second approach we focus on a class of one-sided partially observable stochastic games (OS-POSGs). In this model, the attacker is assumed to be perfectly informed about the current state. Along the same lines of POMDP, the belief space is a simplex are over state space and the value function defined over the belief space is convex. The class of one-sided POSGs has been studied previously in [27] as Level-1 stochastic games with incomplete information. Therefore, one-sided POSG's value function has similar structure to the value function of POMDPs. Let G = (S, A_1, A_2, O, T, R, γ) where, S is a finite set of game states, and O denotes the observation set. The function T(.| s, a_1, a_2) ∈ Δ(O × S) represents probabilistic transition function between states under action profile (a_1,a_2). The current state of the game is revealed to the attacker only. The goal is to find a defense strategy that maximizes the expected discounted reward over an infinite number of stages. Numerical results showed that active deception significantly enhanced the security of the network. A strategy that maps the history of actions and observations for player, i, is called 'behavioral strategy' and denoted by, σ^i.

In OS-POSG, the attacker observes the current state, s. Therefore, his decision rule at each state, s, is π_2 (a_2|s), while the defender (player 1) decision rule is not conditional over the state, and is denoted by, π_1 (a_1). If player 1 played $a_1 \in A_1$ and observed o ∈ O, his updated belief τ (b, a_1, π_2, o) over state future state, s', can be expressed as:

$$\tau\,(b, a_1, \pi_2, o)(s') = \frac{1}{\boldsymbol{P}_{\boldsymbol{b},\pi_1,\pi_2}\,[a_1, \mathrm{o}]} \sum_{s,a_2} \mathrm{b(s)}\pi_1(a_1)\pi_2(a_2|\,\mathrm{s})\mathrm{T}(\mathrm{o}, \mathrm{s}'\,|\,\mathrm{s}, a_1, a_2)\,.$$

The value of strategy σ_1 is

$$val^{\sigma_1}(b) = inf_{\sigma_2 \in \Sigma_2} \mathrm{E}_{b,\sigma_1,\sigma_2}(Disc^{\gamma})$$

Where $Disc^{\gamma}$is the infinite discounted reward, for some $0 \leq \gamma < 1$. The optimal value function can hence be expressed as:

$$V^*(b) = sup_{\sigma_1 \in \Sigma_1} val^{\sigma_1}(b)$$

Although we have defined the value function V^* as the supremum over the strategies of player 1 at each the belief point, however finding the value for the given belief is as hard as solving the game itself. Our approach relies on an alternative characterization of the optimal value function V^* to follow the structure of the optimal value function of

a POMDPs. The idea behind this approach is to start with a coarse approximation $V_0 : \Delta(S) \rightarrow \mathbf{R}$ of the value function V^* , and then iteratively improve the approximation by applying the Bellman's operator H, iteratively,$V_{i+1} = HV_i$. One can show that the function HV resulting from applying H on a convex continuous function V as formulated above is also convex and continuous. Hence, we can apply the operator H iteratively. Operator H can be used to approximate the optimal value function V^*. The bellman operator, H, is a contraction mapping, and hence converges to the unique fixpoint, and which is the optimal value function V^*, therefore [HV](b) leads to the Nash equilibrium of the corresponding stage game. The described structure of the H operator and the value function V(b), we can hence adopt POMDP solving approaching such as value iterations and Heuristic Search Value Iteration (HSVI) for better performance.

5 Results

To show the efficiency of the developed algorithms in sections 3.1 and 3.2, we present sample results that show the effectiveness of the cyber deception strategies developed via the proposed POSG algorithms.

First, we present results for the model introduced in section 3.1, [42]. In this context, the attacker can only reason his actions based on local information, not the whole network. However, the defender is solving his imperfect information game with the defender assuming that the attacker is rational and following Nash strategies at equilibrium for each subgame (i.e., game stage). For a 7-node network, the defender decides where to place a honeypot, while the attacker is evading honeypots to stay stealthy as long as possible and attack real nodes. The defender receives a reward if capturing the attacker in a honeypot while losses if the attacker escaped honeypots. The defender incurs a cost for placing honeypots, and there is a cost per attack paid by the attacker. Both players can choose to stay idle to avoid the cost associated with each action. In Figure 1, the defender reward is plotted versus the capture cost. As shown, the proposed deception algorithm outperforms other schemes. Defender's reward increases as the capture cost incurred by the attacker when caught increases. However, if the cost is very high, it forces the attacker to back off to avoid the high-risk action, the defender reward goes down. Note that, in this scenario, we mainly focus on the capture reward due to successful deception. As shown in Figure 1, a fixed allocation policy does not recognize game dynamics, and hence ignores all observations that are available through the network monitoring systems, IDS, etc. On the other hand, random deception strategies do not consider the network structure, it randomly allocates honeypots as the game evolves.

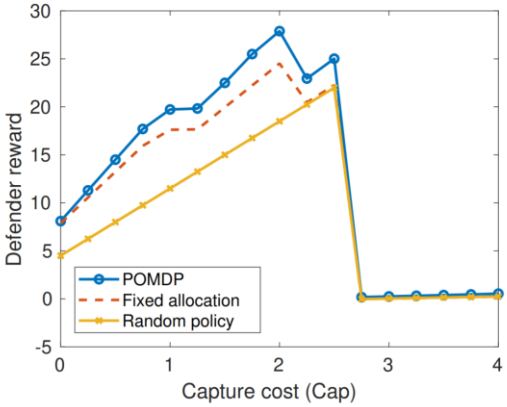

Figure 1. Defender reward against capture cost for a 7-node network

For the second approach described in section 3.2 [29], we developed an algorithm for the OS-POSG. Specifically, a Heuristic Search Value Iteration (HSVI) is used to solve a OS-POSG game modeling a lateral movement problem. The HSVI algorithm leverage a double-oracle algorithm for strategy generation [28].

The game is played over a synthesized computer network. The attacker aims to reach a target node from a source node through the graph edges while minimizing the cost of controlling each of the interconnecting nodes. The attacker can gain control over any of the visited nodes unless countermeasures were taken by the defender, such as the deception mechanism. Using this mechanism, the defender can discover the attacker's location via honeypots. In Figure. 2, we compare three HSVI-based algorithms, also showing the percentage of instances where the algorithms failed to terminate within 2 hours are shown in the bottom. *NH* is the number of honeypots used, and *k* is the average node degree. Figure. 2, clearly illustrates the scalability of the developed heuristic defender algorithm. Our novel algorithms scale several orders of magnitude better compared to the existing state of the art.

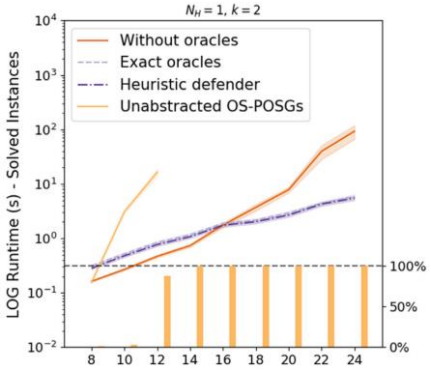

Figure 2. Number of vertices in the network and confidence intervals mark the standard error.

Conclusion

In this paper, we presented a body of work covering cyber deception over attack graphs. We presented several game-theoretic models considering different information structures to capture players' uncertainties. Attack graphs have been used to map out the network topologies along with vulnerabilities of nodes. We highlighted the computational complexity of each game model, especially the partially observable stochastic game model. Solution approaches have been discussed to overcome the intractability of POSGs under specific conditions. Solution approaches have been implemented to solve the proposed game models to generate deception strategies that enhanced network security. To show the effectiveness of cyber deception using the game model, we presented sample numerical results. Our ongoing research focuses on implementing the developed cyber deception in real network settings to refine the model parameters and quantify the deception overhead. We are extending the game model to account for time-varying vulnerabilities.

Acknowledgment

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-19-2-0150. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

1. Al-Shaer, E., Wei, J., Hamlen, K.W., Wang, C.: Towards intelligent cyber deception systems. In: Autonomous Cyber Deception, pp. 21–33. Springer (2019)
2. Almeshekah, M.H., Spafford, E.H.: Cyber security deception. In: Cyber deception, pp. 23–50. Springer (2016)
3. Anwar, A.H., Atia, G., Guirguis, M.: Game theoretic defense approach to wireless networks against stealthy decoy attacks. In: 2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton). pp. 816–821. IEEE (2016)
4. Anwar, A.H., Kamhoua, C., Leslie, N.: Honeypot allocation over attack graphs in cyber deception games. In: 2020 International Conference on Computing, Networking and Communications (ICNC). pp. 502–506. IEEE (2020)
5. Bell, J.B., Whaley, B.: Cheating and Deception. Transaction, New York (1991)
6. Cai, W., Shea, R., Huang, C.Y., Chen, K.T., Liu, J., Leung, V.C., Hsu, C.H.: A survey on cloud gaming: Future of computer games. IEEE Access 4, 7605–7620 (2016)
7. Carroll, T.E., Grosu, D.: A game theoretic investigation of deception in network security. Security and Communication Networks 4(10), 1162–1172 (2011)

8. Cho, J.H., Sharma, D.P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T.J., Kim, D.S., Lim, H., Nelson, F.F.: Toward proactive, adaptive defense: A survey on moving target defense. IEEE Communications Surveys & Tutorials 22(1), 709–745 (2020)
9. Conitzer, V., Sandholm, T.: New complexity results about nash equilibria. Games and Economic Behavior 63(2), 621–641 (2008)
10. Durkota, K., Lisy, V., Bosansky, B., Kiekintveld, C.: Optimal network security hardening using attack graph games. In: Proceedings of the 24th International Joint Conference on Artificial Intelligence (2015)
11. Farhang, S., Hayel, Y., Zhu, Q.: Phy-layer location privacy-preserving access point selection mechanism in next-generation wireless networks. In: 2015 IEEE Conference on Communications and Network Security (CNS). pp. 263–271. IEEE (2015)
12. Fraunholz, D., Schotten, H.D.: Defending web servers with feints, distraction and obfuscation. In: 2018 International Conference on Computing, Networking and Communications (ICNC). pp. 21–25. IEEE (2018)
13. Goldsmith, J., Mundhenk, M.: Competition adds complexity. In: Advances in Neural Information Processing Systems. pp. 561–568 (2008)
14. Kiekintveld, C., Jain, M., Tsai, J., Pita, J., Ordonez, F., Tambe, M.: Computing optimal randomized resource allocations for massive security games. In: Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1. pp. 689–696 (2009)
15. Kiekintveld, C., Lisy, V., Pıbil, R.: Game-theoretic foundations for the strategic use of honeypots in network security. In: Cyber Warfare, pp. 81–101. Springer (2015)
16. La, Q.D., Quek, T.Q., Lee, J., Jin, S., Zhu, H.: Deceptive attack and defense game in honeypot-enabled networks for the internet of things. IEEE Internet of Things Journal 3(6), 1025–1035 (2016)
17. Liao, H.J., Lin, C.H.R., Lin, Y.C., Tung, K.Y.: Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications 36(1), 16– 24 (2013)
18. Madani, O., Hanks, S., Condon, A.: On the undecidability of probabilistic planning and infinite-horizon partially observable markov decision problems. In: AAAI/IAAI. pp. 541–548 (1999)
19. Nguyen, T., Wellman, M.P., Singh, S.: A stackelberg game model for botnet data exfiltration. In: International Conference on Decision and Game Theory for Security. pp. 151–170. Springer (2017)
20. Papadimitriou, C.H., Tsitsiklis, J.N.: The complexity of markov decision processes. Mathematics of operations research 12(3), 441–450 (1987)
21. Pawlick, J., Zhu, Q.: A stackelberg game perspective on the conflict between machine learning and data obfuscation. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS). pp. 1–6. IEEE (2016)
22. Pita, J., Jain, M., Marecki, J., Ordonez, F., Portway, C., Tambe, M., Western, C., Paruchuri, P., Kraus, S.: Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport. In: Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track. pp. 125–132 (2008)
23. Shieh, E., An, B., Yang, R., Tambe, M., Baldwin, C., DiRenzo, J., Maule, B., Meyer, G.: Protect: A deployed game theoretic system to protect the ports of the united states. In: Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 1. pp. 13–20 (2012)

24. Vanek, O., Yin, Z., Jain, M., Bosansky, B., Tambe, M., Pechoucek, M.: Game theoretic resource allocation for malicious packet detection in computer networks. In: AAMAS. pp. 905–912 (2012)
25. Zhang, T., Zhu, Q.: Distributed privacy-preserving collaborative intrusion detection systems for vanets. IEEE Transactions on Signal and Information Processing over Networks 4(1), 148–161 (2018)
26. Shani, G., Pineau, J., Kaplow, R.: A survey of point-based pomdp solvers. Autonomous Agents and Multi-Agent Systems 27(1), 1–51 (2013)
27. Neyman, A., Sorin, S., Sorin, S.: Stochastic games and applications, vol. 570.Springer Science & Business Media (2003)
28. Jain, M., Conitzer, V., Tambe, M.: Security scheduling for real-world networks. In Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems. pp. 215–222. International Foundation for Autonomous Agents and Multiagent Systems (2013)
29. Horák, K., Bošanský, B., Tomášek, P., Kiekintveld, C., Kamhoua, C.: Optimizing honeypot strategies against dynamic lateral movement using partially observable stochastic games. Computers & Security, 87, (2019).
30. Kamdem, G., Kamhoua, C., Lu, Y., Shetty, S., Njilla, L.: A Markov game-theoretic approach for power grid security. In: 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW). pp. 139–144. IEEE (2017)
31. Wang, L., Islam, T., Long, T., Singhal, A., Jajodia, S.: An attack graph-based probabilistic security metric. In: IFIP Annual Conference on Data and Applications Security and Privacy. pp. 283–296. Springer (2008)
32. Anwar, A.H., Kamhoua, C., Leslie, N., Kiekintveld, C.: A game theoretic framework for software diversity for network security. In: International Conference on Decision and Game Theory for Security. Springer (2020)
33. Jia, F., Zhou, K., Kamhoua, C., Vorobeychik, Y.: Blocking adversarial influence in social networks. In: International Conference on Decision and Game Theory for Security. Springer (2020)
34. Milani, S., Shen, W., Chan, K.S., Venkatesan, S., Leslie, N.O., Kamhoua, C.A., Fang, F.: Harnessing the Power of Deception in Attack Graph Games. In: International Conference on Decision and Game Theory for Security. Springer (2020)
35. Kulkarni, A.N., Fu, J., Luo, H., Kamhoua, C.A., Leslie, N.O.: Decoy Placement Games on Graphs with Temporal Logic Objectives. In: International Conference on Decision and Game Theory for Security. Springer (2020)
36. Tsemogne, O., Hayel, Y., Kamhoua, C.A., Deugoue, G.: Partially Observable Stochastic Games for Cyber Deception against Epidemic Process. In: International Conference on Decision and Game Theory for Security. Springer (2020)
37. Xi, B., Kamhoua, C.A.: A Hypergame-based Defense Strategy Toward Cyber Deception in Internet of Battlefield Things (IoBT). Modeling and Design of Secure Internet of Things, Chapter 3, pp. 59–77 (2020)
38. Kamhoua, C.A., Kiekintveld, C.D., Fang, F., Zhu Q.: Game Theory and Machine Learning for Cyber Security. In: Wiley-IEEE press, ISBN: 978-1-119-72392-9, April (2021)
39. Kamhoua, C.A., Njilla, L., Kott, A., Shetty, S.: Modeling and Design of Secure Internet of Things. In: Wiley-IEEE press, ISBN: 978-1-119-59336-2, August (2020)
40. Smith, T., Simmons, R.: Heuristic Search Value Iteration for POMDPs. In: Proceedings Of UAI (2012)

41. Kulkarni, A.N., Luo, H., Leslie, N.O., Kamhoua, C.A., Fu, J.: Deceptive Labeling: Hypergames on Graphs for Stealthy Deception. In: IEEE Control Systems Letters, Vol. 5, No. 3, July (2021)
42. Anwar, A.H., Kamhoua, C., Leslie, N.: A game-theoretic framework for dynamic cyber deception in internet of battlefield things. In: Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. pp. 522–526 (2019)
43. Do, C.T., Tran, N.H., Hong, C., Kamhoua, C.A., Kwiat, K.A., Blasch, E., Ren,S., Pissinou, N., Iyengar, S.S.: Game theory for cyber security and privacy. ACM Computing Surveys (CSUR)50(2), 1–37 (2017)
44. Anwar, A.H., Kelly, J., Atia, G. and Guirguis, M.: Stealthy edge decoy attacks against dynamic channel assignment in wireless networks. In: IEEE Military Communications Conference (MILCOM) pp. 671-676 (2015)
45. Anwar, A.H., Kelly, J., Atia, G. and Guirguis, M.: Pinball attacks against dynamic channel assignment in wireless networks. In: Computer Communications 140 pp. 23-37 (2019)
46. Anwar, A.H., Atia, G. and Guirguis, M.: Adaptive topologies against jamming attacks in wireless networks: A game-theoretic approach. In: Journal of Network and Computer Applications 121 pp. 44-58 (2018)