Moving Target Defense for the CloudControl Game

Koji Hamasaki(✉) and Hitoshi Hohjo

Osaka Prefecture University, Osaka, Japan

Abstract. The recent global spread of cloud computing has streamlined all kinds of tasks by allowing people to go online and get the services they need, when they need them. The cloud is a revolutionary system that saves time, effort, and money. On the other hand, devices connected to the cloud pose the risk of cyber-attacks. One example is Advanced Persistent Threats (APTs), which analyze a target over a long period of time and expose it to danger. The increase in this threat has led to the need for robustness against stealthy attacks. In this paper, we propose Moving Target Defense (MTD) as a defense strategy in the CloudControl game model, which models the interaction between the cloud-connected devices, the defender and the attacker struggling for control of the cloud. We also prove the convergence of this strategy against a static attacker by numerical experiments. Our results contribute to cyber insurance, commercial investment, and corporate policy.

Keywords: Cloud computing · Game theory · Moving Target Defense

1 Introduction

These days the term IoT, which describes physical objects—“things”—connected to the Internet, is often used. At the same time Cyber-Physical Systems (CPS) [1, 2], which is closely related to the IoT, is also getting a lot of attention. CPS is about attaching many sensors to objects to be controlled in the real world, such as people and cars, and analyzing the data collected by these devices in cyberspace and feeding it back to the objects for more optimal control. These technologies will enable a variety of services that have never been available before.

In order to realize CPS/IoT society, a secure and safe networked relationship is needed to communicate. However, with new technology comes the risk of new cyber-attacks, for example, Advanced Persistent Threats (APTs) [3]. They target a specific individual or organization and continuously attack it with a combination of suitable attacks. Because they require a large amount of resources, these attacks are often carried out by huge organizations and have a significant impact on society. Since new technologies such as IoT and CPS have only been created for a short period of time, the vulnerabilities are undiscovered and the risk of a zero-day attacks to exploit them before a fix or countermeasure patch is made is high. APTs are often a combination of these zero-day

© Springer Nature Switzerland AG 2021
T. Nakanishi and R. Nojima (Eds.): IWSEC 2021, LNCS 12835, pp. 241–251, 2021.
https://doi.org/10.1007/978-3-030-85987-9_14

attacks and are highly dangerous. This attack could allow the attacker to take ownership of the cloud to send signals to the device.

In this paper, we propose Moving Target Defense (MTD) [4] as a strategy for the administrator of the cloud which is vulnerable to APT and may be controlled by the attacker. Furthermore, we model a situation in which the device decides whether to trust a command from the cloud controlled by the defender using MTD or the static attacker, and find a Gestalt Nash equilibrium (GNE) through game-theoretic analysis. We clarify that MTD is an effective strategy in this situation. We created a proposed model using the CloudControl game [5, 6]. This game consists of the signaling game and the FlipIt game. The signaling game is a typical incomplete information dynamics game, which have been developed based on the study of two-player language game [7]. Many studies have utilized this game to model various security situations [8–11]. The Flipit game is a recently created game in response to the development of cloud systems [12]. This game is suited for studying systems attacked by APTs [13–19].

Because APTs persistently attack the system, we believe that the defenders can count backwards the time that the defenders have moved since the system's IDs and passwords are no longer available. The attacker should use this information to conduct a dynamic attack. However, the proposed models in [5, 6] used simple and static attacker and defender strategies in the FlipIt game. Van Dijk proposed LM Attacker (LMA) and Defender playing with Exponential Distribution (DED) as dynamic strategies for attackers and defenders in the FlipIt game, respectively [12]. And Hyodo proposed the CloudControl game model that uses the above dynamic strategies in the FlipIt game and proved that GNE exists in the proposed model [20].

In this paper, we show that there is an effective strategy called Moving Target Defense (MTD) in addition to the defender's strategy in the FlipIt game proposed in [12], and we propose the CloudControl game model using that strategy. We also show that GNE is present in that model as well. This can guide the optimal action of defenders and IoT devices against attackers (APTs) who launch advanced attacks. The results of this study will be useful for cyber-insurance, commercial investment and corporate policies.

The remainder of this paper is organized as follows. We proposes the CloudControl game with a defender using MTD in Sect. 2. Then we presents the results of the simulations performed to reveal the presence of GNE in the above proposed model in Sect. 3. We conclude the paper in Sect. 4.

2 Our Model

We model a cloud-based system in which the cloud is the target of APTs. In this model, an attacker capable of APTs can pay the cost and compromise the cloud. The defender, or the cloud administrator, can pay the cost and regain control of the cloud. The cloud sends a message to the device, denoted by r. The device can follow this message, but has an on-board control system to operate autonomously. So it is also possible to use the autonomous motion system without following the message from the cloud.

In this scenario, we uses the CloudControl game that combines two games, the FlipIt game and the signaling game. The FlipIt game takes place between the attacker and the defender, while the signaling game takes place between the possibly compromized cloud and the device. Specifically, the player who controls the resource in the FlipIt game will be the sender of the signaling game.

The model proposed in this study is the CloudControl game model played by a static attacker and a defender using Moving Target Defense (MTD), described below. We investigated whether MTD is an effective strategy against the static attacker (Fig. 1).

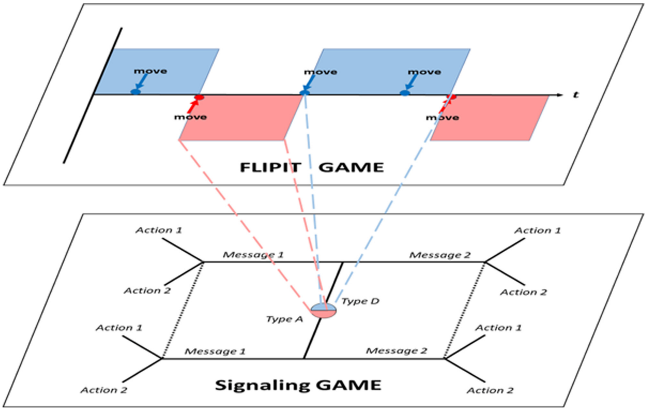

Fig. 1. The CloudControl game. The FlipIt game models the interaction between an attacker and a defender, or a cloud administrator, who compete for ownership of the cloud. The signaling game is played in which the player, who controls the cloud in the FlipIt game, sends a message to a device. The device then decides whether to trust or not to trust the message. (Hyodo, T., Hohjo, H., 2019)

2.1 The Signaling Game in the Proposed Game Model

We describe the symbols used in this study.

- Player: Sender (Cloud(t)), Receiver (Device(r))
- Type of the sender: $T = \{t|t_A, t_D\}$
- Message: $M = \{m|m_L, m_H\}$
- Action: $A = \{a|a_Y, a_N\}$

Player t_A is the attacker and t_D is the defender. In the CloudControl game, the type of the sender is determined by the equilibrium of the FlipIt game. Let m_L and m_H denote low and high risk messages, respectively. After receiving the message, the device chooses an action. Action a_Y represents trusting the message from the cloud, and a_{N} represents not trusting it.

Let $\sigma^S_{t_A}(m)$, $\sigma^S_{t_D}(m)$ be the strategy in which player t_A, t_D sends a message m, and $\sigma^S_r(a|m)$ be the strategy in which the device r takes an action a when it receives a message m. Also let $u^S_{t_A}(m, a)$, $u^S_{t_D}(m, a)$ be the utilities players t_A, t_D gain. Then the expected utilities $\overline{u}^S_{t_A}\left(\sigma^S_{t_A}, \sigma^S_r\right)$, $\overline{u}^S_{t_D}\left(\sigma^S_{t_D}, \sigma^S_r\right)$ in the signaling game of the attacker and defender is as follows.

$$\overline{u}_{t_A}^S\left(\sigma_{t_A}^S,\sigma_r^S\right)=\sum\nolimits_{a\in A}\sum\nolimits_{m\in M}u_{t_A}^S(m,a)\sigma_r^S(a|m)\sigma_{t_A}^S(m) \tag{1}$$

$$\overline{u}_{t_D}^S\left(\sigma_{t_D}^S,\sigma_r^S\right)=\sum\nolimits_{a\in A}\sum\nolimits_{m\in M}u_{t_D}^S(m,a)\sigma_r^S(a|m)\sigma_{t_D}^S(m) \tag{2}$$

Let $\mu(t|m)$ be the belief that the receiver determines the type of the sender is t and $\sigma_r^S(t,m,a)$ be the utility that he gains when he receives the message m, then his expected utility $\overline{u}_r^S\left(\sigma_r^S|m,\mu\right)$ in the signaling game is as follows.

$$\overline{u}_r^S\left(\sigma_r^S|m,\mu\right)=\sum\nolimits_{a\in A}\sum\nolimits_{m\in M}u_r^S(t,m,a)\mu(t|m)\sigma_r^S(a|m) \tag{3}$$

Let p be the probability that an attacker sends a message. The receiver's belief that the sender is in state t when he receives the message m is as follows.

$$\mu(t_A|m)=\frac{\sigma_{t_A}^S(m)p}{\sigma_{t_A}^S(m)p+\sigma_{t_D}^S(m)(1-p)} \tag{4}$$

Each player updates their strategy each game to maximize their own expected utility. We used the ARP model proposed by Bereby-Meyer & Erev [21] to update the strategy. This model is more human-like by learning with reference to the current and past reward values. The ARP model is described below.

The probability $Q_n(time)$ of taking a move n at time is given by

$$Q_n(time)=\frac{q_n(time)}{\sum q_n(time)} \tag{5}$$

$q_n(time)$ is the pure value at the move n and is updated with each passing *time*.Let g_j be the reward for choosing a move j at *time*, then the renewal formula is given by

$$q_n(time+1)=\max\left\{\upsilon,(1-\phi)q_n(time)+E_j\left(n,L_{time}\left(g_j\right)\right)\right\}, \tag{6}$$

where φ is the forgetting rate and v is the guaranteed value. Also the functions E_j and L_{time} are given by

$$E_j\left(n,L_{time}\left(g_j\right)\right)=\begin{cases}L_{time}\left(g_j\right)(1-\varepsilon) & (j=n)\\ L_{time}\left(g_j\right)\varepsilon & (otherwise)\end{cases} \tag{7}$$

$$L_{time}\left(g_j\right)=g_j-\rho(time), \tag{8}$$

where the parameter ε is the weight of the reward. The $\rho(time)$ in Eq. (8) is an important function in the ARP model. As mentioned above, the ARP model learns rewards and the function $\rho(time)$ plays the role. It is given by

$$\rho(time+1)=\begin{cases}\left(1-c^+\right)\rho(time)+\left(c^+\right)g_j & (g_j\geq\rho(time))\\ \left(1-c^-\right)\rho(time)+\left(c^-\right)g_j & (g_j<\rho(time))\end{cases} \tag{9}$$

c^+ and c^- are parameters representing the impact of the next reward when the reward g_j was better and worse than the evaluation function $\rho(time)$, respectively.

2.2 The FlipIt Game in the Proposed Game Model

The FlipIt game in the original CloudControl game is a two-player game in which the attacker and the defender compete for one shared resource along a timeline. In this paper, we envision a system in which a defender can prevent an attack by moving the resource through the network. In the next subsection, we describe the defender's strategy in the proposed game model.

Moving Target Defense (MTD). MTD is a defender's strategy to migrate resources to node i through a fully connected network of $n (n \geq 2)$ nodes with a probability of $p(i)$. Defenders can use this strategy to prevent attackers from discovering vulnerabilities and critical resources in their systems. In other words, this model assumes a situation where the target resource is not visible to the attacker. For simplicity, we assume that the MTD in this study randomly migrates resources to all nodes (Fig. 2).

$$p(i) = \frac{1}{n}, i = 1, \ldots, n \tag{10}$$

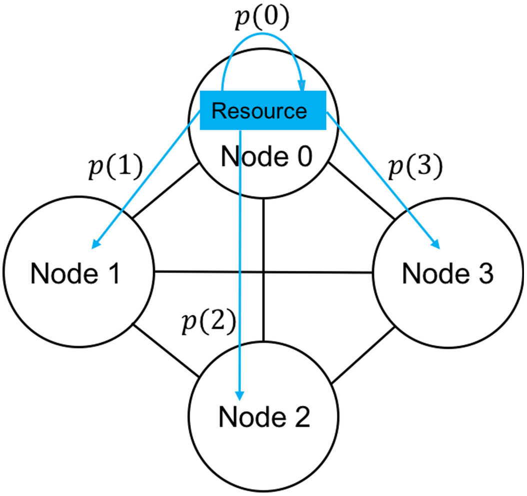

Fig. 2. Moving Target Defense (MTD) when the number of nodes is 3. The defender can migrate a resource to other node, through a fully connected network. $p(0) = p(1) = p(2) = p(3) = 1/4$.

The FlipIt Game with MTD. Let the number of nodes be n. The rules of the FlipIt game in this case are as follows.

- The game begins with the defender in control of the resource on *node* 0 ($time = 1$).
- Both players follow their own strategies at a certain *time* and determine whether to pay the moving cost.
- When the defender moves, he takes the ownership of the resource and may or may not migrate it to another node.

- When the attacker moves, he selects one node at random to attack. The attacker takes the ownership of the resource only if he attacks a node where the resource actually exists.
- When both players move at the same time, the defender takes the ownership of the resource.

For each FlipIt game, the player who controls the resource becomes the sender and plays multiple signaling games with the device (the receiver).

The expected utilities $\overline{u}^F_{t_A}(\alpha_{t_A}, \alpha_{t_D})$, $\overline{u}^F_{t_D}(\alpha_{t_A}, \alpha_{t_D})$ of the FlipIt game for the attacker and defender in the proposed model is as follows.

$$\overline{u}^S_{t_\mathrm{A}}\left(\alpha_{t_A}, \alpha_{t_D}\right) = \overline{u}^S_{t_A}\frac{p}{n} - k_{t_A}\alpha_{t_A} \tag{11}$$

$$\overline{u}^S_{t_D}\left(\alpha_{t_A}, \alpha_{t_D}\right) = \overline{u}^S_{t_D}\left(1 - \frac{p}{n}\right) - k_{t_D}\alpha_{t_D} \tag{12}$$

where $\alpha_{t_A}, \alpha_{t_D}$ is the attacker's and defender's strategy in the FlipIt game, $\overline{u}^S_{t_A}, \overline{u}^S_{t_D}$ is the attacker's and defender's expected utility in the signaling game, p is the probability of the attacker controlling the resource at either node, and k_{t_A}, k_{t_D} is the attacker's and defender's moving cost.

3 Numerical Experiments

In this study, numerical experiments were conducted to identify the existence of GNE. The value of the ARP model used to update the strategy of the signaling game was set to $(\phi, \upsilon, \varepsilon, c^+, c^-, q_n(0)) = (0.001, 0.0001, 0.2, 0.01, 0.02, 1000)$ from [21].

The procedure of the game is as follows.

Step 1. Players are a static attacker and a defender that use MTD, and a device. At the start of the game, all players use a random strategy.
Step 2. The attacker and defender play the FlipIt game ($time < 4000$). Each time the player controlling the resource plays the signaling game with the device, and updates the signaling game strategy.
Step 3. From the expected utility of the signaling game, attackers and defenders find the FlipIt game strategy that maximizes the expected utility of the FlipIt game.
Step 4. The attacker and the defender reset the signaling game strategy and return to a random state.

We repeated Step 2 to Step 4 above 100 times to examine the variability of the expected utilities of attacker and defender in the signaling game and the strategies of both players in the FlipIt game. Also the signaling game was played enough times to reach equilibrium.

Table 1. The gain of the attacker, the defender and the device in the signaling game.

(Sender, Receiver)		Device	
		a_Y	a_N
Attacker	m_L	(12, -1)	(-40, 10)
	m_H	(30, -40)	(-40, 10)
Defender	m_L	(16, 20)	(-10, -5)
	m_H	(3, 3)	(-10, -5)

The gain in the signalling game was set up as shown in the Table 1. The number on the left is the sender's (attacker or defender) gain and the number on the right is the receiver's (device) gain.

We first experimented with fixed $n = 3$ and not fixed k_{t_A}, k_{t_D}. Figure 3 shows the result of the experiment for $k_{t_A} = 20$, $k_{t_D} = 15$. In the top graph, the red dots represent the attacker's expected utility $\overline{\mathrm{u}}^S_{t_A}$ in the signaling game, and the blue dots represent the defender's expected utility $\overline{u}^S_{t_D}$ in the signaling game, with the vertical axis representing the expected utility and the horizontal axis representing the number of sets. In the bottom graph, the red dots represent the attacker's strategy α_{t_A} in the FlipIt game, and the blue dots represent the defender's strategy α_{t_D} in the FlipIt game, with the vertical axis representing the strategy and the horizontal axis representing the number of sets. In this situation, the expected utilities of the attacker and defender in the signaling game and their strategies in the FlipIt game converged to a certain value, respectively. This indicates a convergence to GNE. The converged values were $\overline{u}^S_{t_A} = 12$, $\overline{u}^S_{t_D} = 16$, $\alpha_{t_A} = 0.12$, and $\alpha_{t_D} = 0.15$.

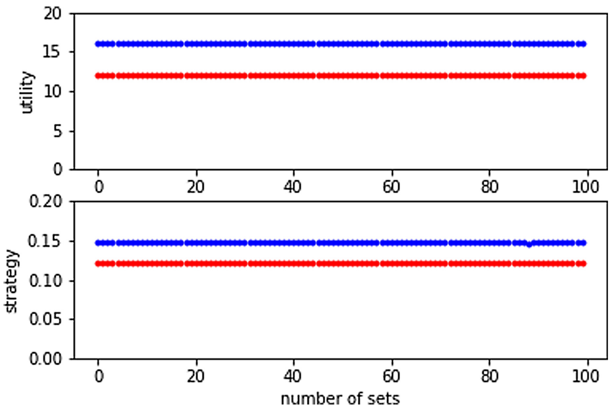

Fig. 3. The changes in the expected utilities $\overline{u}^S_{t_A}, \overline{u}^S_{t_D}$ and strategies $\alpha_{t_A}, \alpha_{t_D}$ with $n = 3, k_{t_A} = 20, k_{\mathrm{t}_D} = 15$.

Figure 4 shows the result of the experiment for $k_{t_A} = 40, k_{t_D} = 30$. In this situation, $\alpha_{t_A} = \alpha_{t_D} = 0.00$. This shows that the attacker and the defender have the strategy of not moving in the FlipIt game even if the signaling game's utility conditions of Table 1. were met. From Eq. (11), (12), the expected utility of the FlipIt game is smaller as the moving cost increases. If they don't benefit from attacking, they won't bother attacking because they won't have to.

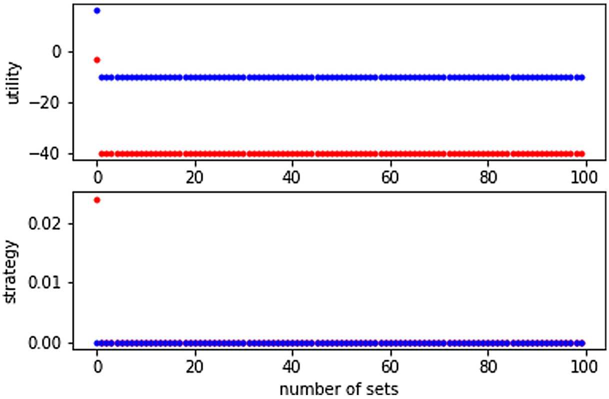

Fig. 4. The changes in the expected utilities $\overline{u}^S_{t_A}, \overline{u}^S_{t_D}$ and strategies $\alpha_{t_A}, \alpha_{t_D}$ with $n = 3, k_{t_A} = 40, k_{t_D} = 30$.

Next, we experimented with fixed $k_{t_A} = 20, k_{t_D} = 15$ and not fixed n. Figure 5 shows the result of the experiment for $n = 5$. In this situation, the expected utilities of the attacker and defender in the signaling game and their strategies in the FlipIt game converged to a certain value, respectively. This indicates a convergence to GNE. The converged values were $\overline{u}^S_{t_A} = 12, \overline{u}^S_{t_D} = 16, \alpha_{t_A} = 0.09$, and $\alpha_{t_D} = 0.07$.

Figure 6 shows the result of the experiment for $n = 10$. In this situation, $\alpha_{t_A} = \alpha_{t_D} = 0.00$. This shows that the attacker and the defender have the strategy of not moving in the FlipIt game. From their results, we found that even when the number of nodes n is large, the attacker chooses not to move. In this situation, that is to say, the attacker cannot find the actual location of the resource among the multiple nodes and gives up on attacking it. However, we don't take into account the costs of building a fully connected network with multiple nodes and of migrating a resource. Therefore, in the real world, if the number of nodes n is large, the defender is likely to have to pay more costs.

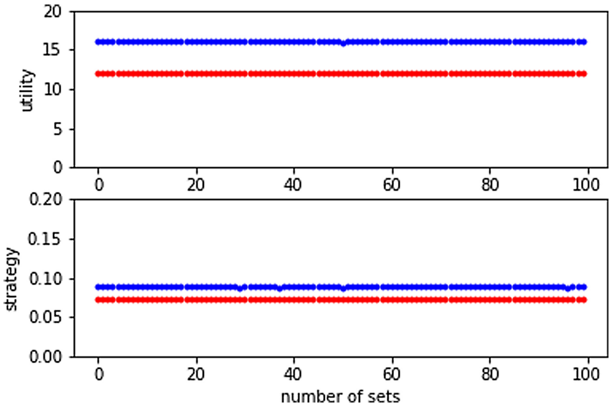

Fig. 5. The changes in expected utilities $\overline{u}^S_{t_A}, \overline{u}^S_{t_D}$ and strategies $\alpha_{t_A}, \alpha_{t_D}$ with $n = 5, k_{t_A} = 20, k_{t_D} = 15$.

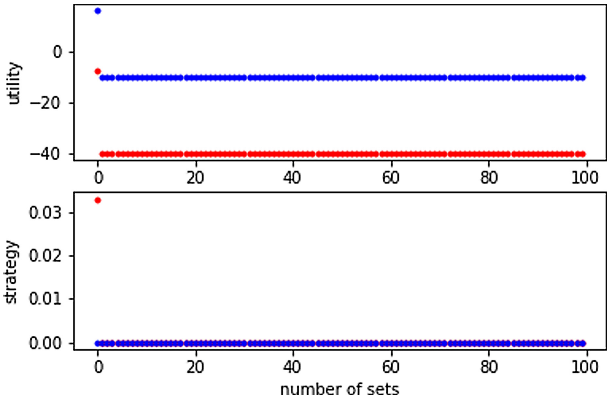

Fig. 6. The changes in the expected utilities $\overline{u}^S_{t_A}, \overline{u}^S_{t_D}$ and strategies $\alpha_{t_A}, \alpha_{t_D}$ with $n = 10, k_{t_A} = 20, k_{t_D} = 15$.

4 Conclusion and Future Work

In this paper, we proposed the cloud control game with a static attacker and a defender using MTD and showed that GNE exists in the proposed model. This equilibrium will help protect cloud-connected CPSs by revealing the frequency of attacks by attackers launching APTs in the future IoT/CPS society and the optimal strategies for MTD and IoT devices against these attackers.

However, the only thing revealed in this study is the presence of GNE in the proposed model. Its equilibrium equation is not clear.

In future work, it is important to find the equilibrium equation in the proposed model. We would also like to revisit a model that takes into account the cost of building the network and of migrating a resource. Furthermore, APTs in the real world are likely to launch more sophisticated attacks. Therefore, we want to clarify whether MTD is an effective strategy for defenders even against advanced and dynamic attackers, and whether GNE exists even in such a model.

References

1. Baheti, R., Gill, H.: Cyber-physical systems. Impact Control Technol. **12**, 161–166 (2011)
2. Lee, E.A.: Cyber physical systems: design challenges. In: 2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC) on Proceedings, Orlando, FL, USA, pp. 363–369. IEEE (2008)
3. Tankard, C.: Advanced persistent threats and how to monitor and deter them. Netw. Secur. **2011**(8), 16–19 (2011)
4. Feng, X., Zheng, Z., Cansever, D., Swami, A., Mohapatra, P.: A signaling game model for moving target defense. In: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications on Proceedings, Atlanta, GA, USA, pp. 1–9. IEEE (2017)
5. Pawlick, J., Farhang, S., Zhu, Q.: Flip the cloud: cyber-physical signaling games in the presence of advanced persistent threats. In: Khouzani, M., Panaousis, E., Theodorakopoulos, G. (eds.) Decision and Game Theory for Security. LNCS, vol. 9406, pp. 289–308. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25594-1_16
6. Pawlick, J., Zhu, Q.: Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. IEEE Trans. Inf. Forensics Secur. **12**, 2906–2919 (2017)
7. Lewis, D.: Convention: A Philosophical Study, 1st edn. Harvard University Press, Cambridge (1969)
8. Casey, W., Morales, J.A., Wright, E., Zhu, Q., Mishra, B.: Compliance signaling games: toward modeling the deterrence of insider threats. Comput. Math. Organ. Theory **22**(3), 318–349 (2016). https://doi.org/10.1007/s10588-016-9221-5
9. Casey, W., Weaver, R., Morales, J.A., Wright, E., Mishra, B.: Epistatic signaling and minority games, the adversarial dynamics in social technological systems. Mob. Netw. Appl. **21**(1), 161–174 (2016). https://doi.org/10.1007/s11036-016-0705-9
10. Christian, E., Choi, C.: Signaling game based strategy for secure positioning in wireless sensor network. Pervasive Mob. Comput. **40**, 611–627 (2017)
11. Khalil, I., Eitan, A., Haddad, M.: Signaling game based approach to power control management in wireless network. In the 8th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks on Proceedings, pp. 139–144. Association for Computing Machinery, New York (2013)
12. van Dijk, M., Juels, A., Oprea, A., Riveat, R.L.: Flipit: the game of “stealthy takecover.” J. Cryptol. **26**, 655–713 (2013). https://doi.org/10.1007/s00145-012-9134-5
13. Laszka, A., Horvath, G., Felegyhazi, M., Buttyan, L.: FlipThem: modeling targeted attacks with FlipIt for multiple resources. In: Poovendran, R., Saad, W. (eds.) Decision and Game Theory for Security. LNCS, vol. 8840, pp. 175–194. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-12601-2_10
14. Zhang, R., Zhu, Q.: FlipIn: a game-theoretic cyber insurance framework for incentive-compatible cyber risk management of internet of things. IEEE Trans. Inf. Forensics Secur. **15**, 2026–2041 (2019)
15. Feng, X., Zheng, Z., Hu, P., Cansever, D., Mohapatra, P.: Stealthy attacks meets insider threats: a three-player game model. In: MILCOM 2015 - 2015 IEEE Military Communications Conference on Proceedings, Tampa, FL, USA, pp. 25–30. IEEE (2015)
16. Oakley, L., Oprea, A.: QFlip: an adaptive reinforcement learning strategy for the FlipIt security game. In: Alpcan, T., Vorobeychik, Y., Baras, J.S., Dán, G. (eds.) Decision and Game Theory for Security. LNCS, vol. 11836, pp. 364–384. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32430-8_22

17. Bowers, K.D., et al.: Defending against the unknown enemy: applying FlipIt to system security. In: Grossklags, J., Walrand, J. (eds.) Decision and Game Theory for Security. LNCS, vol. 7638, pp. 248–263. Springer, Cham (2012). https://doi.org/10.1007/978-3-642-34266-0_15
18. Greige, L., Chin, S.: Reinforcement learning in FlipIt. arXiv preprint arXiv: 2002.12909 (2020)
19. Feng, X., Zheng, Z., Hu, P., Cansever, D., Mohapatra, P.: Stealthy attacks with insider information: a game theoretic model with asymmetric feedback. In: MILCOM 2016 - 2016 IEEE Military Communications Conference on Proceedings, Baltimore, MD, USA, pp. 277–282. IEEE (2015)
20. Hyodo, T., Hohjo, H.: The Gestalt Nash equilibrium analysis in cyber security. In: RIMS Kokyuroku 2126, pp. 9–18. Kyoto University, Kyoto (2019). (in Japanese)
21. Bereby-Meyer, Y., Erev, I.: On learning to become a successful loser: a comparison of alternative abstractions of learning processes in the loss domain. J. Math. Psychol. **42**, 266–286 (1998)