Hindawi
Security and Communication Networks
Volume 2020, Article ID 3151495, 12 pages
https://doi.org/10.1155/2020/3151495

Research Article

Optimal Timing Selection Approach to Moving Target Defense: A FlipIt Attack-Defense Game Model

Jing-lei Tan,[1,2] **Heng-wei Zhang**,[1,2] **Hong-qi Zhang**,[1,2] **Cheng Lei**,[1,2] **Hui Jin**,[1,2] **Bo-wen Li**,[1,2] **and Hao Hu**[1,2]

[1]*PLA SSF Information Engineering University, Zhengzhou, China*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China*

Correspondence should be addressed to Heng-wei Zhang; wlby_zzmy_henan@163.com

Received 11 December 2019; Revised 3 February 2020; Accepted 24 February 2020; Published 9 June 2020

Academic Editor: Cristina Alcaraz

The centralized control characteristics of software-defined networks (SDNs) make them susceptible to advanced persistent threats (APTs). Moving target defense, as an effective defense means, is constantly developing. It is difficult to effectively characterize an MTD attack and defense game with existing game models and effectively select the defense timing to balance SDN service quality and MTD decision-making benefits. From the hidden confrontation between the actual attack and defense sides, existing attack-defense scenarios are abstractly characterized and analyzed. Based on the APT attack process of the Cyber Kill Chain (CKC), a state transition model of the MTD attack surface based on the susceptible-infective-recuperative-malfunctioned (SIRM) infectious disease model is defined. An MTD attack-defense timing decision model based on the FlipIt game (FG-MTD) is constructed, which expands the static analysis in the traditional game to a dynamic continuous process. The Nash equilibrium of the proposed method is analyzed, and the optimal timing selection algorithm of the MTD is designed to provide decision support for the selection of MTD timing under moderate security. Finally, the application model is used to verify the model and method. Through numerical analysis, the timings of different types of attack-defense strategies are summarized.

1. Introduction

With the continuous development of cyberattacks, such as advanced persistent threats (APTs), cybersecurity faces significant challenges [1]. The software-defined network (SDN), as a next-generation network system, is vulnerable to a variety of security threats [2]. Due to the characteristics of the centralized control of SDNs, SDN controllers have become single-point attack targets. Meanwhile, the southbound interface between the control and data layers is vulnerable to network attacks, such as scanning detection, distributed denial of service (DDoS), and fraudulent implantation. Therefore, it is urgent to analyze and predict the security attack and defense behaviors of SDNs. To solve these problems and deter threats faced by SDNs, a moving target defense (MTD), as a "game changing" defense idea, aims to thwart attackers using continuous and dynamic changes, reducing their success rate and increasing the cost and complexity of threats [3, 4].

Although researchers have proposed MTD strategy-selection methods in different network security scenarios, the key to defense is to maximize the revenue by changing the transform timing and selecting the transform attribute values in a limited transform space. Therefore, to study the optimal timing of MTD is particularly important [5–8]. How to choose the MTD timing based on the network attack-defense sides, balance the network availability and MTD security, and maximize the MTD revenue have become key topics in current research. Game theory [9] is an analysis tool to describe the interactions between decision-making subjects. The FlipIt game, as a game theory framework for modeling computer security scenarios, has been widely used in attack-defense scenarios, such as targeted attack modeling, encryption key updates, password policy resets, and cloud auditing. However, few scholars have applied it to study the timing of MTD [10]. This paper is mainly concerned with analyzing the optimal equilibrium point of

attack-defense timing strategies in the framework of the FlipIt game to guide the MTD defender on how to trigger the timing of the implementation.

Based on analysis of the literature, the SDN as the research object and an APT as an attack instance were selected in this study, and an MTD optimal timing selection approach based on the FlipIt game is proposed. The main contributions of this paper are as follows:

(1) The state transition model of the MTD attack surface based on the susceptible-infective-recuperative-malfunctioned (SIRM) infectious disease model is established. The MTD attack and defense process is described as the transformation of the attack surface state, which provides state-variable support for the MTD timing selection model construction and game analysis.

(2) The MTD timing selection model based on the FlipIt game (FG-MTD) was built, which represents the confrontation process between the attack-defense sides as the control of the right side of the attack surface, which is more suitable for the real network attack and defense processes.

(3) The impact of timing on the game revenue is analyzed, and we propose an MTD timing selection algorithm, which provides decision support for the timing of MTD with moderate security.

(4) By numerically analyzing the impact of the MTD attack-defense period and cost on the attack-defense revenue, a FlipIt game theory framework is constructed for the timing of MTD implementation.

The remainder of this paper is organized as follows. Section 2 introduces the basic principles of game theory and the FlipIt game and analyzes the research progress of MTD timing selection. The characteristics of the MTD attack–defense confrontation are described in Section 3. FG-MTD is constructed in Section 4. The game of dynamic attack and defense is described by the FlipIt game. On this basis, the existence of equilibrium of FG-MTD is analyzed. An optimal timing selection algorithm of FG-MTD is designed. Finally, an application example shows that the constructed model conforms to the MTD characteristics and can effectively describe the MTD attack–defense confrontation process and select timing to guide the implementation of MTD.

2. Related Work

This section firstly summarizes the research of FlipIt game and then summarizes the research progress of MTD timing from three aspects. Finally, the shortcomings of the existing results of MTD timing are analyzed, and the research ideas and main work of this paper are explained.

2.1. Basic Principles of Game Theory and FlipIt Game. Game theory is a mathematical tool for studying different players' decision-making processes. The basic assumption is that each player makes rational decisions and considers the optimal strategy while considering other players' decision-making processes. Nash equilibrium is a solution to describe the equilibrium state of the game, in which every player obtains the best return, and a strategy that deviates from the Nash equilibrium always leads to smaller gains.

In 2013, Dijk et al. [11] of the RSA Lab in the United States proposed the FlipIt game for APT attacks. The schematic diagram is shown in Figure 1 [11]. Unlike most games, FlipIt consists of defenders, attackers, and public resources, which allows the players to control public resources at a certain cost of action at any time. However, before the actions of players, the control of public resources is not displayed, so "stealthy takeover" is the most unique feature for the FlipIt game. The goal of each player is to maximize control of resource time while minimizing the cost of action.

The blue and red circles represent the actions of the defender and attacker, respectively. The blue and red shading of a rectangle indicate control of a public resource by the defender and attacker, respectively. The defender has control at time $t = 0$.

In a theoretical study, Bowers et al. [10] examined the application scenarios of the FlipIt game in practical problems, including password reset, key rotation, refreshing a virtual machine (VM), and cloud service auditing. Nochenson and Grossklags [12] studied the FlipIt game of safe real-time strategic behavior and further extended FlipIt game theory by confronting human participants with computer opponents. In practical applications, Lee et al. [13] introduced a cybernetic approach to model competitive malware in the FlipIt game. Pawlick et al. [14] used a combined game of FlipIt and a signal game to describe the interactions between attackers, defenders, and cloud-linking devices. The game between defenders and invisible attackers was investigated [15], and it was found that a periodic defense strategy was the best response for nonadaptive attackers. The FlipThem game extends FlipIt to a set of known multiple resources, and the attacker attempts to destroy one or all of them [16]. In one study [17], internal threats were introduced to the FlipIt game, and the three-player game model was studied. However, the authors considered a multiserver model and adopted a simulation-based solution.

Some scholars have used FlipIt to study MTD. Jones et al. destroyed the attack knowledge by allowing the defender to "mutate" the system, and they extended FlipIt to MTD [18]. Prakesh et al. used multitarget detection resource control to study the MTD [19].

2.2. Timing of MTD Attack Surface Transformation. Research of MTD attack surface transformation timing can be mainly divided into categories of time-driven active MTD (TD-MTD), event-driven reactive MTD (ED-MTD), and time-event hybrid-driven MTD (TE-MTD) strategies. In TD-MTD strategies, the MTD attack surface transformation time is divided into a fixed period (FT-MTD) and random period (RT-MTD), which is an active triggering method to predict the possible network attack behavior by changing the system parameters (such as the IP address, port number, and

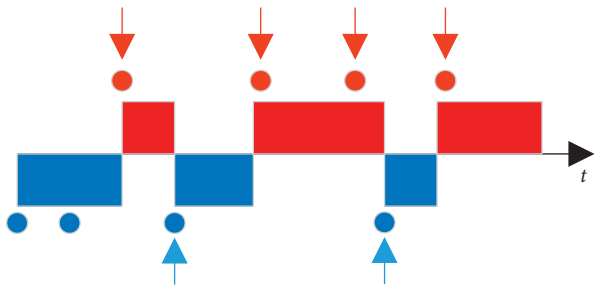

Figure 1: FlipIt game.

MAC address) [20, 21]. However, TD-MTD depends too much on historical experience. In ED-MTD strategies, auxiliary information, such as specific security alerts and security policies, is used to trigger MTD attack surface actions. Unlike TD-MTD, ED-MTD is triggered passively, and the attack surface of the network system adaptively changes [22, 23]. For example, our team [24] maximized the hopping space by routing and port cooperative random hopping. We detected the malicious detection of the attacker and adjusted the hopping to reduce the hopping overhead. However, ED-MTD exhibits a significant hysteresis in response to attacks.

TE-MTD can be based on a fixed-cycle time-event hybrid-driven MTD strategy (FTE-MTD) or a random-cycle time-event hybrid-driven MTD strategy (RTE-MTD). Huang and Ghosh [25] proposed a turn-based model based on server diversification using a server with the same function but different structures to perform attack surface actions. It could be triggered by events, or it could use a randomly selected or fixed action period. Kampanakis et al. [26] proposed an MTD attack surface transformation model based on an SDN. The network parameters were randomized in a fixed time period to trigger the attack surface action, and an analysis engine collected real-time security incidents on the network and evaluated potential attacks by analyzing existing ones. Zangeneh and Shajari [27] modeled ED-MTD using the competitive Markov decision process (CMDP), and the TE-MTD relied on historical alarm data. Thus, the attack surface is transformed more efficiently by combining TD-MTD and ED-MTD.

However, the theoretical analysis framework of the MTD timing problem has not been constructed. MTD timing research has an important focus with application significance, in which the timing problem is integrated and systematic. The work of this paper mainly focuses on the MTD timing strategy. Using the FlipIt game model, the influence on the offensive and defensive gains of different transform frequencies and attack-defense costs is analyzed to guide the timing of MTD.

3. Analysis of Network Attack-Defense Process

The network attack and defense behavior is first modeled in terms of the control of the attacker and defender over the attack surface. The network confrontation process is analyzed from the perspectives of the attacker and the defender. The player can dynamically adjust according to the game history information. In response to information feedback during the game, to fit real network attack and defense scenarios, the MTD timing selection model-based FlipIt game is described from the perspective of incomplete information. The attack-defense confrontation scenarios are then analyzed from the perspectives of attackers and defenders.

3.1. Analysis of Attack Process Based on Cyber Kill Chain. The purpose of network attacks is to determine the vulnerability of the attack surface by analyzing the target system, introduce security threats by using the vulnerability attack surface, and cause loss by carrying out intrusion behaviors. Cyber Kill Chain (CKC) is a widely used sectional model to describe network intrusion. Created by the Lockheed Martin Corporation, it can be used to collect relevant data and for the classification and correlation of attacks. CKC describes common intrusive behavioral patterns used by attackers on network targets [28]. The analysis of the CKC attack stage is important for MTD decision making, which can help network security personnel deploy appropriate defense strategies for different attack stages. Therefore, we must describe different phases of CKC targeting APT scenarios and use them to understand how to use MTD strategies in different phases of the CKC.

The CKC divides attack actions into eight strategies, each of which may be recursive or incoherent, and multiple leapfrog intrusions are implemented based on the results of the previous invasion. As shown in Figure 2, CKC can be divided into left-of-exploitation and right-of-exploitation attack types. Left-of-exploitation attack types are used mainly to detect the target system and build an arsenal by identifying it, and targeting can be used to detect vulnerabilities of the target-system resources. According to the results of the analysis, the corresponding attack tools and methods, which can be defined as a lower-level attacker, can be divided into two attack strategies, D_{A_1} and D_{A_2}. Right-of-exploitation attack types are mainly used to carry out attacks and expand the scope of the damage by implementing an attack target system to achieve the desired state. Using similar vulnerability to expand the range to improve the effect of the attack, which can be defined as high-level attacker, the attack can be divided into six attack strategies D_{A_3}, D_{A_4}, D_{A_5}, D_{A_6}, D_{A_1}, and D_{A_1}.

3.2. Analysis of MTD Attack Surface Transformation Based on SIRM Infectious Disease Model. As discussed in Section 3.1, the attack behavior is persistent, so the following assumptions are defined.

Assumption 1. The attack surface cannot be completely controlled by the attacker immediately.

Assumption 2. The attacker's attack behavior does not have a priority path in the network.

The state transition caused by the attack and defense sides alternately controlling the attack surface must be characterized. In a real network attack and defense

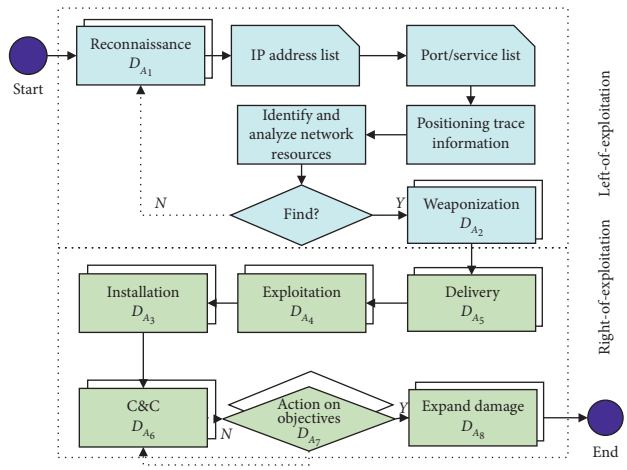

Figure 2: Implementation process of different attack strategies in CKC.

confrontation scenario, the process of CKC exploitation of the vulnerable attack surface to infiltrate and control other attack surfaces is similar to the virus propagation mechanism of the SIR infectious disease model [29]. Hence, the extended SIR infectious disease model is used to describe the state transition of the attack surface in the attack-defense process. According to the basic definition of the attack surface and the moving attack surface [30], we define the following four categories of the state of the network attack surface.

Definition 1. Susceptible attack surface (SAS): The attack surface is in a safe state, but it is highly likely to be attacked because no defense measures have been taken.

Definition 2. Infective attack surface (IAS): The attack surface has been attacked but is still in the attack stage of a low-level attacker. The defender is difficult to detect, and the attack surface is in an infected state.

Definition 3. Recuperative attack surface (RAS): The attack surface is protected by the defense strategy and has an immune effect on the attack behavior. Thus, the attack surface is in an immune state.

Definition 4. Malfunctioned attack surface (MAS): The attack surface is completely controlled by the attacker and is in a damaged state. The network cannot provide services normally.

The relationship between these four attack surface states is shown in Figure 3.

We assume that the total number of network attack surfaces is AAS. The numbers of attack surfaces in the above states at time t are SAS(t), IAS(t), RAS(t), and MAS(t), $\forall t \in [t_0, T]$. Furthermore, $\mathrm{SAS}(t), \mathrm{IAS}(t), \mathrm{RAS}(t), \mathrm{MAS}(t) \geq 0$ and $\mathrm{SAS}(t) + \mathrm{IAS}(t) + \mathrm{RAS}(t) + \mathrm{MAS}(t) = \mathrm{AAS}$.

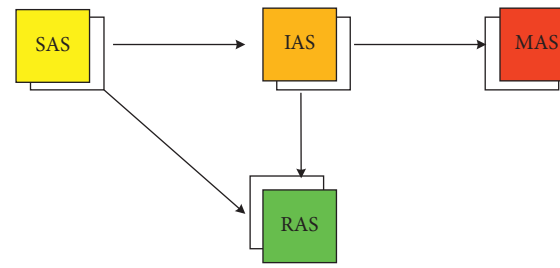

Figure 3: State transformation of MTD network attack surface in a SIRM model.

To simplify the analysis, we categorize a defense strategy as either a low-level conventional or high-level strategy. We use the four attack surface states to model the transformation process of the MTD attack surface.

(i) SAS ⟶ IAS: When SAS faces APT low-level (left-of-exploitation) attack strategies, if the low-level defense strategies fail, then SAS is infected by the APT attacker. At this point, the attacker is still in the left-of-exploitation preparation phase of the attack, and the system does not experience decreased service quality. However, the APT attacker can use IAS to exploit another SAS to achieve further attack effects. For example, when an APT attacker discovers system vulnerability, it is not eager to launch an attack but instead continually raises authority to achieve higher control rights.

(ii) SAS ⟶ RAS: When the SAS faces APT low-level (left-of-exploitation) attack strategies, if the low-level strategy is successful, then the SAS is converted to a RAS, which can have a certain defense effect on the APT attack. For example, the defender adopts a strategy such as patch upgrading to resist the reconnaissance tracking strategy of the APT attack.

(iii) IAS ⟶ RAS: When the IAS faces APT high-level (right-of-exploitation) attack strategies, if the high-level MTD strategy is successful, then the IAS will be converted to a RAS to avoid system damage. For example, defenders use network fingerprints, forwarding path hopping, and other strategies to prevent APT attackers from installing an implant attack strategy.

(iv) IAS ⟶ MAS: When the IAS faces APT high-level (right-of-exploitation) attack strategies, if the high-level MTD strategy fails, then the IAS will be converted to a MAS, and the system gradually loses the service function. For example, an APT attacker bypasses the defense strategy through a load delivery strategy, causing the system to be broken and causing service interruptions.

In summary, as $\forall t \in [t_0, T]$, $\mathrm{SAS}(t) + \mathrm{IAS}(t) + \mathrm{RAS}(t) + \mathrm{MAS}(t) = \mathrm{AAS}$, the differential equations of the MTD

network attack surface state transition based on the SIRM infectious disease model are expressed as

$$\begin{cases} \dot{\mathrm{SAS}} = -\dfrac{\alpha \mathrm{IAS}(t)\mathrm{SAS}(t)}{\mathrm{AAS}} - \beta \mathrm{SAS}(t), \\ \dot{\mathrm{IAS}} = \dfrac{\alpha \mathrm{IAS}(t)\mathrm{SAS}(t)}{\mathrm{AAS}} - \lambda \mathrm{IAS}(t) - \mu \mathrm{IAS}(t), \\ \dot{\mathrm{RAS}} = \beta \mathrm{SAS}(t) + \mu \mathrm{IAS}(t), \\ \dot{\mathrm{MAS}} = \lambda \mathrm{IAS}(t). \end{cases} \tag{1}$$

The above differential equations describe the rate of change of the SAS, IAS, RAS, and MAS with time, which provides state variables for the construction of the FG-MTD model in the next section, where α is the probability of changing from a SAS to an IAS, β is the probability of transforming from an IAS to a RAS, λ is the probability of transforming from an IAS to a MAS, and μ is the probability of transforming from an IAS to a RAS.

4. Construction of MTD FlipIt Attack-Defense Game Model

4.1. MTD Timing Selection Based on the FlipIt Attack-Defense Game Model. Based on the analysis in Section 3, the FlipIt game based on the MTD timing selection model is defined below, including the total game time, the set of offensive and defensive participants, the offensive and defensive game states, the attack and defense action set, the participant timing period strategy space, and the offensive and defensive utility function six basic elements.

Definition 5. FG-MTD can be formalized as a sextuple, $\mathrm{FG-MTD} = (N, T, S, D, P, U)$.

(1) $N = (N_A, N_D)$ is the player set of the attack-defense game, where N_D is the defender and N_A is the attacker.

(2) $T = T_A + T_D \in [0, +\infty)$ is the time horizon of the attack-defense game, i.e., the sum of the total times T_A and T_D for which the attacker and defender control the attack surface, respectively.

(3) $S = (S_A, S_D)$ is the set of network states in the attack-defense confrontation process, whose details are in Section 3.2.

(4) $D = (D_A, D_D)$ is the set of offensive and defensive action vectors in FG-MTD, where $D_A = \{D_{A^1}, D_{A_2}, \ldots, D_{A_n}\}$ is the set of optional attack actions, which can be categorized as high- and low-level attack strategies, whose details are provided in Section 3.1. Similarly, $D_D = \{D_{D_1}, D_{D_2}, \ldots, D_{D_m}\}$ is the set of optional defense actions, which can be categorized as high- and low-level defense strategies, where the high-level defense strategies consist of six MTD strategies and the low-level defense strategies consist of four conventional strategies, whose details are shown in Section 5.1. At any time t, attackers and defenders may take action to gain control of the attack surface.

(5) $P = (P_A, P_D)$ is the attack-defense time period strategy set of the FG-MTD, where $P_A = \{P_{A_1}, P_{A_2}, \ldots, P_{A_n}\}$ and $P_D = \{P_{D_1}, P_{D_2}, \cdots, P_{D_m}\}$, respectively, which indicate collections of attacker- and defender-selectable time period strategies. Both are decided by the durations of four attack surfaces in the SIRM model randomly, where $P_A = (t_j - t_i) \cdot \int_{t_i}^{t_j} \dot{\mathrm{SAS}} + \dot{\mathrm{IAS}} + \dot{\mathrm{MAS}}\, \mathrm{d}t$ and $P_D = (t_j - t_i) \cdot \int_{t_i}^{t_j} \dot{\mathrm{RAS}}\, \mathrm{d}t$.

(6) $U = (U_A, U_D)$ is the utility set of the attacker and defender, where U_A and U_D represent the utility functions of the attacker and defender, respectively. The calculation method is shown in Section 4.2.

4.2. Attack-Defense Time Strategy Utility Quantification. The quantification of the attack-defense timing is the basis for the timing of MTD selection, and whether the quantification is reasonable directly affects the timing selection result. To objectively measure the utility, the approach in this paper is based on the FG-MTD timing selection model, and the attack-defense time period is treated as a unified indicator of utility. We make the following definitions.

Definition 6. Attack-defense cost (C_{AD}): The attack-defense cost is $C_{AD} = \{C_A, C_D\}$, where C_A is the attack cost, and C_D is the defense cost. The two costs vary for different elements of the offensive and defensive action set. The attack cost is determined by the complexity of the attack and increases with the attack complexity, and the defense cost increases similarly with the complexity of the defense implementation.

Definition 7. Attack-defense benefit (B_{AD}): The attack-defense benefit is $B_{AD} = \{B_A, B_D\}$, which indicates the direct benefits from both the offense and defense. For the scenario of the MTD timing selection, we define the attack-defense benefit with the game time, i.e., $T = B_A + B_D$.

Definition 8. Attack-defense benefit rate ($r_{B_{AD}}$): The attack and defense benefits are normalized to simplify the calculation, so $r_{ADB} = r_{AB} + r_{DB} = 1$.

Definition 9. Attack-defense utility (U_{AD}): The attack-defense utility $U_{AD} = B_{AD} - C_{AD}$ is the difference between the attack-defense benefits and costs. The attack utility is $U_A = B_A - C_A$, and the defense utility is $U_D = B_D - C_D$.

Definition 10. Attack-defense utility rate ($\theta_{U_{AD}}$): The attack-defense utility is normalized to simplify the calculation, so the attack-defense utility yield is $\theta_{U_{AD}} = \theta_{U_A} + \theta_{U_D}$, where the attack utility yield is $\theta_{U_A} = \liminf_{t \longrightarrow \infty} \theta_{U_A}(t)$ and the defense utility yield is $\theta_{U_D} = \liminf_{t \longrightarrow \infty} \theta_{U_D}(t)$.

4.3. Game Equilibrium Solution and Algorithm Design. We first explain FG-MTD game strategy and then analyze the use of the utility function to solve the game equilibrium strategy.

We use the attack-defense time strategy set (P_A, P_D) to define the game model of the FG-MTD, FG-MTD(P_A, P_D). According to basic game theory concepts [11], the FG-MTD (P_A, P_D) Nash equilibrium strategy is

$$\begin{aligned} &\text{FG-MTD}\left(P_A, P_D^*\right) \geq \text{FG-MTD}\left(P_A, P_D\right), \\ &\text{FG-MTD}\left(P_A^*, P_D\right) \geq \text{FG-MTD}\left(P_A, P_D\right). \end{aligned} \tag{2}$$

We assume that the APT attack time period P_A is greater than the defense time period P_D, and let $\eta = P_D/P_A$ be the probability of an attacker's random action during the defense time period. The APT attacker controls the period within the defense time period, which is represented by $\eta/2$. FG-MTD is a non-zero-sum game. We define the attacker utility function

$$U_A = B_A - C_A = \frac{\eta}{2} - \frac{C_A}{P_A} = \frac{P_D}{2P_A} - \frac{C_A}{P_A}, \tag{3}$$

and defense utility function

$$U_D = B_D - C_D = 1 - \frac{\eta}{2} - \frac{C_D}{P_D} = 1 - \frac{P_D}{2P_A} - \frac{C_D}{P_D}. \tag{4}$$

When $P_A \leq P_D$, we can obtain the attacker and defender utility functions as follows:

$$\begin{aligned} U_A &= 1 - \frac{P_A}{2P_D} - \frac{C_A}{P_D}, \\ U_D &= \frac{P_A}{2P_D} - \frac{C_D}{P_D}. \end{aligned} \tag{5}$$

Theorem 1. *A Nash equilibrium exists for the FlipIt game based on the MTD model of the FG-MTD, FG-MTD(P_A, P_D):*

$$\begin{cases} P_D^* = \dfrac{1}{2 \cdot C_A},\ P_A^* = \dfrac{C_D}{2 \cdot C_A^2},\ C_D < C_A, \\ P_D^* = P_A^* = \dfrac{1}{2 \cdot C_A}, \quad C_D = C_A, \\ P_D^* = \dfrac{C_D}{2 \cdot C_A^2},\ P_A^* = \dfrac{1}{2 \cdot C_A}, \quad C_D > C_A. \end{cases} \tag{6}$$

The related proofs of Theorem 1 can be found in [11].

Based on FG-MTD and its equilibrium calculation process, the optimal MTD timing selection algorithm for the FG-MTD is given as Algorithm 1.

5. Case Study and Numerical Analysis

Below, we present an attack-defense scenario based on the APT and SDN and show an example with different attack-defense strategies to validate the effectiveness of the FG-MTD. The designed optimal MTD timing selection algorithm is verified by a series of numerical analyses. In addition, we compare our method to others.

5.1. Case Environment. We will use the SDN part node topology to build an experimental network environment [31]. As shown in Figure 4, LDAP servers, FTP servers, application servers, and other servers are the application targets 1 of the MTD strategies, where the application server acts as the control server. Meanwhile, the APT attacker invades the availability of the SDN network according to the illustrated intrusion path. APT attackers have user-level access to the LDAP servers, and their goal is to steal the sensitive information stored in a Linux database server. The vulnerability information of each server is shown in Table 1.

The possible attack paths for the APT attacker are as follows:

Path 1: LDAP Servers ⟶ FTP Servers ⟶ Linux Database

Path 2: LDAP Servers ⟶ Application Servers ⟶ FTP Servers ⟶ Linux Database

Based on the analysis of the network attack-defense process presented in Section 3 and literature results [30], the attack-defense actions are shown in Table 2. There are eight attack strategies, as shown in Section 3.1.1. There are ten defense strategies, including six high-level MTD strategies, i.e., the IP address, communication port, communication protocol, forwarding path, fingerprint, and data storage hopping, and four low-level conventional defense strategies, i.e., monitoring and detection, patch upgrade, data deletion, and service shutdown.

5.2. Numerical Analysis. Based on the time strategy set of attack-defense players, we will evaluate the proposed FG-MTD model by numerical analysis. First, according to the utility quantification method presented in Section 4.2, we use the basic definition of the time game return function to analyze the state of the attack surface of the MTD network over time. The trends are shown in Figure 5.

As time passes, the number of SASs declines and the number of RASs increases, while for the IAS and MAS, their number has been relatively small. From the [0, 6] time period, the number of SASs decreased by 95.4%. Meanwhile, due to appropriate MTD defense timing, the RASs increased by 93.2% during the [0, 4] time period. This shows that the choice of defense timing is important for MTD. Improper defense timing will lead to an increase in the proportion of IASs, which will lead to system malfunction.

We take $P_A > P_D$ as an example. As for the specific types of attack-defense strategies, the quantitative numerical analysis of the impact of MTD implementation timing on the attack-defense utility is carried out.

Figure 6 shows the relationship between the attack utility and period for different types of attack strategies. In the defense period $P_D = 1$, for high-level attack strategies, as the attack period increases, the attack utility is still increasing. The attack period has little effect on high-level attack strategies, and the key factor of the profit of the level attack strategies is the attack cost. Because low-level attack strategies have lower attack costs, their attack income trends downward as the attack period increases. Therefore, the

Input FG-MTD Model
Output Optimal Timing P_D^*
BEGIN
Initialize FG − MTD = (N, T, S, D, P, U)
// Initialize MTD optimal timing selection model FG-MTD
Initialize D_A, D_D
// Initialize the action space for attack–defense players
Initialize $P_A = \{P_1, \ldots, P_n\}$, $1 \le k \le n$
// Initialize the defender time period strategies space P_D
Initialize $P_D = \{P_1, \ldots, P_m\}$, $1 \le i \le m$
// Initialize the defender time period strategies space P_A based on historical attack data
For $(k = 1; k \le n; k++)$
For $(i = 1; i \le m; i++)$
{
If $P_A > P_D$
Calculate $\begin{cases} U_A = (P_D/2P_A) - (C_A/P_A), \\ U_D = 1 - (P_D/2P_A) - (C_D/P_D), \end{cases}$
Else
Calculate $\begin{cases} U_A = 1 - (P_A/2P_D) - (C_A/P_D), \\ U_D = (P_A/2P_D) - (C_D/P_D). \end{cases}$
}
// Traverse each type of attack and calculate the attack–defense strategy combination utility
Output P_D^*
// Output optimal timing
END

Algorithm 1: FG-MTD game optimal timing selection algorithm.

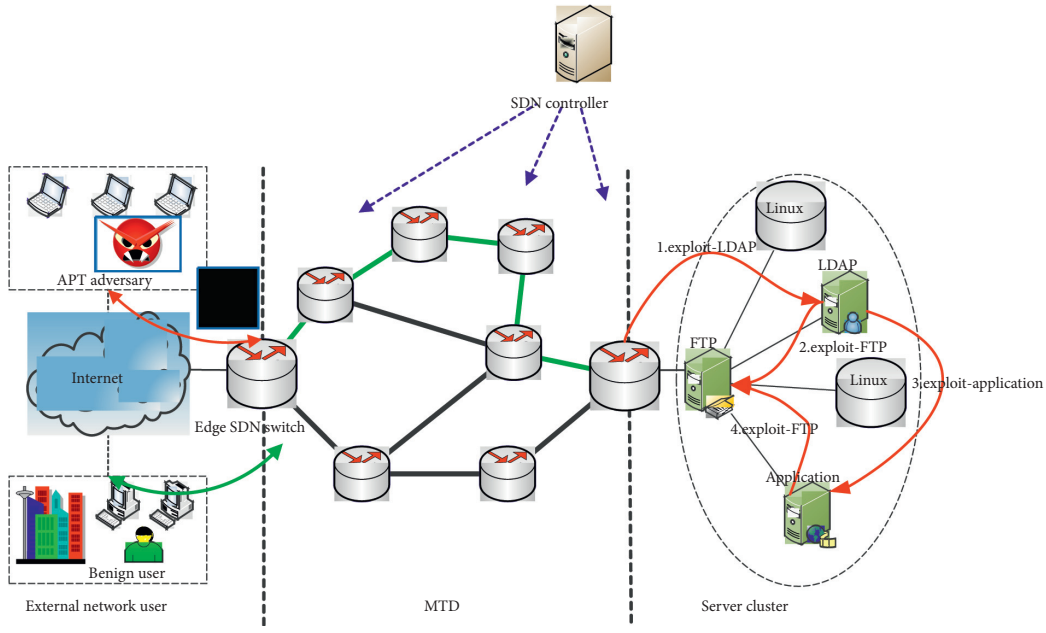

Figure 4: Experimental system structure diagram.

Table 1: Server vulnerability information.

Endpoint name	Vulnerability information	CVE ID
FTP servers	Incorrect access control vulnerability	CVE-2019-12815
Application servers	Remote desktop services execution code vulnerability	CVE-2019-0708
LDAP servers	String length processing vulnerability	CVE-2015-5330

Table 2: Description of network attack and defense strategies in the experiment.

Number	Attack–defense strategies	Strategy description
D_{A_1}	Reconnaissance	Detect valuable information about target system
D_{A_2}	Weaponization	Create targeted attack payloads for target system
D_{A_3}	Delivery	Deliver payload to target system
D_{A_4}	Exploit	Penetration exploits to trigger malicious code
D_{A_5}	Installation	Install malware on target system
D_{A_6}	Command and control (C&C)	Remote control of target system through C&C
D_{A_7}	Action on objectives	Achieve damage to target system
D_{A_8}	Expand damage	Horizontal action in target system to expand scope of attack damage
D_{D_1}	IP address hopping	{IP, C}
D_{D_2}	Communication port hopping	{port, 64512}
D_{D_3}	Communication protocol hopping	{protocol, 5}
D_{D_4}	Forwarding path hopping	{forwarding path, 576}
D_{D_5}	Fingerprint hopping	{fingerprint, 128}
D_{D_6}	Data storage hopping	{data storage, 2^{12}}
D_{D_7}	Monitoring detection	Monitor process behavior using IDS
D_{D_8}	Patch upgrade	Repair damaged network resources by installing patches
D_{D_9}	Data deletion	Delete related data in the communication service
$D_{D_{10}}$	Service close	Close current service function

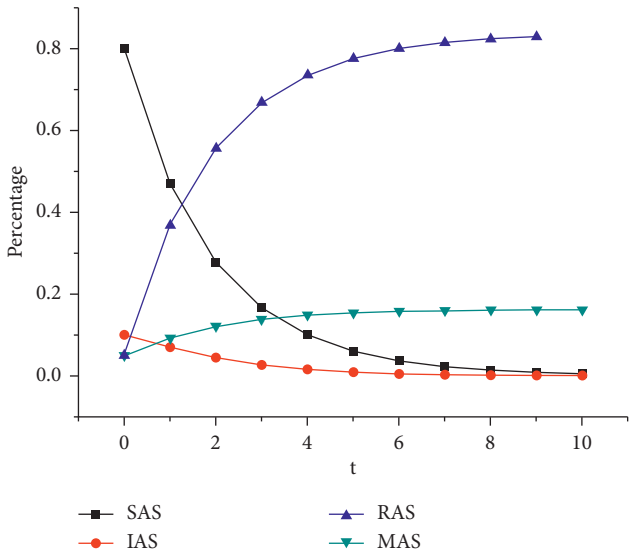

Figure 5: Proportion of states of different MTD network attack surfaces changing with time.

attack period has a significant impact on their attack utility. Similarly, as the attack cost increases, the attack utility trends downward for both high- and low-level attack strategies.

In Figure 7, when the defense period is fixed, with the increase in the attack period, the attack utility will increase for a high-level attack strategy and decrease for a low-level attack strategy. The attack period has less impact on the high-level attack strategies because their attack utility is still increasing. As the defense period decreases, the attack utility decreases for both high- and low-level attack strategies. The defense period is crucial for defending against different types of attackers.

For different attack periods, the relationship between the defense utility and defense period is as follows. The defense period step is 0.5. As shown in Figure 8, for low-level defense strategies, as the defense period increases, the defense utility first increases and then decreases. In particular, when the attack period is $P_A = 5.5$, the best defense period is $P_D^* = [3.29, 3, 34]$, during which the defense utility is $U_D^* = 0.3970$. When the attack period is $P_A = 7$, the best defense period is $P_D^* = [3.71, 3.78]$, during which the defense utility is $U_D^* = 0.4655$. Thus, for the low-level defense strategies, there is an optimal defense period for the different attack periods, which maximizes the defense utility. For high-level defense strategies, the defense utility increases continuously as the defense period increases. Therefore, the influence of the defense period is small for high-level defense strategies. Different attack periods have less impact on it, but due to the higher deployment cost, its defense utility is lower than that of low-level defenders. The defense utility continues to decrease as the attack period increases, and when the defense period is too large, the defense utility will continue to decrease.

As for different types of defense strategies, the relationship between the defense utility and defense period is as follows, where the step of the defense period is 0.5. As shown in Figure 9, when the fixed attack period is $P_A = 6$, the defense utility of high-level defense strategies increases with the increase in the defense period. As the defense period increases and approaches the attack period, the impact of the defense period on the defense gain gradually decreases. The low-level attack utility increases with the increase in the defense period, and the defense utility increases first and then decreases. In particular, when the defense cost is $C_D = 0.5$, the best defense period is $P_D^* = 2.45$, and the best defense utility is $U_D^* = 0.5918$. When the defense cost is $C_D = 1.5$, the best defense utility is $U_D^* = 0.2929$, and the defense period can be randomly selected in the range of 4.20–4.28. The defense utility decreases with increasing defense costs for both high- and low-level defense strategies.

In summary, we conclude the following from our numerical experiments.

Therefore, for key core devices, a high-level defense strategy can be used to implement MTD with a larger

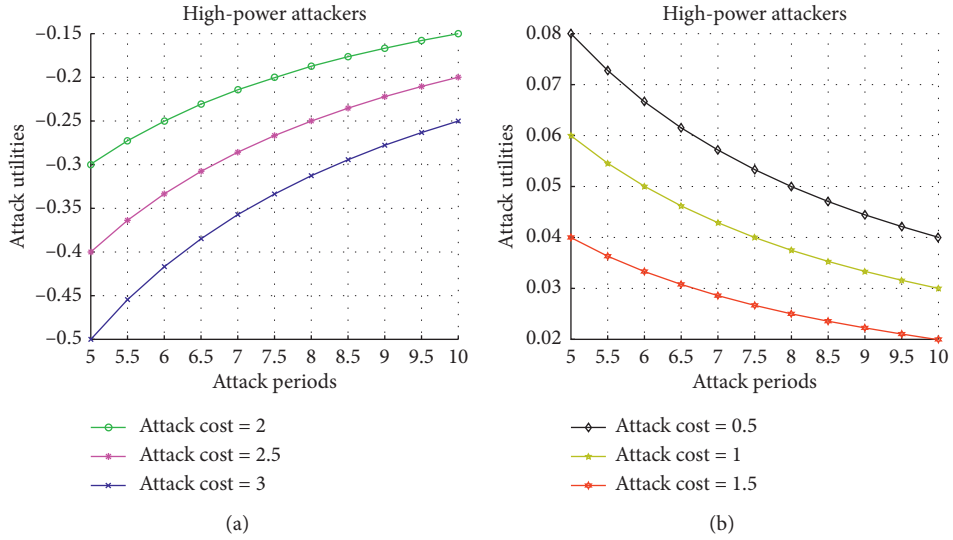

Figure 6: Attack cost and utility relationship diagram for different types of attack strategies.

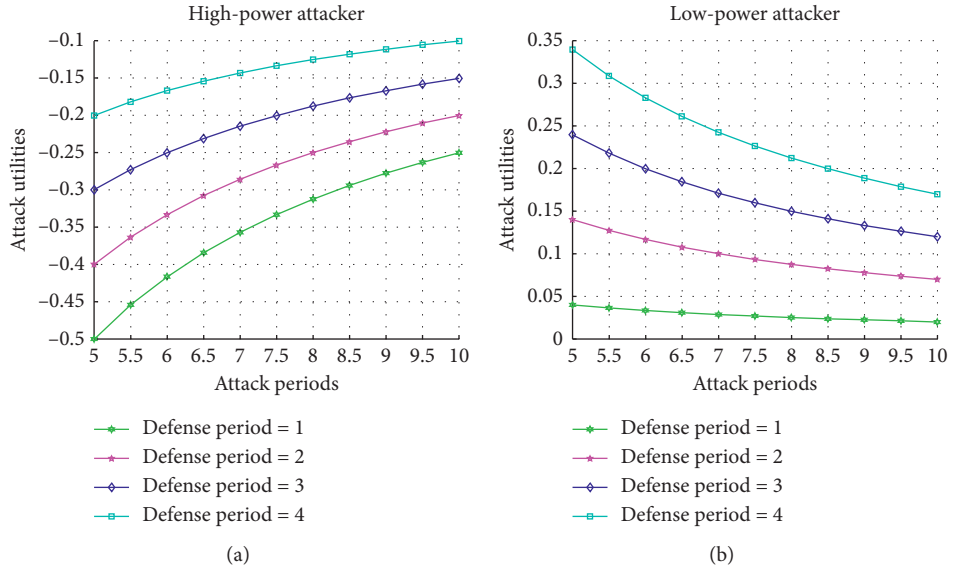

Figure 7: Defense period and utility relationship diagram of different types of attack strategies.

defense cycle. For noncore devices, a low-level defense strategy can be used to implement MTD with an appropriate defense cycle.

5.3. Analysis and Comparison of Results. Comparisons between our research and existing research are summarized in Table 3. Most MTD decision-making research focuses on spatial strategy-selection methods while ignoring the timing factors that are equally important for defense decision making. Manadhata et al. studied a two-person nonzero and complete information stochastic game for spatial strategy selection. Kambhampati et al. proposed a spatial strategy-selection method based on a Bayesian game. However, this static single-stage game model has difficulty describing attack-defense scenes. Liu et al. proposed an MTD spatial strategy-selection method based on a signaling game and built a method for MTD attack-defense cost quantification, but the approach cannot accurately describe the dynamic characteristics of MTD. Based on this, a Markov MTD spatial strategy selection was established in our earlier work. We described the transformation process of the MTD state through a Markov decision process, and we provided an optimal defense strategy-selection algorithm. Chowdhary et al. studied MTD spatial strategy detection based on an incomplete-information stochastic dynamic game-in-a-cloud network environment. The above research focused on MTD spatial strategy selection. Our work introduces the FlipIt game to the MTD timing decision. A CKC-based attack method and MTD network attack surface

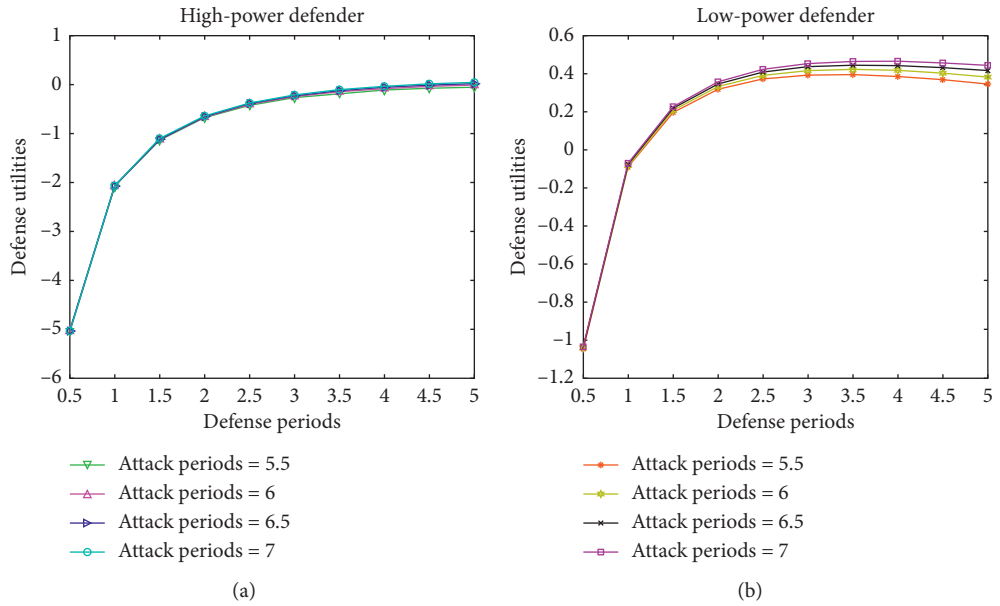

Figure 8: Attack period and utility relationship diagram of different types of defense strategies.

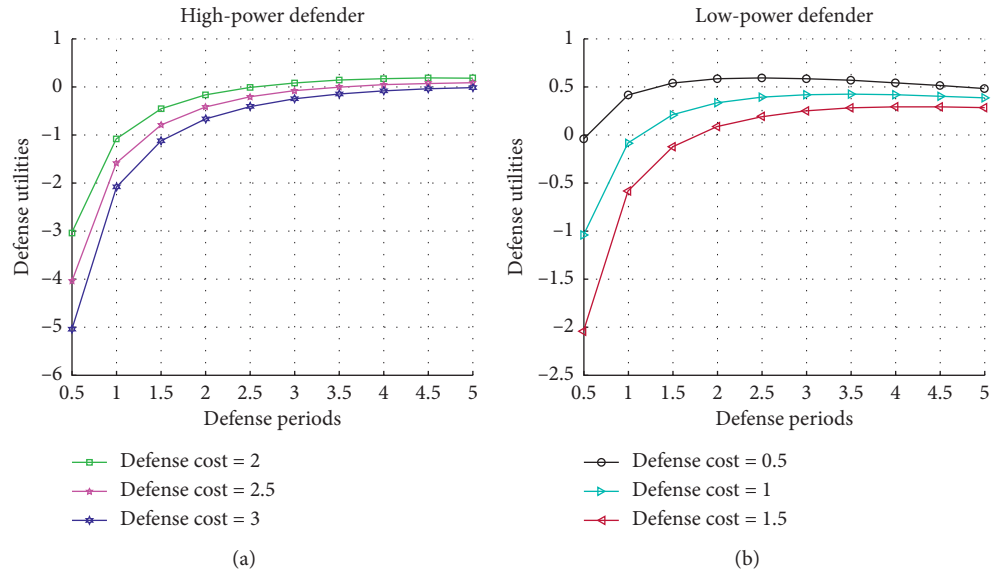

Figure 9: Defense cost and utility relationship diagram of different types of defense strategies.

Table 3: Comparisons of different methods for MTD strategy solution.

Literature	Game type	Information type	Decision-making objectives	Dynamic	Optimal solution method
Manadhata et al.	Stochastic game	Complete information	Spatial strategy selection	Static	Not given
Kambhampati et al.	Bayesian game	Complete information	Spatial strategy selection	Static	Not given
Liu et al.	Signaling game	Incomplete information	Spatial strategy selection	Dynamic	Given
Lei et al.	Markov game	Complete information	Spatial strategy selection	Static	Given
Chowdhary et al.	Markov game	Incomplete information	Spatial strategy selection	Dynamic	Not given
Our method	FlipIt game	Incomplete information	Temporal strategy selection	Dynamic	Given

transformation method based on the SIRM infectious disease model were analyzed. A model of FG-MTD is proposed, which provides theoretical support for MTD timing.

(1) The defense period and attack cost are the main factors affecting the attack utility. For high-level attack strategies, the attack cost has a much greater

impact than the attack period on the attack utility, and for low-level attack strategies, the attack period is negatively correlated with the attack utility. The attack timing problem is particularly important for low-level attackers. Therefore, it is important to find the optimal defense timing to resist attacks.

(2) The defense cost is the main factor affecting the defense utility. For low-level defense strategies, there is an optimal defense timing, so the defense period plays a key role. For high-level defense strategies, the defense cost is a key factor that constrains its utility. Therefore, to reduce the implementation cost of an MTD strategy is a key breakthrough in strategy design.

6. Conclusion

With the rapid development of SDNs, their security faces significant challenges. MTD is a new active defense strategy that can change the rules of the game. However, the decision-making problem of MTD timing based on game theory is still in its infancy. There are still many limitations in terms of the theoretical basis, game model, and equilibrium solution. It is difficult to solve the MTD timing problem to establish a general and effective theoretical method to guide MTD timing decisions.

Based on the timing of MTD decision making, we introduced APT attack behavior based on CKC and analyzed the attack surface transformation process of MTD based on the SIRM infectious disease model. Based on this, we constructed an MTD model based on the FlipIt game, presented the benefits for both sides, and provided methods for performing the calculations and determining the equilibrium solution. We also introduced a timing selection algorithm for FG-MTD. The applicability and effectiveness of the FG-MTD model and algorithm were verified by examples, numerical experiments, and comprehensive comparisons. The theoretical basis of MTD timing selection was established. We plan to test our method on real SDN systems and explore the efficacy of our model in real MTD settings. In future research, we will explore MTD spatiotemporal decision-making methods and consider the corresponding game models.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Authors' Contributions

Jing-lei Tan and Heng-wei Zhang contributed equally to this work.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (Grant no. 2016YFF0204003) and the National Natural Science Foundation of China (Grant no. 61471344).

References

[1] L.-X. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou, "Effective repair strategy against advanced persistent threat: a differential game approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1713–1728, 2019.

[2] V. Varadharajan, K. Karmakar, U. Tupakula, and M. Hitchens, *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 897–912, 2018.

[3] V. Heydari, S. I. Kim, and S. M. Yoo, "Scalable anti-censorship framework using moving target defense for web servers," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 5, pp. 1113–1124, 2017.

[4] J. H. Jafarian, E. Al-Shaer, and D. Qi, "An effective address mutation approach for disrupting reconnaissance attacks[J]," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 12, pp. 2562–2577, 2015.

[5] A. Nochenson and J. Grossklags, "Moving target defense for web applications using Bayesian stackelberg games: (extended abstract),"in *Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems*, pp. 1377-1378, New York, NY, USA, June 2013.

[6] L. Jiang, Z. Hong-Qi, and L. Yi, "Research on optimal selection of moving target defense policy based on dynamic game with incomplete information," *Acta Electronica Sinica*, vol. 46, no. 1, pp. 82–89, 2018.

[7] C. Lei, D. H. Ma, and H. Q. Zhang, "Optimal strategy selection for moving target defense based on Markov game," *IEEE Access*, vol. 5, pp. 156–169, 2017.

[8] A. Chowdhary, S. Sengupta, D. Huang, and S. Kambhampati, "Markov game modeling of moving target defense for strategic detection of threats in cloud networks," 2018, https://arxivorg/abs/1812.09660.

[9] A. R. Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in IoT-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4405–4414, 2019.

[10] K. D. Bowers, M. V. Dijk, R. Griffin et al., "Defending against the unknown enemy: applying FLIPIT to system security," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, 2012.

[11] M. V. Dijk, A. Juels, A. Oprea et al., "FlipIt: the game of "stealthy takeover," *Journal of Cryptology*, vol. 26, no. 4, pp. 655–713, 2013.

[12] A. Nochenson and J. Grossklags, "A behavioral investigation of the FlipIt game," in *Proceedings of the 12th Workshop on the Economics of Information Security (WEIS)*, Springer, Washington, DC, USA, June 2013.

[13] P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran, "A host takeover game model for competing malware," in *Proceedings of the IEEE Conference on Decision and Control*, IEEE, Osaka, Japan, pp. 4523–4530, December 2015.

[14] J. Pawlick, S. Farhang, and Q. Zhu, "Flip the cloud: cyber-physical signaling games in the presence of advanced persistent threats," in *Proceedings of the 6th International Conference on Decision and Game Theory for Security (GameSec)*, Springer, London, UK, pp. 289–308, 2015.

[15] M. Zhang, Z. Zheng, and N. B. Shroff, "Stealthy attacks and observable defenses: a game theoretic model under strict resource constraints," in *Proceedings of the 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 813–817, IEEE, Atlanta, GA, USA, December 2014.

[16] A. Laszka, G. Horvath, M. Felegyhazi, and L. B. Flipthem, "Modeling targeted attacks with flipit for multiple resources," in *Lecture Notes in Computer Science*, pp. 175–194, Springer, Berlin, Germany, 2014.

[17] X. Feng, Z. Zheng, P. Hu, D. Cansever, and P. Mohapatra, "Stealthy attacks meets insider threats: a three-player game model," in *Proceedings of the MILCOM 2015 - 2015 IEEE Military Communications Conference*, pp. 25–30, IEEE, Tampa, FL, USA, October 2015.

[18] S. Jones, A. Outkin, J. Gearhart et al., "Evaluating moving target defense with PLADD," Sandia National Laboratories (SNL-NM), Albuquerque, NM, USA, SAND2015-8432R607305, 2015.

[19] A. Prakash and M. P. Wellman, "Empirical game-theoretic analysis for moving target defense," in *Proceedings of the Second ACM Workshop on Moving Target Defense*, ACM, Denver, CO, USA, pp. 57–65, October 2015.

[20] F. Gillani, E. Al-Shaer, S. Lo, Q. Duan, M. Ammar, and E. Zegura, "Agile virtualized infrastructure to proactively defend against cyber attacks," in *Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 729–737, IEEE, Hong Kong, China, 2015.

[21] M. Taguinod, A. Doupé, Z. Zhao, and G.-J. Ahn, "Toward a moving target defense for web applications," in *Proceedings of the IEEE International Conference on Information Reuse and Integration (IRI)*, pp. 510–517, IEEE, San Francisco, CA, USA, August 2015.

[22] S. A. DeLoach, X. Ou, R. Zhuang, and S. Zhang, "Model-driven, moving-target defense for enterprise network security," in *Models@run.time*, pp. 137–161, Springer, Berlin, Germany, 2014.

[23] R. Lent, "Evaluating a migration-based response to dos attacks in a system of distributed auctions," *Computers & Security*, vol. 31, no. 3, pp. 327–343, 2012.

[24] H.-Q. Zhang, C. Lei, D.-X. Chang, and Y.-J. Yang, "Network moving target defense technique based on collaborative mutation," *Computers & Security*, vol. 70, pp. 51–71, 2017.

[25] Y. Huang and A. K. Ghosh, "Introducing diversity and uncertainty to create moving attack surfaces for web services," in *Moving Target Defense*, pp. 131–151, Springer, Berlin, Germany, 2011.

[26] P. Kampanakis, H. Perros, and T. Beyene, "Sdn-based solutions for moving target defense network protection," in *Proceedings of the 15th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–6, IEEE, Sydney, NSW, Australia, June 2014.

[27] V. Zangeneh and M. Shajari, "A cost-sensitive move selection strategy for moving target defense," *Computers and Security*, vol. 75, pp. 72–91, 2018.

[28] L. Martin, "Cyber kill chain (CKC)," 2017, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[29] W. Guo, Q. Zhang, and L. Rong, "A stochastic epidemic model with nonmonotone incidence rate: sufficient and necessary conditions for near-optionality," *Information Sciences*, vol. 467, pp. 670–684, 2018.

[30] S. Sengupta, A. Chowdhary, A. Sabur et al., "A survey of moving target defenses for network security," *IEEE Communications Surveys & Tutorials*, 2019, https://arxiv.org/abs/1905.00964.

[31] A. Chowdhary, S. Sengupta, A. Alshamrani, D. Huang, and A. Sabur, "Adaptive MTD security using Markov game modeling," in *Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 577–581, New York, NY, USA, IEEE, 2018.