

Game theoretic analysis for the mechanism of moving target defense*

Gui-lin CAI[†], Bao-sheng WANG^{†‡}, Qian-qian XING

(College of Computer, National University of Defense Technology, Changsha 410073, China)

[†]E-mail: caiguilin08@nudt.edu.cn; wangbaosheng@126.com

Received Dec. 9, 2016; Revision accepted July 12, 2017; Cross-checked Dec. 20, 2017

Abstract: Moving target defense (MTD) is a novel way to alter the asymmetric situation of attacks and defenses, and a lot of MTD studies have been carried out recently. However, relevant analysis for the defense mechanism of the MTD technology is still absent. In this paper, we analyze the defense mechanism of MTD technology in two dimensions. First, we present a new defense model named MP2R to describe the proactivity and effect of MTD technology intuitively. Second, we use the incomplete information dynamic game theory to verify the proactivity and effect of MTD technology. Specifically, we model the interaction between a defender who equips a server with different types of MTD techniques and a visitor who can be a user or an attacker, and analyze the equilibria and their conditions for these models. Then, we take an existing incomplete information dynamic game model for traditional defense and its equilibrium result as baseline for comparison, to validate the proactivity and effect of MTD technology. We also identify the factors that will influence the proactivity and effectiveness of the MTD approaches. This work gives theoretical support for understanding the defense process and defense mechanism of MTD technology and provides suggestions to improve the effectiveness of MTD approaches.

Key words: Network security; Moving target defense (MTD); Defense mechanism; Defense model; Game theory
<https://doi.org/10.1631/FITEE.1601797>

CLC number: TP393

1 Introduction


Moving target defense (MTD) (NITRD, 2010) has been proposed as a novel way to reverse the asymmetric situation between attacks and defenses for years, and numerous papers on the topic have been published. These works cover several facets of MTD, and we have summarized them and drawn some conclusions in a previous work (Cai *et al.*, 2016a). At the same time, research on attack against MTD techniques has been carried out (Winterrose *et al.*, 2014; Winterrose and Carter, 2014). Those studies are in the ascendant, and it indicates that the interaction between attacks and defenses will evolve

to a new stage. However, so far, there is still a research gap on the defense model and defense mechanism analyses for the MTD technology, which we attempt to fill in this study.

In this paper, we first present a new defense model, the MP2R model, to describe the general defense process of MTD technology. Through comparing the MP2R model with the traditional PPDRR model, one can intuitively find the differences between MTD and traditional defense, and the proactivity and effect of the MTD approaches. Then, we analyze the defense mechanism of the three main types of MTD approaches, from an abstract perspective, by using incomplete information dynamic game theory. This gives a theoretical support for the proactivity and effect of the proposed MTD technology.

[‡] Corresponding author

* Project supported by the National Basic Research Program (973) of China (No. 2012CB315906)

 ORCID: Gui-lin CAI, <http://orcid.org/0000-0002-9322-2539>

© Zhejiang University and Springer-Verlag GmbH Germany 2017

2 Defense model for MTD technology

The general defense process of traditional defense approaches conforms to the policy, protection, detection, response, and recovery (PPDRR) model (Fig. 1) (Liu *et al.*, 2011). Policy is the core of a defense system. Under the guidance of policy, protection, detection, response, and recovery constitute a complete and dynamic security cycle to defend attacks in a reactive way. In other words, defense is triggered by the detection of anomalous events.

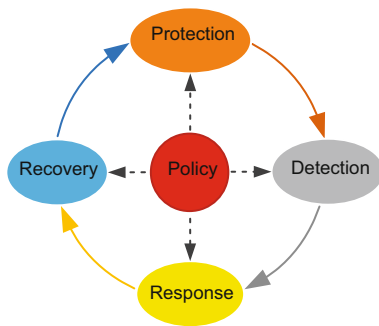


Fig. 1 The policy, protection, detection, response, and recovery (PPDRR) model for traditional defense

In the MTD field, defense is achieved by shifting the attack surface of the target system. In other words, the defender makes the attack surface of the target system ‘move’ to defend against attacks. The movement can be achieved in many ways (NITRD, 2009) and these ways can be categorized into different types. First, the movement (i.e., the attack surface shifting) can be state-dependent or state-independent. The state is usually related to the target system itself and the environment in which the target system resides. The change of the state usually indicates that there is detection or observation of anomalous events, such as the behaviors of the attacker, accidental faults, and changes in system performance. Second, the movement can be time-triggered, or event-triggered, or both. In the time-triggered mechanism, the movement is triggered by the event of timer-expiring, and the decision about whether the movement occurs at particular point-in-time can be stat-dependent or state-independent. In the event-triggered mechanism, the movement is always state-dependent.

Currently, numerous MTD approaches have been proposed, and most of them are designed to move by time-triggered mechanism and the deci-

sion about whether the movement occurs at particular point-in-time is state-independent. In other words, these MTD approaches can provide proactive defense independent of the state of the environment in which it resides. To be more effective and practical, an MTD system should also be equipped with reactive ability, which is state-dependent and responds to an anomalous event observed or perceived (Carvalho *et al.*, 2012). Some existing MTD approaches are designed to have proactive and reactive abilities simultaneously, such as ChameleonSoft (Azab *et al.*, 2011) and moving attack surface (MAS) (Huang and Ghosh, 2011). Therefore, the operation mode of MTD approaches is no longer consistent with that of the traditional PPDRR model. Accordingly, a new defense model is produced, which incorporates the MTD principle and can be called MP2R (MTD-policy-protection-(detection) response (recovery)) (Fig. 2). The MP2R model includes the processes of both proactive defense and reactive defense. In the model, the ratio of proactive defense is x , while the ratio of reactive defense is $(1 - x)$, where $x \in (0.5, 1)$ is used to express that MTD is mainly a proactive technique. The value of x is determined by the defender/administrator as a security-cost trade-off.

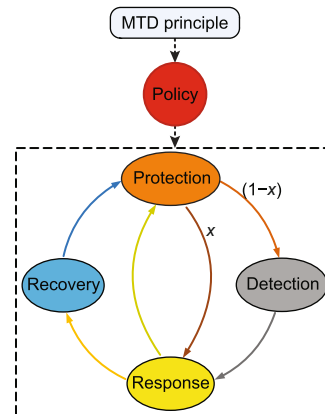


Fig. 2 The MP2R model for moving target defense (x is the ratio of proactive defense)

In the MP2R model, under the guidance of policy that adopts the MTD principle, there are four complete and dynamic security cycles to provide proactive and reactive defense (Fig. 3).

In the proactive mode, the defense process is state-independent and the attack surface is shifted periodically or erratically. Thus, it does not need

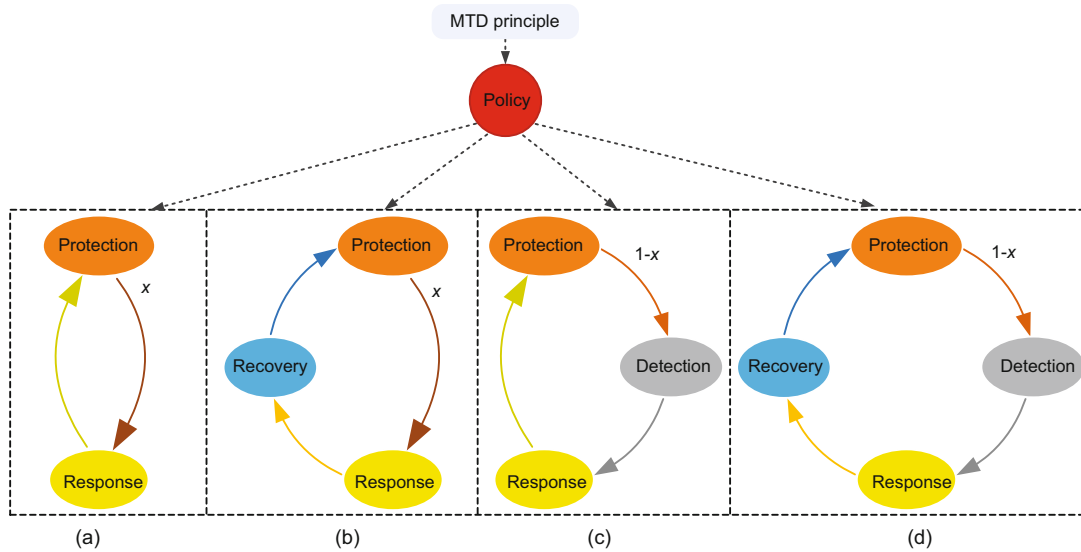


Fig. 3 The four complete and dynamic security cycles in MP2R: (a) policy-protection-response cycle; (b) policy-protection-response-recovery cycle; (c) policy-protection-detection-response cycle; (d) policy-protection-detection-response-recovery cycle

the detection and recovery links and corresponds to the first cycle, the ‘policy-protection-response’ cycle (Fig. 3a). Although this defense cycle can be effective, it cannot ensure that attacks will not be successful. If the target is compromised by the attacker and cannot provide normal functionality, the recovery link should be embodied in the defense process, and thus produces the second cycle, the ‘policy-protection-response-recovery’ cycle (Fig. 3b).

In the reactive mode, the defense process is triggered by anomalous events, or, it is state-dependent. Therefore, the detection link should be embodied. When the defense process enters the response link, if the target can still provide its functionality, the MTD approach just needs to shift the attack surface immediately to protect the target. This corresponds to the third cycle, the ‘policy-protection-detection-response’ cycle (Fig. 3c). Otherwise, if the target is compromised by the attacker and cannot provide normal functionality, the recovery should be performed to make the target restore to its pristine state or a more secure state than its past state, thus generating the fourth cycle, the ‘policy-protection-detection-response-recovery’ cycle (Fig. 3d), which can be regarded as the PPDRR model.

In conclusion, one can see that the MP2R model is more effective than the PPDRR model. For every attack, if it can be defended by the defense process corresponding to the PPDRR model, it must be de-

fended by the defense process corresponding to the MP2R model. This is because the PPDRR model is included in the MP2R model. Moreover, the MP2R model contains the proactive defense process that is state-independent and is not contained by the PPDRR model. The proactive ability of MTD approaches can make the information collected by adversaries have short validity period, and thus makes the target more secure. As a result, the MP2R model is the strengthening and extension of the PPDRR model, in which the occurrence of the defense process corresponding to the PPDRR model is decreased. In deploying traditional defense approaches, the probability of the occurrence of the defense process corresponding to the PPDRR model is 1. When deploying MTD approaches, the probability of the occurrence of the defense process corresponding to the PPDRR model is $(1 - x)$, where $x \in (0.5, 1)$.

3 Approach and scenario for game theoretic analysis

Game theory has been commonly used to investigate the interaction between the attacker and defender in the field of network security (Lye and Wing, 2005; Carroll and Grosu, 2011; Manshaei *et al.*, 2013). There are studies on MTD strategy design using game theory (Colbaugh and Glass, 2012; Manadhata, 2013; Zhu and Başar, 2013; Carter *et al.*,

2014; Prakash and Wellman, 2015; Vadlamudi *et al.*, 2016), but application of game theory on any other aspect is still absent.

Jia *et al.* (2006) proved that the interaction between attacker and defender is a non-cooperative dynamic game with incomplete information. Therefore, we use incomplete information dynamic game theory to investigate the defense mechanism of MTD from an abstract point of view. Specifically, we use incomplete information dynamic game models to model the interaction between the defender and the attacker while deploying MTD technology, and obtain the equilibria and their conditions. At the same time we take the incomplete information dynamic game model for the traditional defense and its equilibrium proposed by Shi *et al.* (2009) as a baseline for comparison. Thereafter, we compare the equilibria and their conditions when deploying MTD technology to the equilibrium and its condition when deploying the traditional defense approaches, and after further discussion, validate the proactivity and effectiveness of MTD technology. Also, we identify the factors that would influence the effect of MTD.

We now describe the game theory scenario considered in this study and the baseline game for comparison.

3.1 Study scenario

The scenario we have examined is as follows. There are two players: one is a defender who can equip a server with different MTD approaches to improve the server's security while enabling it to provide a specific service such as web service, and the other is a visitor who can be a normal user or an attacker that attempts to launch attacks.

Existing MTD approaches can be categorized into three main categories, namely, software transformations (ST) (Jajodia *et al.*, 2011), dynamic platform techniques (DPT) (Okhravi *et al.*, 2014), and network address shuffling (NAS) (Carroll *et al.*, 2014). Each of these attempts to use its own methodology for designing various approaches to defend against the attacker. Their running patterns should follow the 'hidden' pattern or the 'variation' pattern (Cai *et al.*, 2016b). The major difference between the two patterns is that the MTD approaches with 'hidden' pattern would make the attacker lose the target and thus break off the connection with the target, while the MTD approaches with 'variation' pattern

can disrupt attack but cannot prevent the attacker from re-connecting with the target. The approaches in the categories of ST and DPT conform to the 'variation' pattern, and the approaches in the category of NAS conform to the 'hidden' pattern. In the study scenario in this study, we consider that the MTD approaches deployed by the defender can be of three types: the 'hidden' MTD, the 'variation' MTD, and 'mixed' MTD (i.e., the combination of the 'hidden' and 'variation' MTDs). The relationship between them is shown in Fig. 4.

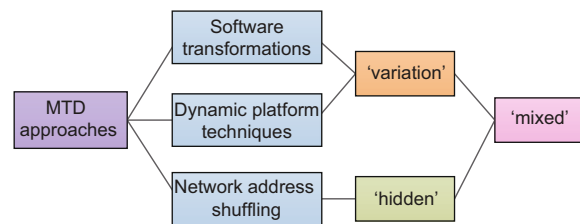


Fig. 4 The relationship between the categories and the running patterns of major MTD approaches

The MTD approaches with different running patterns can dynamically change a certain server property (i.e., shifting the attack surface) in different ways, and their running patterns would exhibit in the process of serving. Therefore, the external service mode would be different when different types of MTD techniques are deployed. Here, according to the types of MTD deployed, we consider that the server can provide three kinds of service, hid-service, var-service, and the combination of the two. Moreover, the defense is included in each type of service. Furthermore, because different types of MTD techniques would influence the attacker in different ways, the utilities for the interaction between the defender and the attacker would be different when deploying different types of MTD, and we will discuss them in detail in Section 4.

3.2 Baseline game

We take the game under the situation of traditional defense proposed by Shi *et al.* (2009) as the baseline game for comparison.

The scenario taken in the baseline game is that a server provides the web service and is deployed with a traditional defense approach, and an attacker attempts to launch a DoS attack. Through modeling the interaction between the defender and the attacker, Shi *et al.* (2009) arrived at an equilibrium

result that the server should provide service while both the attacker and the user should request service under the condition $p < 2/(2+k)$, where p represents the attack probability (the probability that the visitor is an attacker from the view of the server) and k ($k > 1$) the attack damage factor. Both p and k are determined and controlled by the attacker, and the server finds it difficult to accurately predict their values. Therefore, the conclusion is that the traditional defense is passive.

4 Game specification

Corresponding to the three situations where the defender deploys ‘hidden’, ‘variation’, or ‘mixed’ MTD, in this section, we specify three game models between the defender and the visitor.

We will describe the general definition of the three models (including the set of players, the type space for each player, and the action set for each player) in Section 4.1, and define the utility-matrix for the three situations in Section 4.2.

4.1 Types and actions

1. The set of players

The set of players can be defined as $\Gamma = \{1, 2\}$, in which ‘1’ represents the defender and ‘2’ represents a visitor. The Harsanyi transformation is usually performed to analyze a game of incomplete information, which introduces a hypothetical player called ‘Nature’ (usually denoted as N) (Carroll and Grosu, 2011). The game usually begins with a selection that player N selects the type of either player 1 or 2.

2. The type space for each player

The type space of player 1 can be of two cases. One is for the situation where he/she provides one kind of service (hid-service or var-service) and it can be defined as $T_1 = \{t_{11}\} = \{\text{service}\}$. The other is for the situation where he/she provides two kinds of services (hid-service and var-service) and it can be defined as $T_1 = \{t_{11}, t_{12}\} = \{\text{hid-service}, \text{var-service}\}$. The type space of player 2 is always $T_2 = \{t_{21}, t_{22}\} = \{\text{attacker}, \text{user}\}$.

3. The action set for each player

The action set of player 1 is $A_1 = \{a_{11}, a_{10}\}$, where a_{11} means that the defender enables the server to provide normal service to the visitor and a_{10} means that the defender disables the server from providing service. The action set of player 2 is

$A_2 = \{a_{21}, a_{20}\}$, where a_{21} means that the visitor acquires service from the server (for the attacker, attacking is happening while he/she is acquiring service), and a_{20} means that the visitor does not acquire the service.

In the scenario under study, we assume that player N moves first by choosing the type of visitor; i.e., the game begins when the visitor attempts to request and acquire the service, and then the defender chooses his/her strategy. The defender does not know the actual type of visitor, but he/she has a prior probability distribution over all visitor types. Here we assume that the prior probability distribution is $p_1 = \{p(t_{11}, t_{21}) = p, p(t_{11}, t_{22}) = 1 - p\}$, $p \in [0, 1]$.

4.2 Utility-matrix

In this study, an important premise of the game between the defender and the visitor is that the defender can equip a server with different types of MTD techniques. Compared with the traditional defense approach, MTD technology can increase the attacker’s work effort for launching a successful attack by shifting the server’s attack surface periodically or erratically. Therefore, in addition to the initial deployment cost, there is always another cost, defense cost. For the defender, the decision on choosing a_{10} or a_{11} is made based on the information he/she observes, in which the running state of the deployed MTD is included. Therefore, for each equilibrium, no matter which action the defender chooses, he/she has paid the same defense cost to ensure the normal operation of the deployed MTD. Here we assume that the average defense cost is s ($s > 0$).

To describe the effect of MTD against attacks, we introduce a blocking factor β ($\beta > 1$). The value of β will be determined based on the criteria defined by the defender and can be customized for each MTD approach. The value of β is the effect manifestation of the deployed defense method which pays a certain defense cost. Intuitively, the greater the value of β , the better the defense effect.

For a given MTD method, the faster the server’s attack surface shifts, the more defense costs the defender should pay, and meanwhile, the more efforts the attacker has to make and pay for attacking, the larger the value of β will be. Thus, there is a positive correlation between the defense cost s and the blocking factor β . Moreover, they are influenced by the

shifting frequency of MTD: the higher the frequency, the larger the values of s and β .

In this section, we will discuss the utility-matrix for the interaction between the defender and the visitor. Because the deployment of MTD approaches would just influence the interaction between the defender and the attacker, we discuss the utility-matrix for the interaction between the defender and the user and the interaction between the defender and the attacker in Sections 4.2.1 and 4.2.2, respectively. Moreover, we show the utility-matrix for the interaction between the defender and the visitor while deploying different types of MTD in Section 4.2.2.

4.2.1 Utility-matrix for the defender and the user

For the interaction between the defender and the user, no matter which type of service is provided, it must ensure that a normal user can visit the service normally. Thus, the utilities of the defender and the user can be considered to be the same while deploying different types of MTD approaches. As mentioned above, no matter which action (a_{10} or a_{11}) the defender chooses, he/she should pay the same defense cost. Therefore, the utility-matrix for the defender and the user can be described as follows:

If the user requests and acquires the service, we assume that the user obtains the payoff a while the defender obtains the payoff $a-s$ ($a > s$).

If the user requests but does not acquire the service, the user obtains the payoff $-a$ while the defender obtains the payoff $-a-s$.

Otherwise, the user would obtain the payoff of 0 while the defender would obtain the payoff $-s$.

Table 1 shows the utility-matrix for the interaction between the defender and a user.

Table 1 The utility-matrix for defender and user under the ‘hidden’ MTD

		User	
		a_{21}	a_{20}
Defender	a_{11}	$(a-s, a)$	$(-s, 0)$
	a_{10}	$(-a-s, -a)$	$(-s, 0)$

4.2.2 Utility-matrix for the defender and the attacker

For the interaction between the defender and the attacker, when the attacker tries to acquire the

service to obtain essential information for attack, he/she must pay a cost b ($b > 0$), regardless of success. Obviously, $a > b$. Furthermore, the introduction of MTD would change their behaviors, and different types of MTD would make different influence. This can be further discussed as follows:

1. Utilities for the situation with ‘hidden’ MTD

We know that for each MTD approach, there is a large configuration space for attack surface shifting (Hobson *et al.*, 2014; Zhuang *et al.*, 2014). In the situation of ‘hidden’ MTD approaches, the configuration space is considered to consist of multiple candidate network addresses. Here we assume the number of addresses is N_1 , and the value of the blocking factor is set to β_1 .

Next, we describe the change of the interaction behaviors between the attacker and the defender induced by the introduction of ‘hidden’ MTD. Specifically, if the attacker obtains the server’s current address and the server changes its configuration (i.e., the address), the attacker will lose the target and thus the attack cannot be continued. As a result, the utility-matrix for the interaction between the defender and the attacker will be influenced.

To specify the influence, we extend the service type from 1 to N_1 ; i.e., the type space of player 1 is extended from $T_1 = \{t_{11}\} = \{\text{service}\}$ to $T'_1 = \{t_{11}, t_{12}, \dots, t_{1N_1}\} = \{\text{service 1, service 2, } \dots, \text{service } N_1\}$, where service i ($1 \leq i \leq N_1$) means that the server is providing the service with address i . Also, we extend the action set of the attacker to $A'_2(t_{21}) = \{a_{21}, a_{22}, \dots, a_{2N_1}, a_{20}\}$, where a_{2i} means that the attacker attempts to attack service i , and a_{20} still means that the attacker does not attack. The action set of player 1 remains $A_1 = \{a_{11}, a_{10}\}$, i.e., $A_1(t_{11}) = A_1(t_{12}) = \dots = A_1(t_{1N_1}) = \{a_{11}, a_{10}\}$.

In this situation, if the attacker takes action a_{2i} when the server provides service i , the attacker would obtain payoff ka/β_1 while paying cost b , and thus his/her actual payoff is $ka/\beta_1 - b$, where k ($k > 1$) is the attack damage factor defined by Shi *et al.* (2009). At the same time, the defender obtains payoff $-ka/\beta_1$ while paying defense cost s , so his/her actual payoff is $-ka/\beta_1 - s$.

If the attacker take action a_{2i} when the server provides service j ($j \neq i$), the attacker will obtain actual payoff $-b$ since he/she cannot find the server, while the defender obtains the actual payoff $-s$.

Otherwise, the attacker obtains the actual payoff 0 while the defender obtains the actual payoff $-s$.

The utility-matrix for the interaction between the defender and the attacker in this situation is shown in Table 2.

To better and more easily analyze and compare with the baseline game, we normalize the type space of the defender from T'_1 to $T_1 = \{t_{11}\} = \{\text{service}\}$ again, in which service represents the set of $\{\text{service 1, service 2, \dots, service } N_1\}$ before normalization. Accordingly, we normalize the action set of the attacker. Specifically, we treat it as $A_2(t_{21}) = \{a_{21}, a_{20}\}$, in which a_{21} represents the set of $\{a_{21}, a_{22}, \dots, a_{2N_1}\}$ before normalization and means that the attacker attempts to attack, and a_{20} means that the attacker does not attack.

Accordingly, we need to normalize the utility-matrix presented in Table 2 as well. By considering the utility-matrix between the defender and the user presented in Table 1, the utilities of the defender and the visitor after normalization are shown in Table 3.

2. Utilities for the situation with ‘variation’ MTD

In this situation, we assume that the size of the configuration space is N_2 ; i.e., the configuration space consists of N_2 candidate software variations or platforms with diverse properties. Also, we assume that the value of the blocking factor is set to β_2 .

Similar to the situation with ‘hidden’ MTD, we can extend the type space of the defender from 1 to N_2 , in which service i means that the server is providing the service with configuration i ($1 \leq i \leq N_2$). Configuration i can be the software variation i , or the platform with property type i , or the i th combination of the two. Also, we can accordingly extend the action set of the attacker to $A'_2(t_{21}) = \{a_{21}, a_{22}, \dots, a_{2N_2}, a_{20}\}$. The meaning of a_{2i} ($1 \leq i \leq N_2$) is the same as that for the situation with ‘hidden’ MTD.

Also, the introduction of ‘variation’ MTD does not influence the normal user but changes the interaction behaviors between the attacker and the defender. However, the utility-matrix for the interaction between the defender and the attacker should be different from that in the situation of ‘hidden’ MTD. In this situation, no matter which configuration is configured with the server, the attacker will connect to the server and collect information. In other words, if the attacker takes action a_{2i} ($1 \leq i \leq N_2$), he/she

can always obtain the actual payoff $ka/\beta_2 - b$.

For the defender, if the server provides service i when the attacker takes action a_{2i} , he/she can obtain the actual payoff $-ka/\beta_2 - s$. If the server provides service j ($j \neq i$), then he/she can obtain the actual payoff $-s$. Otherwise, if the server does not provide service, his/her actual payoff is $-s$.

Therefore, the utility-matrix for the interaction between the defender and the attacker can be described as Table 4.

Similar to the situation with ‘hidden’ MTD, we can normalize the type space of the defender, the action set of the attacker, and the utility-matrix as in Table 4. By taking the utility-matrix between the defender and the user in Table 1 into account, we can obtain the utilities of the defender and the visitor after normalization (Table 5).

3. Utilities for the situation with ‘mixed’ MTD

In this situation, the server can provide both the hid-service and var-service. Since each type of MTD has its own configuration space, here we assume that the number of configurations for the ‘hidden’ pattern MTD is N_1 and the value of the blocking factor for the ‘hidden’ MTD is β_1 . The number of configurations for the ‘variation’ pattern MTD is N_2 , and the value of the blocking factor for the ‘variation’ MTD is β_2 .

Based on the analyses above, we can describe the utilities of the defender and the visitor in this situation in Table 6.

5 Equilibria and analyses

In this section, we analyze the equilibria and their conditions for the three models in Section 4, corresponding to the cases of deploying ‘hidden’ MTD, ‘variation’ MTD, and ‘mixed’ MTD, respectively. We also take the baseline game for comparison to further discuss the defense mechanism of MTD.

Based on the definition of the game models in Section 4, we know that in the situation with ‘hidden’ or ‘variation’ MTD, the strategy space of player 1 is $S_1 = \{a_{11}, a_{10}\}$; i.e., player 1 has two pure service strategies. With ‘mixed’ MTD, the strategy space of player 1 is $S_1 = \{(a_{11}, a_{11}), (a_{11}, a_{10}), (a_{10}, a_{11}), (a_{10}, a_{10})\}$; i.e., player 1 has four pure service strategies, in which (a_{1i}, a_{1j}) is the combination of the strategies for the two service types, hid-service and var-service ($i, j \in \{0, 1\}$).

Table 2 The utility-matrix for defender and attacker under the ‘hidden’ MTD

		Attacker						
		a_{21}	a_{22}	a_{23}	\dots	a_{2N_1}	a_{20}	
Defender	Service 1	a_{11}	$(-ka/\beta_1 - s, ka/\beta_1 - b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$
		a_{10}	$(-s, -b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$
	Service 2	a_{11}	$(-s, -b)$	$(-ka/\beta_1 - s, ka/\beta_1 - b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$
		a_{10}	$(-s, -b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$
	\dots	\dots	\dots	\dots	\dots	\dots	\dots	\dots
	Service N_1	a_{11}	$(-s, -b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-ka/\beta_1 - s, ka/\beta_1 - b)$	$(-s, 0)$
a_{10}		$(-s, -b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$	

Table 3 The utility-matrix for defender and visitor under the ‘hidden’ MTD

		Visitor			
		Attacker		User	
		a_{21}	a_{20}	a_{21}	a_{20}
Defender	a_{11}	$(-ka/(\beta_1 N_1) - s, ka/(\beta_1 N_1) - b)$	$(-s, 0)$	$(a - s, a)$	$(-s, 0)$
	a_{10}	$(-s, -b)$	$(-s, 0)$	$(-a - s, -a)$	$(-s, 0)$

Table 4 The utility-matrix for defender and attacker under the ‘variation’ MTD

		Attacker						
		a_{21}	a_{22}	a_{23}	\dots	a_{2N_2}	a_{20}	
Defender	Service 1	a_{11}	$(-ka/\beta_2 - s, ka/\beta_2 - b)$	$(-s, ka/\beta_2 - b)$	$(-s, ka/\beta_2 - b)$	\dots	$(-s, ka/\beta_2 - b)$	$(-s, 0)$
		a_{10}	$(-s, -b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$
	Service 2	a_{11}	$(-s, ka/\beta_2 - b)$	$(-ka/\beta_2 - s, ka/\beta_2 - b)$	$(-s, ka/\beta_2 - b)$	\dots	$(-s, ka/\beta_2 - b)$	$(-s, 0)$
		a_{10}	$(-s, -b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$
	\dots	\dots	\dots	\dots	\dots	\dots	\dots	\dots
	Service N_2	a_{11}	$(-s, ka/\beta_2 - b)$	$(-s, ka/\beta_2 - b)$	$(-s, ka/\beta_2 - b)$	\dots	$(-ka/\beta_2 - s, ka/\beta_2 - b)$	$(-s, 0)$
a_{10}		$(-s, -b)$	$(-s, -b)$	$(-s, -b)$	\dots	$(-s, -b)$	$(-s, 0)$	

Table 5 The utility-matrix for defender and visitor under the ‘variation’ MTD

		Visitor			
		Attacker		User	
		a_{21}	a_{20}	a_{21}	a_{20}
Defender	a_{11}	$(-ka/(\beta_2 N_2) - s, ka/\beta_2 - b)$	$(-s, 0)$	$(a - s, a)$	$(-s, 0)$
	a_{10}	$(-s, -b)$	$(-s, 0)$	$(-a - s, -a)$	$(-s, 0)$

Table 6 The utility-matrix for defender and visitor under the ‘mixed’ MTD

		Visitor				
		Attacker		User		
		a_{21}	a_{20}	a_{21}	a_{20}	
Defender	hid-service	a_{11}	$(-ka/(\beta_1 N_1) - s, ka/(\beta_1 N_1) - b)$	$(-s, 0)$	$(a - s, a)$	$(-s, 0)$
		a_{10}	$(-s, -b)$	$(-s, 0)$	$(-a - s, -a)$	$(-s, 0)$
	var-service	a_{11}	$(-ka/(\beta_2 N_2) - s, ka/\beta_2 - b)$	$(-s, 0)$	$(a - s, a)$	$(-s, 0)$
		a_{10}	$(-s, -b)$	$(-s, 0)$	$(-a - s, -a)$	$(-s, 0)$

Also, there are four pure visiting strategies; i.e., the strategy space of player 2 is $S_2 = \{(a_{21}, a_{21}), (a_{21}, a_{20}), (a_{20}, a_{21}), (a_{20}, a_{20})\}$, in which (a_{2i}, a_{2j}) is the strategy combination for the attacker and the user ($i, j \in \{0, 1\}$). For the visitor, the visiting strategy (a_{20}, a_{20}) means that the attacker does not attack and at the same time the user does not request service, and this does not have any practical significance. Hence, we will not take this situation into account in this study.

5.1 Discussion for ‘hidden’ MTD

5.1.1 Equilibria for the game model with ‘hidden’ MTD

According to the description in Sections 4.1 and 4.2, the extensive form of the game with ‘hidden’ MTD can be shown in Fig. 5, in which the utilities are taken from Table 3.

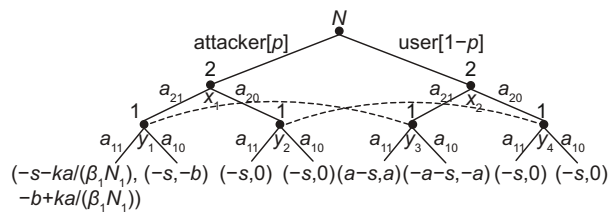


Fig. 5 The extensive form presentation for the game with ‘hidden’ MTD

From Fig. 5, we can know that player 2 has two information sets, $H_2 = \{h_2^1, h_2^2\}$. They are both singleton information sets because the visitor knows his/her own type. $h_2^1 = \{x_1\}$ means that player N chooses the type of attacker, and $h_2^2 = \{x_2\}$ means that player N chooses the type of user. Player 1 also has two information sets, $H_1 = \{h_1^1, h_1^2\}$, which are composed of two decision nodes. $h_1^1 = \{y_1, y_3\}$ means that the defender observes the visitor’s action a_{21} , and $h_1^2 = \{y_2, y_4\}$ means that the defender observes the visitor’s action a_{20} .

In this study, we consider only the visiting strategies (a_{21}, a_{21}) , (a_{21}, a_{20}) , and (a_{20}, a_{21}) , because strategy (a_{20}, a_{20}) has no practical significance. For the defender, all the three strategies will make him/her observe action a_{21} . Therefore, we consider only the left information set h_1^1 here.

To analyze the equilibria for this situation, we first discuss whether there exist pure strategy equilibria or not from the defender’s perspective. Here

we take the visiting strategy (a_{21}, a_{21}) as an example.

As mentioned above, the defender has a prior probability distribution $p_1 = \{p, 1 - p\}$ over all visitor types. On the basis of the information set h_1^1 and according to the Bayes formula, after observing the visitor’s action a_{21} , the defender can obtain the posterior probability distribution as follows:

$$\tilde{p}_1(t_{21}|a_{21}) = \frac{p(t_{11}, t_{21})}{p(t_{11}, t_{21}) + p(t_{11}, t_{22})} = p,$$

$$\tilde{p}_1(t_{22}|a_{21}) = \frac{p(t_{11}, t_{22})}{p(t_{11}, t_{21}) + p(t_{11}, t_{22})} = 1 - p.$$

According to Table 3, we can find that the defender’s expected payoff obtained by playing strategy a_{11} is

$$u_1(a_{11}) = \tilde{p}_1(t_{21}|a_{21}) \cdot u_1(a_{11}, a_{21}, t_{21}) + \tilde{p}_1(t_{22}|a_{21}) \cdot u_1(a_{11}, a_{21}, t_{22}) = p \cdot (-s - ka/(\beta_1 N_1)) + (1 - p) \cdot (a - s),$$

and the expected payoff by playing strategy a_{10} is

$$u_1(a_{10}) = \tilde{p}_1(t_{21}|a_{21}) \cdot u_1(a_{10}, a_{21}, t_{21}) + \tilde{p}_1(t_{22}|a_{21}) \cdot u_1(a_{10}, a_{21}, t_{22}) = p \cdot (-s) + (1 - p) \cdot (-a - s).$$

The defender will choose strategy a_{11} if $u_1(a_{11})$ is larger than $u_1(a_{10})$, i.e.,

$$p \cdot (-s - ka/(\beta_1 N_1)) + (1 - p) \cdot (a - s) > p \cdot (-s) + (1 - p) \cdot (-a - s),$$

which gives

$$p < \frac{2}{2 + k/(\beta_1 N_1)}.$$

From the analyses, we can obtain the conclusion that, for the defender, strategy a_{11} is better than a_{10} under the condition $p < 2/(2 + k/(\beta_1 N_1))$. Otherwise, strategy a_{10} is better than a_{11} .

Then, we analyze whether visiting strategy (a_{21}, a_{21}) is better than the other three visiting strategies from the point of view of the visitor.

1. When $p < 2/(2 + k/(\beta_1 N_1))$, the defender would choose strategy a_{11} . Under this condition, the visitor’s expected payoffs for playing the four visiting strategies can be presented as follows:

$$u_2((a_{21}, a_{21})) = p \cdot (ka/(\beta_1 N_1) - b) + (1 - p) \cdot a,$$

$$u_2((a_{21}, a_{20})) = p \cdot (ka/(\beta_1 N_1) - b) + (1 - p) \cdot 0,$$

$$u_2((a_{20}, a_{21})) = p \cdot 0 + (1 - p) \cdot a,$$

$$u_2((a_{20}, a_{20})) = p \cdot 0 + (1 - p) \cdot 0.$$

Since $a > 0$, when $ka/(\beta_1 N_1) - b > 0$ ($\beta_1 N_1 < ka/b$), $u_2((a_{21}, a_{21}))$ is larger than the others; i.e., strategy (a_{21}, a_{21}) is the best visiting strategy against the defender's strategy a_{11} .

Therefore, the defender and visitor strategy combination $(a_{11}, (a_{21}, a_{21}))$ will reach an equilibrium under the conditions $p < 2/(2 + k/(\beta_1 N_1))$ and $\beta_1 N_1 < ka/b$.

2. When $p > 2/(2 + k/(\beta_1 N_1))$, the defender would choose strategy a_{10} . Under this condition, the visitor's expected payoffs for playing the four visiting strategies are:

$$\begin{aligned} u_2((a_{21}, a_{21})) &= p \cdot (-b) + (1 - p) \cdot (-a), \\ u_2((a_{21}, a_{20})) &= p \cdot (-b) + (1 - p) \cdot 0, \\ u_2((a_{20}, a_{21})) &= p \cdot 0 + (1 - p) \cdot (-a), \\ u_2((a_{20}, a_{20})) &= p \cdot 0 + (1 - p) \cdot 0. \end{aligned}$$

Since $a > b > 0$ and $0 \leq p \leq 1$, $u_2((a_{20}, a_{20}))$ is the largest value; i.e., strategy (a_{20}, a_{20}) is the best visiting strategy against the defender's strategy a_{10} .

Therefore, the defender and visitor strategy combination $(a_{10}, (a_{21}, a_{21}))$ cannot reach an equilibrium.

Next, we discuss whether there are equilibria or not for visiting strategies (a_{21}, a_{20}) and (a_{20}, a_{21}) , and obtain the following conclusions:

1. For visiting strategy (a_{21}, a_{20}) , no matter which value is assigned to factor p , the defender can always choose strategy a_{10} . Conversely, for the defender's strategy a_{10} , through analyses similar to those above, we can see that the visiting strategy (a_{20}, a_{20}) is the best. Therefore, the defender and visitor strategy combination $(a_{10}, (a_{21}, a_{20}))$ cannot reach an equilibrium.

2. For visiting strategy (a_{20}, a_{21}) , no matter which value is assigned to factor p , the defender can always choose strategy a_{11} . Conversely, for the defender's strategy a_{11} , the visiting strategy (a_{20}, a_{21}) is the best when $\beta_1 N_1 > ka/b$. Therefore, the defender and visitor strategy combination $(a_{11}, (a_{20}, a_{21}))$ will reach an equilibrium under the condition $\beta_1 N_1 > ka/b$.

We summarize the perfect Bayesian equilibria (PBE) for the situation with 'hidden' MTD and their conditions in Table 7. The equilibrium is denoted by E_i ($i = 1, 2$) and given as a tuple (s_{1m}, s_{2n}, p_a) , where s_{1m} ($s_{1m} \in S_1$) is the defender's strategy, s_{2n} ($s_{2n} \in S_2$) the visitor's strategy, and p_a the de-

fender's belief on that the visitor is an attacker. In addition, as mentioned in Section 4.2, the defender pays the same defense cost s no matter whether the server provides service. Therefore, s is lost in the calculation. Furthermore, its influence on the effect of 'hidden' MTD is manifested through the blocking factor β , and we will discuss it in Section 5.1.2.

Table 7 Equilibria for situation 'hidden' MTD and the corresponding conditions

Perfect Bayesian equilibrium	Condition
$E_1 ((a_{11}, (a_{21}, a_{21})), p)$	$p < \frac{2}{2 + k/(\beta_1 N_1)}$ and $\beta_1 N_1 < \frac{ka}{b}$
$E_2 ((a_{11}, (a_{20}, a_{21})), p)$	$\beta_1 N_1 > \frac{ka}{b}$

5.1.2 Effect of 'hidden' MTD

As mentioned in Section 3.2, the baseline game has an equilibrium result that the server should provide service while the attacker and the user should request service under the condition $p < 2/(2 + k)$ (p and k are determined and controlled by the attacker).

In our game with 'hidden' MTD, equilibrium $E_1 ((a_{11}, (a_{21}, a_{21})))$ is equivalent to the equilibrium result of the baseline game. However, from Table 7, we can see that the conditions for equilibrium E_1 are changed to $p < 2/(2 + k/(\beta_1 N_1))$ and $\beta_1 N_1 < ka/b$. The conditions are related not only to parameters p and k determined and controlled by the attacker, but also to parameters N_1 and β_1 determined and controlled by the defender. Specifically, when the defender increases the value of $\beta_1 N_1$ under the limited condition $\beta_1 N_1 < ka/b$, either he/she increases the frequency or the number of candidate addresses of the deployed MTD, the value of factor p will be increased. This phenomenon indicates two facts: (1) the attacker has to increase his/her attack probability to try to obtain his/her expected payoff; (2) the adjustment for 'hidden' MTD can make the defender defend against stronger attacks.

When the defender continues to increase the value of $\beta_1 N_1$ and make it satisfy the condition $\beta_1 N_1 > ka/b$, the equilibrium is changed to E_2 , which means that the defender should provide service and the user requests service normally while the attacker should take action a_{20} (i.e., no attacking) to obtain his/her expected payoff. This is the greatest expectation for the defender.

From either equilibrium E_1 or E_2 , we can see that the introduction of ‘hidden’ MTD can influence the actions of the attacker greatly (the attacker must increase his/her attack probability or give up the attack to obtain his/her expected payoff). This reflects the proactivity and effectiveness of ‘hidden’ MTD. Furthermore, the influence can be achieved in two ways: one is to increase the shifting frequency of the MTD approach, and the other is to increase the configuration space of the MTD approach.

5.2 Discussion for ‘variation’ MTD

5.2.1 Equilibria for the game model with ‘variation’ MTD

According to the descriptions in Sections 4.1 and 4.2, the extensive form of the game with ‘variation’ MTD can be shown as in Fig. 6, which is similar to that of the game with ‘hidden’ MTD, and the difference is that the utilities are from Table 5.

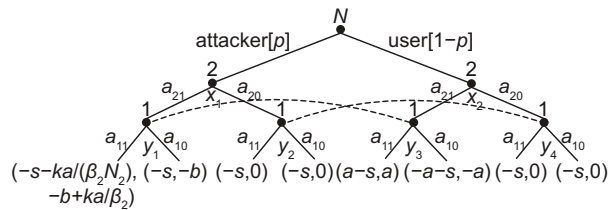


Fig. 6 The extensive form presentation for the game with ‘variation’ MTDs

Similar to the situation with ‘hidden’ MTD, player 1 has two information sets, and only the left information set h_1^1 is considered. Also, after observing the visitor’s action a_{21} , player 1 will obtain the posterior probability $\tilde{p}_1 = (p, 1-p)$ for the visitor’s types.

Then, through computation and analyses similar to those in Section 5.1.1, we can obtain the following conclusions:

1. For visiting strategy (a_{21}, a_{21}) , when $p < 2/(2 + k/(\beta_2 N_2))$, the defender will choose strategy a_{11} ; otherwise, the defender will choose strategy a_{10} . Therefore, conversely, there are two subcases to be analyzed. One is, when the defender chooses strategy a_{11} , through the analyses similar to those above, we can see that visiting strategy (a_{21}, a_{21}) is the best when $\beta_2 < ka/b$. Therefore, the defender and visitor strategy combination $(a_{11}, (a_{21}, a_{21}))$ is in equilibrium under the conditions $p < 2/(2 + k/(\beta_2 N_2))$ and

$\beta_2 < ka/b$. The other is, when the defender’s strategy is a_{10} , again through similar analyses, we can see that the visiting strategy (a_{20}, a_{20}) is the best. As a result, the strategy combination $(a_{10}, (a_{21}, a_{21}))$ cannot reach an equilibrium.

2. For visiting strategy (a_{21}, a_{20}) , no matter which value is assigned to factor p , the defender can always choose strategy a_{10} . Conversely, for defender’s strategy a_{10} , visiting strategy (a_{20}, a_{20}) is the best. Therefore, strategy combination $(a_{10}, (a_{21}, a_{20}))$ cannot reach an equilibrium.

3. For visiting strategy (a_{20}, a_{21}) , no matter which value is assigned to factor p , the defender can always choose strategy a_{11} . Conversely, for the defender’s strategy a_{11} , visiting strategy (a_{20}, a_{21}) is the best. Therefore, the strategy combination $(a_{11}, (a_{20}, a_{21}))$ will reach an equilibrium under the condition $\beta_2 > ka/b$.

We summarize the PBE for the situation with ‘variation’ MTD and their conditions in Table 8, in which the equilibria are represented in the same form as in Table 7. Moreover, as in Section 5.1, defense cost s is lost in the calculation and its effect on ‘variation’ MTD through blocking factor β will be discussed in Section 5.2.2. Furthermore, the same phenomenon will also be presented in Section 5.3.

Table 8 Equilibria for situation ‘variation’ MTD and the corresponding conditions

Perfect Bayesian equilibrium	Condition
$E_1 ((a_{11}, (a_{21}, a_{21})), p)$	$p < \frac{2}{2 + k/(\beta_2 N_2)}$ and $\beta_2 < \frac{ka}{b}$
$E_2 ((a_{11}, (a_{20}, a_{21})), p)$	$\beta_2 > \frac{ka}{b}$

5.2.2 Effect of ‘variation’ MTD

As mentioned in Section 3.2, the baseline game has an equilibrium result that the server should provide service while the attacker and the user should request service under the condition $p < 2/(2 + k)$ (p and k are determined and controlled by the attacker).

In our game with ‘variation’ MTD, equilibrium $E_1 (a_{11}, (a_{21}, a_{21}))$ is equivalent to the equilibrium result of the baseline game. However, from Table 8, one can see that the conditions for equilibrium E_1 are changed to $p < 2/(2 + k/(\beta_2 N_2))$ and $\beta_2 < ka/b$. These conditions are related not only to parameters p and k determined and controlled by the attacker,

but also to parameters N_2 and β_2 determined and controlled by the defender. Specifically, when the defender increases the value of $\beta_2 N_2$ under the limited condition $\beta_2 < ka/b$, either he/she increases the frequency or the number of configurations of the deployed MTD, the value of factor p will be increased. This phenomenon indicates two facts: (1) the attacker has to increase his/her attack probability to attempt to obtain his/her expected payoff; (2) the adjustment for ‘variation’ MTD can make the defender defend against stronger attacks.

When the defender continues to increase β_2 when satisfying $\beta_2 > ka/b$, the equilibrium is changed to E_2 , which means that the defender should provide service and the user requests service normally while the attacker should take action a_{20} (i.e., no attacking) to obtain his/her expected payoff. This is the greatest expectation for the defender.

From either equilibrium E_1 or E_2 , we can see that the introduction of ‘variation’ MTD can greatly influence the actions of the attacker (the attacker must increase his/her attack probability or give up the attack to obtain his/her expect payoff), which reflects the proactivity and effectiveness of ‘variation’ MTD. This influence can be achieved in two ways: one is to increase the shifting frequency of the MTD approach, and the other is to increase the configuration space of the MTD approach.

Furthermore, one condition for equilibrium E_1 is $\beta_2 < ka/b$, and the condition for equilibrium E_2 is $\beta_2 > ka/b$. These can be considered to be: when deploying ‘variation’ MTD, the defender should influence the attacker only through increasing the shuffling frequency. This is the main difference from the situation with ‘hidden’ MTD, and it is reasonable because compared with preparing N_2 candidate addresses for ‘hidden’ MTD, preparing N_2 software variations or N_2 platforms with diverse properties is more complex and challenging, and the cost is much higher. Therefore, the defender should choose mainly the way of changing the value of β_2 to influence the action of the attacker.

5.3 Discussion for ‘mixed’ MTD

5.3.1 Equilibria for the game model with ‘mixed’ MTD

In this subsection, we will analyze the equilibria for the game with ‘mixed’ MTD. In this situation,

for the defender, he/she can deploy the two types of MTD approaches simultaneously, but there is no necessity to run them at the same time for two reasons: (1) the objectives of the two types of MTD are the same; (2) it is not cost-effective to do so. Therefore, the defender can enable the server just to provide hid-service or var-service, or the two types of service alternately.

If the defender makes the server provide hid-service and var-service alternately, from the view of the attacker, the service strategy would be considered as (a_{11}, a_{11}) . If the defender enables only one of the two types of service, the service strategy should be considered as (a_{11}, a_{10}) or (a_{10}, a_{11}) . The service strategy (a_{10}, a_{10}) does not have any practical significance and thus we do not consider it in this study.

Furthermore, from the defender’s perspective, when he/she enables the ‘hidden’ MTD, the game is as shown in Fig. 5. When the defender enables the ‘variation’ MTD, the game from the defender’s perspective is as shown in Fig. 6. In addition, as mentioned above, no matter which case it is, the defender can obtain a posterior probability distribution $\tilde{p}_1 = (p, 1-p)$ after observing the attacker’s action a_{21} . From the attacker’s perspective, the game should be of the form shown in Fig. 7, where the utilities are from Table 6.

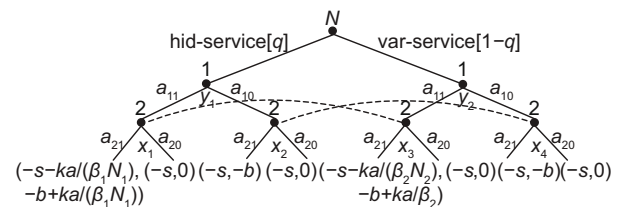


Fig. 7 The game from the attacker’s view when ‘mixed’ MTD is deployed

From Fig. 7, we can see that player 1 has two information sets, $H_1 = \{h_1^1, h_1^2\}$. They are both singleton information sets because the defender knows the server’s service type. $h_1^1 = \{y_1\}$ means that player N chooses hid-service, and $h_1^2 = \{y_2\}$ means that player N chooses var-service.

Player 2 also has two information sets, $H_2 = \{h_2^1, h_2^2\}$. These two information sets are composed of two decision nodes. $h_2^1 = \{x_1, x_3\}$ means that the attacker observes the defender’s action a_{11} , and $h_2^2 = \{x_2, x_4\}$ means that the attacker observes the defender’s action a_{10} . Furthermore, from the

view of the attacker, all the three service strategies considered in this study, i.e., (a_{11}, a_{11}) , (a_{11}, a_{10}) , and (a_{10}, a_{11}) , will make the attacker observe action a_{11} . Therefore, only the left information set needs to be considered here. In addition, the attacker should have a prior probability distribution over all service types, which can be denoted as $p_2 = \{p(t_{21}, t_{11}) = q, p(t_{21}, t_{12}) = 1 - q\}$, $q \in [0, 1]$. On the basis of the attacker's left information set and according to the Bayes formula, he/she can obtain the posterior probability distribution $\tilde{p}_2 = (q, 1 - q)$ after observing the defender's action a_{11} .

To analyze the equilibria for the situation with 'mixed' MTD, we first take the visiting strategy (a_{21}, a_{21}) as an example to discuss whether there exist pure strategy equilibria from the view of the defender.

According to Table 6, we can see that when providing hid-service, the defender's expected payoff by playing strategy a_{11} is

$$\begin{aligned} u_1(a_{11}|t_{11}) &= \tilde{p}_1(t_{21}|a_{21}) \cdot u_1(a_{11}, t_{11}, a_{21}, t_{21}) \\ &\quad + \tilde{p}_1(t_{22}|a_{21}) \cdot u_1(a_{11}, t_{11}, a_{21}, t_{22}) \\ &= p \cdot (-s - ka/(\beta_1 N_1)) \\ &\quad + (1 - p) \cdot (a - s), \end{aligned}$$

and the expected payoff by playing strategy a_{10} is

$$\begin{aligned} u_1(a_{10}|t_{11}) &= \tilde{p}_1(t_{21}|a_{21}) \cdot u_1(a_{10}, t_{11}, a_{21}, t_{21}) \\ &\quad + \tilde{p}_1(t_{22}|a_{21}) \cdot u_1(a_{10}, t_{11}, a_{21}, t_{22}) \\ &= p \cdot (-s) + (1 - p) \cdot (-a - s). \end{aligned}$$

The defender will choose strategy a_{11} for hid-service if $u_1(a_{11}|t_{11})$ is larger than $u_1(a_{10}|t_{11})$, i.e.,

$$\begin{aligned} p \cdot (-s - ka/(\beta_1 N_1)) + (1 - p) \cdot (a - s) \\ > p \cdot (-s) + (1 - p) \cdot (-a - s), \end{aligned}$$

which gives

$$p < \frac{2}{2 + k/(\beta_1 N_1)}.$$

From the analyses, we can see that when the service is hid-service, for the defender, strategy a_{11} is better than a_{10} under the condition $p < 2/(2 + k/(\beta_1 N_1))$; otherwise, strategy a_{10} is better than a_{11} .

Similarly, we can obtain that when the service is var-service, for the defender, strategy a_{11} is better

than a_{10} under the condition $p < 2/(2 + k/(\beta_2 N_2))$; otherwise, strategy a_{10} is better than a_{11} .

Therefore, the service strategy chosen by the defender can be one of the following three cases:

1. Under the conditions $p < 2/(2 + k/(\beta_1 N_1))$ and $p < 2/(2 + k/(\beta_2 N_2))$, the service strategy should be (a_{11}, a_{11}) .

2. Under the condition $2/(2 + k/(\beta_1 N_1)) < p < 2/(2 + k/(\beta_2 N_2))$ (when $\beta_1 N_1 < \beta_2 N_2$), the service strategy should be (a_{10}, a_{11}) . Otherwise, the service strategy should be (a_{11}, a_{10}) .

3. Under the conditions $p > 2/(2 + k/(\beta_1 N_1))$ and $p > 2/(2 + k/(\beta_2 N_2))$, the service strategy should be (a_{10}, a_{10}) , and this situation is out of our consideration.

Then, we analyze whether visiting strategy (a_{21}, a_{21}) is better than the other three visiting strategies for the first two cases.

1. When $p < 2/(2 + k/(\beta_1 N_1))$ and $p < 2/(2 + k/(\beta_2 N_2))$

In this situation, the visitor's expected payoffs for playing a_{21} and a_{20} are

$$\begin{aligned} u_2(a_{21}, t_{21}) &= q \cdot (ka/(\beta_1 N_1) - b) \\ &\quad + (1 - q) \cdot (ka/\beta_2 - b), \\ u_2(a_{21}, t_{22}) &= q \cdot a + (1 - q) \cdot a = a, \end{aligned}$$

and

$$\begin{aligned} u_2(a_{20}, t_{21}) &= q \cdot 0 + (1 - q) \cdot 0 = 0, \\ u_2(a_{20}, t_{22}) &= q \cdot 0 + (1 - q) \cdot 0 = 0. \end{aligned}$$

To ensure that the visitor chooses strategy (a_{21}, a_{21}) , the following conditions should be satisfied:

$$\begin{aligned} u_2(a_{21}, t_{21}) &> u_2(a_{20}, t_{21}), \\ u_2(a_{21}, t_{22}) &> u_2(a_{20}, t_{22}). \end{aligned}$$

Since the values of β_1 and β_2 should be in the same order of magnitude, and the value of N_1 is usually not small, e.g., a Class C subnet (Al-Shaer et al., 2013), we suppose $\beta_1 N_1 > \beta_2$, which gives

$$\beta_2 < \beta_1 N_1 < ka/b,$$

or

$$q < \frac{1 - \beta_2 b/(ka)}{1 - \beta_2/(\beta_1 N_1)} \text{ when } \beta_2 < ka/b < \beta_1 N_1.$$

Therefore, the defender and visitor strategy combination $((a_{11}, a_{11}), (a_{21}, a_{21}))$ can reach an equilibrium under either conditions $p < 2/(2+k/(\beta_1 N_1))$, $p < 2/(2+k/(\beta_2 N_2))$, and $\beta_2 < \beta_1 N_1 < ka/b$, or conditions $p < 2/(2+k/(\beta_1 N_1))$, $p < 2/(2+k/(\beta_2 N_2))$, and $q < (1-\beta_2 b/(ka))/(1-\beta_2/(\beta_1 N_1))$ when $\beta_2 < ka/b < \beta_1 N_1$.

2. When $\beta_1 N_1 < \beta_2 N_2$

In this situation, using the same analysis approach as described above, we can conclude that the defender and visitor strategy combination $((a_{10}, a_{11}), (a_{21}, a_{21}))$ can reach an equilibrium under the conditions $2/(2+k/(\beta_1 N_1)) < p < 2/(2+k/(\beta_2 N_2))$, $\beta_2 < ka/b$, $q < 1/2$, and $q < 1-\beta_2 b/(ka)$.

3. When $\beta_1 N_1 > \beta_2 N_2$

In this situation, the defender and visitor strategy combination $((a_{11}, a_{10}), (a_{21}, a_{21}))$ can reach an equilibrium under the conditions $2/(2+k/(\beta_2 N_2)) < p < 2/(2+k/(\beta_1 N_1))$, $\beta_1 N_1 < ka/b$, $q > 1/2$, and $q > \beta_1 N_1 b/(ka)$.

Next, we discuss whether there are equilibria or not for the visiting strategies (a_{21}, a_{20}) and (a_{20}, a_{21}) and we arrive at the following conclusions:

1. For the visiting strategy (a_{21}, a_{20}) , no matter which value is assigned to factor p , the defender can always choose strategy (a_{10}, a_{10}) . Conversely, for the defender's strategy (a_{10}, a_{10}) , through analyses similar to those above, we can find $u_2(a_{20}, t_{21}) > u_2(a_{21}, t_{21})$; i.e., for the attacker, he/she should choose action a_{20} rather than a_{21} . Therefore, the defender and visitor strategy combination $((a_{10}, a_{10}), (a_{21}, a_{20}))$ cannot reach an equilibrium.

2. For the visiting strategy (a_{20}, a_{21}) , no mat-

ter which value is assigned to factor p , the defender can always choose strategy (a_{11}, a_{11}) . Conversely, for the defender's strategy (a_{11}, a_{11}) , through analyses similar to those above, we can deduce that the visiting strategy (a_{20}, a_{21}) is the best either when $\beta_1 N_1 > \beta_2 > ka/b$, or when $\beta_1 N_1 > ka/b > \beta_2$ and $q > (1-\beta_2 b/(ka))/(1-\beta_2/(\beta_1 N_1))$. Therefore, the defender and visitor strategy combination $((a_{11}, a_{11}), (a_{20}, a_{21}))$ can reach an equilibrium either under the condition $\beta_1 N_1 > \beta_2 > ka/b$, or under the conditions $q > (1-\beta_2 b/(ka))/(1-\beta_2/(\beta_1 N_1))$ and $\beta_1 N_1 > ka/b > \beta_2$.

We summarize the PBE for the situation with 'mixed' MTD and their conditions in Table 9, in which the equilibria are represented by the same form as in Table 7.

5.3.2 Effect of 'mixed' MTD

As mentioned in Section 3.2, the baseline game has an equilibrium result that the server should provide service while the attacker and the user should request service under the condition $p < 2/(2+k)$, in which parameters p and k are determined and controlled by the attacker.

In our game with 'mixed' MTD, the three equilibria E_1-E_3 are equivalent to the equilibrium result of the baseline game, but the conditions are greatly changed. From Table 9, one can see that in our game, the conditions for E_1-E_3 are associated with not only parameters p and k determined and controlled by the attacker, but also parameters β_1 , β_2 , N_1 , N_2 , and q determined and controlled by the defender. As discussed in Section 5.2, for 'variation' MTD, the defender should mainly use the method of changing the value of β_2 to influence the attacker,

Table 9 Equilibria for situation 'mixed' and the corresponding conditions

Perfect Bayesian equilibrium	Condition
$E_1 (((a_{11}, a_{11}), (a_{21}, a_{21})), p)$	$p < \frac{2}{2+k/(\beta_1 N_1)}$ and $p < \frac{2}{2+k/(\beta_2 N_2)}$, and $\beta_2 < \beta_1 N_1 < \frac{ka}{b}$ or $p < \frac{2}{2+k/(\beta_1 N_1)}$ and $p < \frac{2}{2+k/(\beta_2 N_2)}$, and $q < \frac{1-\beta_2 b/(ka)}{1-\beta_2/(\beta_1 N_1)}$ when $\beta_2 < \frac{ka}{b} < \beta_1 N_1$
$E_2 (((a_{10}, a_{11}), (a_{21}, a_{21})), p)$	$\frac{2}{2+k/(\beta_1 N_1)} < p < \frac{2}{2+k/(\beta_2 N_2)}$, $q < \frac{1}{2}$, $q < 1-\frac{\beta_2 b}{ka}$, and $\beta_2 < \frac{ka}{b}$, when $\beta_1 N_1 < \beta_2 N_2$,
$E_3 (((a_{11}, a_{10}), (a_{21}, a_{21})), p)$	$\frac{2}{2+k/(\beta_2 N_2)} < p < \frac{2}{2+k/(\beta_1 N_1)}$, $q > \frac{1}{2}$, $q > \frac{\beta_1 N_1 b}{ka}$, and $\beta_1 N_1 < \frac{ka}{b}$, when $\beta_1 N_1 > \beta_2 N_2$,
$E_4 (((a_{11}, a_{11}), (a_{20}, a_{21})), p)$	$q > \frac{1-\beta_2 b/(ka)}{1-\beta_2/(\beta_1 N_1)}$ when $\beta_1 N_1 > \frac{ka}{b} > \beta_2$ or $\beta_1 N_1 > \beta_2 > ka/b$

and thus here the defender should consider only the change on the value of β_2 but not on the value of N_2 for var-service.

Now we have some further discussions on the four equilibria in these situations.

First, according to the conditions for equilibria E_1 – E_4 , the defender can increase the values of β_2 and $\beta_1 N_1$ to force the attacker to increase his/her attack probability or even to stop attack to retain his/her expected payoff. This can be viewed as the proactivity and effectiveness of ‘mixed’ MTD.

Second, the equilibria for ‘mixed’ MTD are related to the equilibria for ‘hidden’ and ‘variation’ MTDs, but not a simple combination of them. There are some new features, which are reflected mainly in the values of p and q :

1. For equilibria E_1 and E_4 , the hid-service and var-service are enabled to serve. From equilibria E_1 and E_4 , we can see that there are some ways to reach an equilibrium.

For equilibrium E_1 , under the conditions $p < 2/(2 + k/(\beta_1 N_1))$ and $p < 2/(2 + k/(\beta_2 N_2))$, the defender can just increase the values of β_2 and $\beta_1 N_1$ without considering the value of q , to force the attacker to increase his/her attack probability if the attacker wants to obtain his/her expected payoff. However, the influence is limited because of the existence of the limited conditions $\beta_2 < \beta_1 N_1 < ka/b$, $p < 2/(2 + k/(\beta_1 N_1))$, and $p < 2/(2 + k/(\beta_2 N_2))$.

To increase the influence, the defender can continue to increase the values of β_2 and $\beta_1 N_1$. When the value of $\beta_1 N_1$ is increased to satisfy the limited condition $\beta_2 < ka/b < \beta_1 N_1$, he/she has to consider the range of factor q (the probability of enabling the hid-service):

$$q < \frac{1 - \beta_2 b/(ka)}{1 - \beta_2/(\beta_1 N_1)}.$$

From this inequality, we can see that: (1) When the defender adjusts only the value of β_2 , the larger the value of β_2 , the smaller the value of q . This means that the greater the shuffling frequency of the enabled ‘variation’ MTD, the stronger the ability to confuse the attacker and disrupt attacks. Thus, the probability for the defender to enable the hid-service is accordingly lower. (2) When the defender adjusts only the value of $\beta_1 N_1$, the larger the value of $\beta_1 N_1$, the smaller the value of q . This means that under the limited condition $\beta_2 < ka/b < \beta_1 N_1$, if the defender

sets a higher frequency or larger configuration space for the ‘hidden’ MTD, the probability that the defender has to enable the hid-service again is lower. This is because the ‘hidden’ MTD can make the attacker lose the target. Also, the higher the shuffling frequency or the larger the configuration space, the lower the probability that the attacker finds the target again.

As mentioned above, the ‘hidden’ MTD can make the attacker lose the target, and the ‘variation’ MTD can just disrupt the attack over and over but cannot prevent the attacker from connecting to the target again. Intuitively, the defense ability of the ‘hidden’ MTD is stronger than the ‘variation’ MTD. Therefore, still under the limited condition $\beta_2 < ka/b < \beta_1 N_1$, the defender can increase the value of q to strength his/her defense. If the defender increases the value of q (i.e., enables the hid-service with much a higher probability) and makes it satisfy $q > (1 - \beta_2 b/(ka))/(1 - \beta_2/(\beta_1 N_1))$, the equilibrium would change to equilibrium E_4 where the defender provides a normal service, and the user requests the service while the attacker is not attacking, which is the greatest expectation for the defender.

Furthermore, if the defender also increases the value of β_2 and makes it satisfy the limited condition $\beta_1 N_1 > \beta_2 > ka/b$, then no matter which values factors p and q are, the defender and the attacker would remain in equilibrium E_4 . This is because, under this condition, either ‘hidden’ MTD or ‘variation’ MTD has a sufficient ability to disrupt attacks: the larger the value of β_2 , the higher the frequency of the deployed ‘variation’ MTD. Even though the defender cannot prevent the attacker from connecting to the server, he/she can rapidly disrupt the attack time after time. The larger the value of $\beta_1 N_1$, the lower the probability that the attacker finds the target and then launches another attack.

2. For equilibrium E_2 , the hid-service is disabled, and thus the defender should just increase the value of β_2 to influence the action of the attacker.

Equilibrium E_2 here is similar to equilibrium result E_1 in Section 5.2, but there are some differences in their conditions. In equilibrium E_2 here, the lower bound for the value of factor p is increased, and, from the view of the attacker, the probability of providing hid-service roughly satisfies $0 < q < 1/2$. According to these features, we can see that although the hid-service is not really serving, its existence (exactly, the

attacker's belief that the defender enables hid-service to serve) can effectively confuse the attacker. Specifically, compared with E_1 in Section 5.2, the attacker has to increase his/her attack probability to obtain the equivalent payoff to E_1 in Section 5.2. With the increase of the value of β_2 , the value of q decreases, which means that with investigation and analysis, the attacker would change his/her belief on the probability distribution over the service types. Specifically, the belief that the defender actually provides only the var-service is gradually confirmed. This conforms to the actual situation in the real world.

3. For equilibrium E_3 , the var-service is disabled, and thus the defender should increase the value of $\beta_1 N_1$ to influence the action of the attacker. Equilibrium E_3 here is similar to equilibrium result E_1 in Section 5.1, but there are some differences in their conditions. In equilibrium E_3 here, the lower bound for the value of factor p is increased, and from the view of the attacker, the probability of providing hid-service roughly satisfies $q > 1/2$. From these features, we can see that although the var-service is not really serving, its existence (exactly, the attacker's belief that the defender enables var-service to serve) can effectively confuse the attacker. Specially, compared with the E_1 in Section 5.1, the attacker has to increase his/her attack probability to obtain the equivalent payoff to E_1 in Section 5.1. With the increase of the value of $\beta_1 N_1$, the value of q increases, which means that with investigation and analysis, the attacker would change his/her belief on the probability distribution over the service types. In other words, the belief that the defender actually provides only the hid-service is gradually confirmed. This conforms to the actual situation in the real world.

6 Related work

As far as we know, the only related work that can be found in this direction was conducted by Shi *et al.* (2009). In that work, the authors analyzed the hopping mechanism of their service hopping approach (Shi *et al.*, 2007) by using incomplete information dynamic game theory. The work is meaningful; however, the analyses just took the initial fixed configuration characteristic (i.e., the size of the configuration space) of the hopping approach into account, without considering the characteristics manifested in the running process. Moreover, the condi-

tions for the equilibrium of the game in the situation of service hopping (i.e., $N \gg k$, $N \gg a > b$, and $N > ka/b$) were greatly limited.

Compared with Shi *et al.* (2009), there are four advantages in our study:

1. We have analyzed the defense mechanism of the three main types of MTD approaches from a more abstract perspective, while Shi *et al.* (2009) analyzed a specific service hopping approach, which is one of the 'hidden' MTD approaches in our case.

2. We have introduced a blocking factor β to represent the effect of MTD approaches on disrupting attack. Specifically, it reflects the influence caused by the shifting frequency of the MTD approach for defending.

3. We have taken the defense cost s into consideration. This is an important characteristic manifested in the running of each MTD. It is produced by the target's attack surface shifting, and its effect is manifested through the blocking factor β in our analyses.

4. Compared with Shi *et al.* (2009), the understanding and analyses of the effect of MTD approaches are different. We consider that the deployment of an MTD approach can influence only the attacker notably, and thus in the analyses we extend only the attacker's action set. Shi *et al.* (2009) considered that the deployment of the service hopping approach would influence both the attacker and the user, and thus extended the visitor's action set for analysis.

7 Conclusions

In this paper, we have investigated the defense mechanism of MTD technology in two dimensions. We first presented a defense model MP2R that is used to describe the defense process of MTD techniques. By comparing the MP2R model with the traditional PPDRR model, one can intuitively find the proactivity and effectiveness of MTD technology intuitively. Then, to analyze and verify the defense mechanism of MTD technology in theory, we used incomplete information dynamic game theory. We specified the game models for the interaction between a defender who equips a server with different types of MTD approaches and a visitor who can be a normal user or an attacker. Thereafter, we investigated and characterized the equilibria and their

conditions for these models. Moreover, by comparing the equilibria and their conditions of our game models with the equilibrium and its condition of the baseline game presented by Shi *et al.* (2009), we verified the proactivity and effectiveness of the MTD technology, and identified that the size of the configuration space and the shifting frequency are the two key factors that influence the effect of MTD.

In the MTD field, deception defense may be incorporated with other MTD approaches (Carroll *et al.*, 2014; Moody *et al.*, 2014), or directly be considered as an MTD approach (Urias *et al.*, 2015). However, we have not analyzed the situation with deception defense in this paper, and it can be our future work.

References

- Al-Shaer, E., Duan, Q., Jafarian, J.H., 2013. Random host mutation for moving target defense. *Int. Conf. on Security and Privacy in Communication Systems*, p.310-327. https://doi.org/10.1007/978-3-642-36883-7_19
- Azab, M., Hassan, R., Eltoweissy, M., 2011. ChameleonSoft: a moving target defense system. *7th Int. Conf. on Collaborative Computing: Networking, Applications and Worksharing*, p.241-250. <https://doi.org/10.4108/icst.collaboratecom.2011.247115>
- Cai, G., Wang, B., Hu, W., *et al.*, 2016a. Moving target defense: state of the art and characteristics. *Front. Inform. Technol. Electron. Eng.*, **17**(11):1122-1153. <https://doi.org/10.1631/FITEE.1601321>
- Cai, G., Wang, B., Luo, Y., *et al.*, 2016b. Characterizing the running patterns of moving target defense mechanisms. *18th Int. Conf. on Advanced Communication Technology*, p.191-196. <https://doi.org/10.1109/ICACT.2016.7423324>
- Carroll, T., Grosu, D., 2011. A game theoretic investigation of deception in network security. *Secur. Commun. Netw.*, **4**(10):1162-1172. <https://doi.org/10.1002/sec.242>
- Carroll, T., Crouse, M., Fulp, E., *et al.*, 2014. Analysis of network address shuffling as a moving target defense. *IEEE Int. Conf. on Communications*, p.701-706. <https://doi.org/10.1109/ICC.2014.6883401>
- Carter, K., Riordan, J., Okhravi, H., 2014. A game theoretic approach to strategy determination for dynamic platform defenses. *1st ACM Workshop on Moving Target Defense*, p.21-30. <https://doi.org/10.1145/2663474.2663478>
- Carvalho, M., Bradshaw, J., Bunch, L., *et al.*, 2012. Command and control requirements for moving-target defense. *IEEE Intell. Syst.*, **27**(3):79-85. <https://doi.org/10.1109/MIS.2012.45>
- Colbaugh, R., Glass, K., 2012. Predictability-oriented defense against adaptive adversaries. *IEEE Int. Conf. on Systems, Man, and Cybernetics*, p.2721-2727. <https://doi.org/10.1109/ICSMC.2012.6378159>
- Hobson, T., Okhravi, H., Bigelow, D., *et al.*, 2014. On the challenges of effective movement. *1st ACM Workshop on Moving Target Defense*, p.41-50. <https://doi.org/10.1145/2663474.2663480>
- Huang, Y., Ghosh, A., 2011. Introducing diversity and uncertainty to create moving attack surfaces for web services. *In: Jajodia, S., Ghosh, A., Swarup, V., et al. (Eds.), Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Springer New York, New York, p.131-151. https://doi.org/10.1007/978-1-4614-0977-9_8
- Jajodia, S., Ghosh, A., Swarup, V., *et al.*, 2011. *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Springer Science & Business Media.
- Jia, C., Zhong, A., Zhang, W., *et al.*, 2006. Incomplete informational and dynamic game model in network security. *J. Comput. Res. Dev.*, **43**(Suppl.):530-533 (in Chinese).
- Liu, C., Zhang, Y., Chen, R., 2011. Research on dynamic model for network security based on artificial immunity. *Int. J. Knowl. Lang. Process.*, **2**(3):21-35.
- Lye, K.W., Wing, J., 2005. Game strategies in network security. *Int. J. Inform. Secur.*, **4**(1-2):71-86. <https://doi.org/10.1007/s10207-004-0060-x>
- Manadhata, P., 2013. Game theoretic approaches to attack surface shifting. *In: Jajodia, S., Ghosh, A., Subrahmanian, V., et al. (Eds.), Moving Target Defense II: Application of Game Theory and Adversarial Modeling*. Springer New York, New York, p.1-13. https://doi.org/10.1007/978-1-4614-5416-8_1
- Manshaei, M., Zhu, Q., Alpcan, T., *et al.*, 2013. Game theory meets network security and privacy. *ACM Comput. Surv.*, **45**(3):25. <https://doi.org/10.1145/2480741.2480742>
- Moody, W.C., Hu, H., Apon, A., 2014. Defensive maneuver cyber platform modeling with stochastic Petri Nets. *Int. Conf. on Collaborative Computing: Networking, Applications and Worksharing*, p.531-538. <https://doi.org/10.4108/icst.collaboratecom.2014.257559>
- NITRD, 2009. *National Cyber Leap Year Summit 2009. Co-chairs' Report*. https://www.nitrd.gov/fileupload/files/National_Cyber_Leap_Year_Summit_2009_CoChairs_Report.pdf
- NITRD, 2010. *NITRD CSIA IWG Cybersecurity Game-Change Research and Development Recommendations*. <https://www.nitrd.gov/cybersecurity/>
- Okhravi, H., Hobson, T., Bigelow, D., *et al.*, 2014. Finding focus in the blur of moving-target techniques. *IEEE Secur. Priv.*, **12**(2):16-26. <https://doi.org/10.1109/MSP.2013.137>
- Prakash, A., Wellman, M., 2015. Empirical game-theoretic analysis for moving target defense. *2nd ACM Workshop on Moving Target Defense*, p.57-65. <https://doi.org/10.1145/2808475.2808483>
- Shi, L., Jia, C., Lu, S., 2007. DoS evading mechanism upon service hopping. *IFIP Int. Conf. on Network and Parallel Computing Workshops*, p.119-122. <https://doi.org/10.1109/NPC.2007.59>
- Shi, L., Jia, C., Lv, S., 2009. A game theoretic analysis of service hopping mechanism for DoS defense. *J. Electron. Inform. Technol.*, **31**(1):228-232 (in Chinese).

- Urias, V.E., Stout, W.M.S., Loverro, C., 2015. Computer network deception as a moving target defense. Int. Carnahan Conf. on Security Technology, p.1-6. <https://doi.org/10.1109/CCST.2015.7389665>
- Vadlamudi, S., Sengupta, S., Kambhampati, S., et al., 2016. Moving target defense for web applications using Bayesian Stackelberg games. arXiv:1602.07024.
- Winterrose, M.L., Carter, K.M., 2014. Strategic evolution of adversaries against temporal platform diversity active cyber defenses. Proc. Symp. on Agent Directed Simulation, p.9.
- Winterrose, M.L., Carter, K.M., Wagner, N., et al., 2014. Adaptive attacker strategy development against moving target cyber defenses. arXiv:1407.8540.
- Zhu, Q., Başar, T., 2013. Game-theoretic approach to feedback-driven multi-stage moving target defense. *LNCIS*, **8252**:246-263. https://doi.org/10.1007/978-3-319-02786-9_15
- Zhuang, R., DeLoach, S., Ou, X., 2014. Towards a theory of moving target defense. 1st ACM Workshop on Moving Target Defense, p.31-40. <https://doi.org/10.1145/2663474.2663479>