Computer Science Review 48 (2023) 100544

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

A survey: When moving target defense meets game theory

Jinglei Tan, Hui Jin[1], Hongqi Zhang, Yuchen Zhang, Dexian Chang, Xiaohu Liu, Hengwei Zhang*

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
Henan Key Laboratory of Information Security, Zhengzhou 450001, China

ARTICLE INFO

Article history:
Received 17 November 2022
Received in revised form 18 January 2023
Accepted 12 February 2023
Available online 22 February 2023

Keywords:
Moving target defense
Game theory
Spatial MTD strategies
Temporal MTD strategies
Spatiotemporal MTD strategies
Bounded rationality MTD strategies

ABSTRACT

Moving target defense (MTD) can break through asymmetry between attackers and defenders. To improve the effectiveness of cybersecurity defense techniques, defense requires not only advanced and practical defense technologies but effective, scientific decision-making methods. Due to complex attacker–defender interaction, autonomous, automatic, accurate, and effective selection of the optimal strategy is a challenging topic in the field of MTD. The essence of cybersecurity lies in the interaction between the attacker and defender. Game theory is a useful mathematical tool for strategy selection in a competitive environment. It provides strong theoretical support for the analysis of cyberattack and defense behaviors and subsequent decision-making, and can significantly improve the decision-making ability of MTD. This study presents the basic concepts of MTD and game theory, followed by a literature review, to study MTD decision-making methods based on game theory from the dimensions of space, time, space–time, and bounded rationality. Limitations of MTD game decision-making studies are discussed, as well as research directions, to provide references for future research.

Contents

* Corresponding author at: State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China.
E-mail address: wlby_zzmy_henan@163.com (H. Zhang).

[1] Co-First Author.

https://doi.org/10.1016/j.cosrev.2023.100544
1574-0137/

1. Introduction

With the rapid and continuous development of network technologies, the network information system has become increasingly complex. Cyberspace is not only the focus of government, industry, and academia; it is relevant to the daily life of every individual. Cyberspace is the object of more and more prominent threats, such as cyberattacks. Security attacks continuously emerge, and attacker–defender interaction intensifies. Advanced persistent threats (APTs) are common because of strong concealment, long incubation periods, and strong confrontation, posing a peculiar security threat to cyberspace [1]. According to the "ENISA Threat Landscape 2022 (ETL)" report released by the European Union Agency for Cybersecurity [2], the global cybersecurity situation is not optimistic, with a record number of network loopholes, increasingly diverse extortion methods, and new attack strategies, bringing challenges to traditional defense technologies, and an unprecedented level of global cybersecurity competition.

Due to their small scale, security issues were not as obvious in the early stages of network information systems. With their rapid development, highly interconnected systems have become prone to various attacks. While a target network information system cannot be damaged directly through physical attacks, anonymous attacks can be remotely launched, such as through phishing emails and malicious data packets. Once one device in a system is compromised, an attacker can take it as a platform from which to launch lateral attacks at a very low cost, causing significant impact on the security of the entire system. To effectively defend against malicious attacks requires the defender to monitor the status of a system around the clock, continuously analyze changes in network traffic, and patch discovered loopholes. Defense strategies such as firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) have to a certain extent provide good solutions for network traffic monitoring and asset protection. As the internet expands, the cost of security management and maintenance continues to grow.

Cybersecurity faces an asymmetric situation: it is easy to attack and difficult to defend, and defense has the disadvantage of passivity. As a novel, disruptive defense method, moving target defense (MTD) can break through asymmetry. MTD continuously changes the vulnerable attack surface of a system through dynamic configuration, increasing its elasticity and unpredictability and providing active defenses. To improve the effectiveness of cybersecurity defense requires not only advanced and practical defense technologies, but effective scientific decision-making methods. Due to complex attacker–defender interaction, the autonomous, automatic, accurate, and effective selection of the optimal strategy is a challenging topic in MTD. The essence of cybersecurity lies in the interaction of the attacker and defender. Game theory is a mathematical tool for strategy selection in a competitive environment, providing theoretical support for the analysis of cyberattack and defense behaviors and subsequent decision-making; hence it can improve the decision-making ability of MTD.

By using search tools and databases such as Google Academic and Web of Science, we have collected references covering topics such as MTD and game theory. The references mainly focus on the recent 10 years. The existing reviews conducted relevant investigations on MTD and game theory. Zhu et al. [3] mainly focused on the study of network deception defense centered on game theory and machine learning. Zhang et al. [4] summarized and reviewed representative deception technologies in network active defense in the past three decades, including honeypots, honeytokens, and MTD. Pawlick et al. [5] studied the development of deception defense technology from the perspective of game theory, but did not involve other defense technologies other than deception defense. Cho et al. [6] reviewed the classification, design and application of active and adaptive MTD. Cai et al. [7] discussed the theory, strategy and evaluation of MTD, and analyzed the safety and effectiveness characteristics of MTD. Similarly, Sengupta et al. [8] reviewed the decision-making, implementation and evaluation of MTD at the network layer, but did not fully discuss the decision-making methods of MTD based on game theory.

The rest of this survey is organized as follows: Section 2 introduces MTD and game theory, respectively. Section 3 presents different spatial and temporal strategies used in MTD. Section 4 reviews MTD game decision-making methods from the dimensions of space, time, space–time, and bounded rationality. Section 5 discusses the limitations of MTD game decision-making studies and future research directions.

2. MTD and game theory overview

The attacker, whose action the traditional network defense mechanism cannot accurately predict, gradually gains a competitive advantage in the cyberattack and defense game, which poses a security threat and generates high defense costs. The main reasons for the disadvantage of cyber defense are as follows:

(1) Limited by the technology level, and with the continuous increase of the system scale and logical complexity, it is difficult for developers of software systems and network communications to build a system without loopholes. In addition, software design focuses primarily on availability and stability [9], and less on security;

(2) The network ecosystem cannot achieve complete autonomy, and the security of its components cannot be guaranteed during construction. Software and hardware components may come from different manufacturers, making it easy to insert backdoors, and difficult to find them;

(3) The network architecture is deterministic and static [10], which places cybersecurity defense at a disadvantage. The attacker has a time advantage, and can persistently detect and mine vulnerabilities and implement targeted attacks, which defenders can only discover and patch after the fact;

(4) There is a cost gap between attackers and defenders. The defender must identify and repair all security loopholes to the extent possible; hence the defense cost is high. The attacker only needs to find one loophole to cause huge damage. The homogeneity of network architecture benefits attackers and decreases their cost.

It can be seen that the attacker knows its attack object, time, target, and method, whereas the defender is uncertain and must

spend significant time and resources to evade any attack detection or intrusion activities. The traditional static defense is unable to adapt to attacker–defender interaction in contemporary network systems, and attackers benefit from inherent asymmetries in time, cost, and information. There is no theoretical symmetry between defenders and attackers; hence it is imperative to develop a new defense technology.

2.1. MTD connotation theory

Cybersecurity has evolved from passive to active. A disruptive MTD technology has emerged to address asymmetric threats. While defense strategies blindly reduce the vulnerable attack surface of an exposed network information system, MTD limits its exposure time through dynamics, randomness, and heterogeneity. The idea is to build a dynamic network information system. By implementing continuous and dynamic changes to confuse attackers, MTD reduces the homogeneity, static property, and certainty of a system, thereby increasing the uncertainty and unpredictability for the attacker.

The idea of MTD was actually applied in the battlefield of ancient China. The famous military thinker Sun Wu wrote in The Art of War, "Those who attack and succeed, attack what is not defended; those who defend and succeed, defend what is not attacked. Therefore, for those who are good at attacking, the enemy does not know what to defend; and for those who are good at defending, the enemy does not know what to attack". This reflects the importance of combining feints and real actions to improve overall military strength. The ideas of active and random changes in defense have long been applied to cybersecurity. Frequency hopping technology in wireless communication [11] achieves covert communication by changing the communication frequency pseudo-randomly.

The National Cyber Leap Year Summit 2009, Co-Chairs' Report [12] first proposed the concept of MTD: "An important benefit of moving target defense is to decrease the known attack surface area of our systems to adversaries while simultaneously shifting it. … By making the attack surface of software appear chaotic to adversaries, we force them to significantly increase the work effort to exploit vulnerabilities for every desired target". In 2010, the NITRD CSIA IWG Cybersecurity Game-Change Research & Development Recommendations [13] made a series of recommendations in the area of cyberattack defense technologies and clarified the concept of moving targets. In 2014, the Report on Implementing the Federal Cybersecurity Research and Development Strategy [14] defined the vision of MTD research, i.e., to develop, evaluate, and deploy diverse mechanisms and strategies that dynamically shift and change over time to increase complexity and costs for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency. It also clarified the agencies undertaking MTD research tasks, including the Defense Advanced Research Projects Agency, Army Research Laboratory, National Institute of Standards and Technology, National Security Agency, Office of Naval Research, and Office of the Secretary of Defense. Since then, MTD research has taken center stage and realized a series of accomplishments.

MTD aims to create a dynamic network information system by shifting or disguising resources probed by attackers. When malware gains access to MTD systems, it cannot find resources to cause damage. A dynamic and active mechanism can disrupt attackers, provide reliable network defense, and reduce the certainty, homogeneity, and stativity of a system, reducing the probability of a successful attack. This greatly reduces the attack time, making it difficult to complete. MTD is attack-agnostic, and therefore effective against many variations of known and unknown attacks. Fig. 1 shows the theoretical framework of MTD.

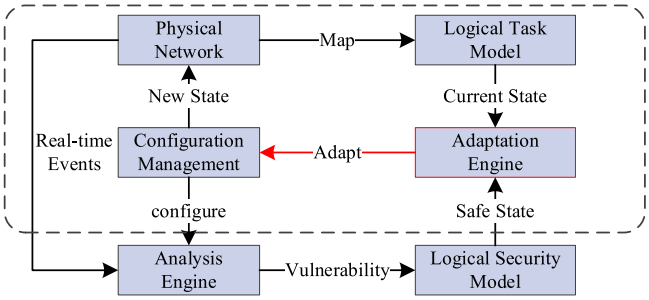

Fig. 1. Theoretical framework of MTD.

The physical network is mapped to a logical task model, whose current state is obtained by the adjustment engine. The analysis engine obtains real-time events on the physical network and uses traditional defense mechanisms such as intrusion detection and firewalls to analyze vulnerabilities. The logical security model generates a logical security state and sends it to the adjustment engine. The configuration management module implements the response MTD strategy. A closed self-feedback dynamic adjustment defense system has been formed. Specific MTD strategies will be discussed in Section 3.

2.2. MTD principles

MTD continuously changes the attack surface and exploration surface (Fig. 2), to confuse the attacker and increasing the difficulty and cost of an attack. It forces the attacker to continuously pursue the target, thereby eliminating the advantages of time, information asymmetry, and cost.

MTD requires the defender to constantly shift the attack surface. Intuitively, defenders can shift the attack surface by changing resources or their force. However, not all changes can shift the attack surface, and the defender must change at least one type of attack surface resource (e.g., IP address, number of open ports), or the impact of a certain type of resource (e.g., permissions required to execute certain commands). With all else unchanged, i.e., no new vulnerabilities and/or risks, an attack whose context have undergone the above changes will no longer be effective. As shown in Fig. 3, MTD increases the attacker's reconnaissance space through dynamic changes to increase the attack cost and complexity, and shortens the attacker's reconnaissance time through continuous changes to reduce the time advantage and information asymmetry advantage of the attack. The internal attack surface is the set of all the vulnerabilities of the network system, it only changes with the actual structure of the network and nodes, and can be actually seen by the administrator. The external attack surface is the set of exploitable vulnerabilities obtained by the attacker through reconnaissance, which changes with the active nodes in the network, services provided, etc. Exploration space is one way for defenders to increase the attack cost by expanding the external attack surface. It increases the exploration cost from a spatial perspective, which can be achieved by providing false active nodes and services. Configuration space changes are implemented under the premise of functional equivalence, which have a mapping relationship with the external attack surface changes. Hence, the attacker must pay more, increase the time, or change the method.

2.3. Game theory basics

Game theory [15] is a mathematical analysis tool to describe and analyze the behavior of multi-agents, to study decision-making in confrontational environments. When the payoffs of

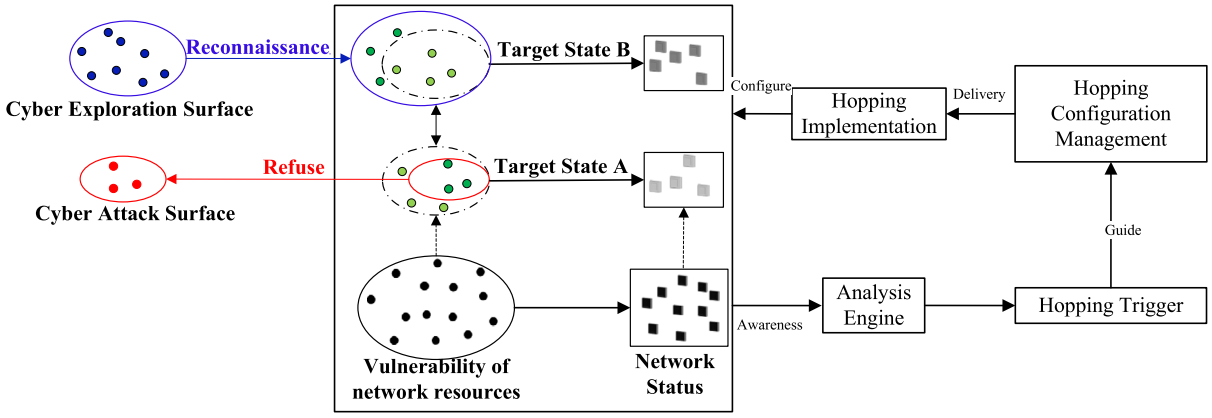

Fig. 2. Constantly changing network attack surface and exploration surface of MTD system.

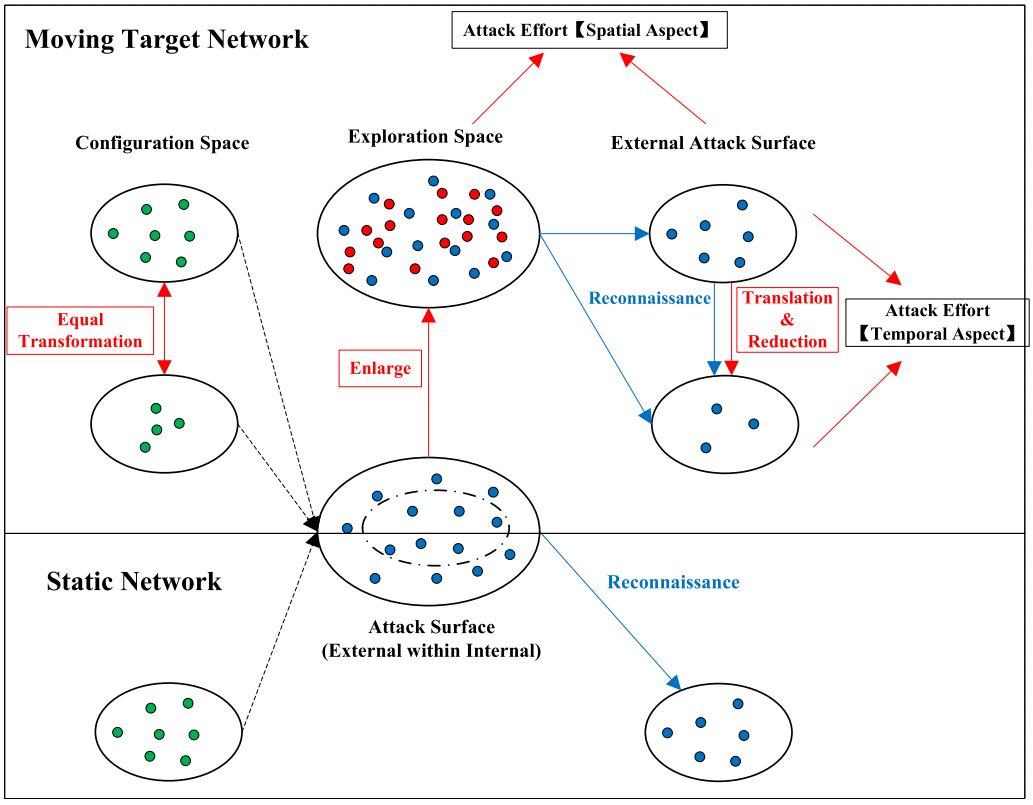

Fig. 3. MTD principles.

players impact each other, game theory selects the strategy with the maximum payoffs, and the equilibrium state is determined by the choices of the players, who seek to maximize their payoffs. Hence it is suitable for a strategy selection problem of multiple interdependent players. The strategy of one player is related to that of others, and it affects their decision-making. Based on the game rules, players choose and implement strategies according to the known information in order to maximize their payoffs. The elements of a game include the participants, strategy set, information, payoffs, order, equilibrium, and rationality, as shown in Table 1.

Fig. 4 shows the relationship between game theory and MTD attack–defense. The attacker and defender are the players. The attack and defense strategy space constitutes the strategy set. The game information consists of knowledge of the opponent's strategy in the confrontation and strategic payoffs. The sequence of strategies implemented by attackers and defenders is the game order, and their optimal strategies form the game equilibrium.

With similar characteristics to game theory, MTD attack-defense can be regarded as a special game process [16] in which the attacker detects and exploits the vulnerable attack surface of the network information system and tries to control it by various methods. MTD changes or transfers the attack surface through dynamic randomization, and diversification methods, to increase the attack complexity. Thus, the goals of the attacker and defender are antagonistic. The effectiveness of a selected strategy of an attacker or defender also depends on the opponent's strategy; hence their strategies are dependent. In addition, both aim to select the optimal strategy based on the cost and payoff, so the attacker and defender are competing. Game theory has the characteristics of antagonistic objectives, strategic dependence, and a competitive relationship between the players, which are consistent with those of MTD attack–defense; hence it has been

Table 1
Basic elements of a game.

Elements	Description
Player	The decision-maker who selects the optimal strategy from the strategy set
Strategy set	The set of all strategies available for each player, which describes when the player takes what action
Payoff	Gains of each player
Information	Knowledge that helps players to select strategies, such as about strategy sets and payoffs
Game order	The order in which players select and implement a strategy
Equilibrium	The optimal strategy when all players have maximum payoffs
Degree of rationality	The player's ability to maximize its payoff and seek optimal strategies

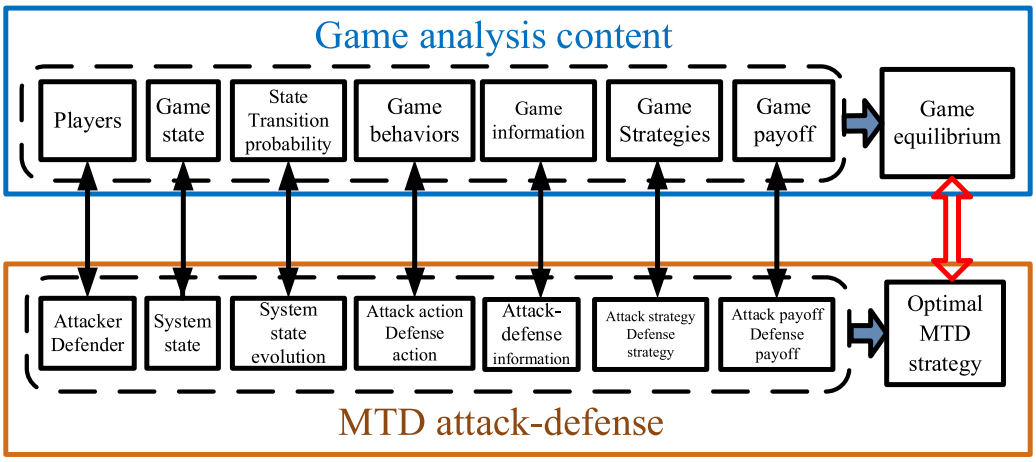

Fig. 4. Correspondence between game theory and attacker–defender interaction in MTD.

found to be an effective means to study MTD decision-making problems.

The application of game theory to MTD requires appropriate game models for different scenarios. Current models assume a completely rational attacker and defender. Models can be static or dynamic, depending on strategies, and can have complete or incomplete information, resulting in four types of models [17]: complete information static, incomplete information static, complete information dynamic, and incomplete information dynamic.

Due to the continuous and dynamic characteristics of cyberattacks and defenses, it is sometimes difficult to meet the constraints of the simultaneous actions of attackers and defenders. Hence, dynamic game models are more appropriate. In MTD, the attacker and defender have either complete or incomplete information regarding each other's strategies and their payoffs, i.e., MTD can have complete or incomplete information.

Because of the continuity and dynamics of network attack and defense confrontation, it is difficult to meet the constraints of simultaneous actions of both attack and defense sides. Therefore, compared with the static game model, the dynamic game model is more consistent with the actual network attack and defense. At present, there are two situations in the MTD attack and defense process: (1) Both sides of MTD attack and defense know each other's strategy set and the payoff generated by implementing the strategy, which is called complete information. For example, the attacker knows that the defender will adopt firewall technology, intrusion detection technology and other defensive measures when protecting the target network system. The defender knows the resource vulnerability or vulnerability set used by the attacker when attacking the target network system, and both attack and defense parties know the payoff brought by the implementation of their strategies. (2) Both sides of MTD attack and defense do not fully understand the opponent's strategy set and the payoff generated by implementing the strategy, which is called incomplete information. For example, the attacker does not know the defense strategy deployment to the target network system and whether honeypot defense technology and other attack deception means are used. The defender is not clear about the payoff generated by the attacker's use of zero-day vulnerabilities and new security threats. Therefore, the attack–defense confrontation model can be divided into dynamic game models under complete information and incomplete information, corresponding to two typical application scenarios — complete information and incomplete information attack–defense application scenarios.

Classical game theory has limitations in the aspects of the rationality assumption, equilibrium solution, equilibrium selection, and experimental environment: (1) The assumption of complete rationality does not match the facts. It assumes that players always show perfect analysis and reasoning, judgment and decision-making, and information processing in a dynamic confrontational environment, and that they know how to realize their own best interests and seek optimal strategies. However, in reality, decision-making takes place in a complex environment, and it is impossible for a player to have perfect rationality; (2) It is difficult to find equilibrium. While the Nash equilibrium exists in theory, Nash did not prove that it could be constructed; (3) It is difficult to choose from multiple Nash equilibria. Classical game theory emphasizes the equilibrium state, while ignoring the dynamic process of reaching it. Therefore, when a Nash equilibrium is not unique, a player cannot predict the real result of a game. In fact, the equilibrium formation is a dynamic convergence process in which the players constantly revise their strategies; (4) The requirements for the experiment environment are high. The optimal response of the game model depends on the authenticity and reliability of the simulation data. Therefore, the experimental environment must be continuously improved.

3. Classification of MTD strategies

We consider MTD strategies as either spatial or temporal. Spatial strategies determine the target to be changed, i.e., the strategy taken by a network information system to effectively defend against attacks. Temporal strategies define the time when a target is moved, i.e., the time required to transfer to a new state.

Table 2
Classification of spatial MTD strategies at different protocol stack hierarchy levels.

No.	Strategy	Switching parameters
1	REL-MTD	RAM address, instruction set
2	SL-MTD	Instruction sequence, packet formats, programming language, interpretable language of application codes
3	DL-MTD	Memory data and application data in data layer, such as format, syntax, encoding, encryption method, and representation
4	PL-MTD	Operating system version, CPU hardware architecture, operating system instance, platform data format, virtual machine, and host security configuration
5	NL-MTD	IP addresses, communication ports, network protocols, network topology, and routing paths

3.1. Spatial MTD strategies

3.1.1. Classification by network protocol stack hierarchy

Spatial MTD strategies are feasible defense measures for different system elements, security threats, and application scenarios. The purpose is to increase the complexity of cyberattacks by reducing system homogeneity, stativity, or certainty. According to the network stack protocol layers, strategies include the runtime environment layer MTD (REL-MTD), software layer MTD (SL-MTD), data layer MTD (DL-MTD), platform layer MTD (PL-MTD), and network layer MTD (NL-MTD) [18], as shown in Table 2.

REL-MTD dynamically changes parameters such as the RAM address and instruction set of the runtime environment layer, and can be divided into two categories: (1) Address space layout randomization (ASLR) [19] randomizes the code, function library, stack, function, and other memory layout parameters. Examples include address space layout permutation (ASLP) [20], memory randomization (MR) [21], and code obfuscation [22]; (2) Instruction set randomization (ISR) [23] randomizes ports, interfaces and other parameters of the operating system. Examples are RandSys [24], randomized instruction set emulation (RISE) [25], and CIAS code call randomization [26].

SL-MTD dynamically changes parameters in the software layer, such as the instruction sequence, packet format, programming language, and interpretable language. Examples include compact control flow integrity and randomization (CCFIR) [27], software diversity based on distributed coloring algorithms [28], proactive obfuscation (PO), and GenProg automatic software repair [29].

DL-MTD dynamically changes the parameters of memory and application data in the data layer, such as the format, syntax, encoding, encryption method, and representation. Examples are data diversity (DD) [30], redundant data diversity (RDD) [31], data randomization (DR) [32], and HERMES cryptographic key randomization [33].

PL-MTD dynamically changes the operating system version, CPU hardware architecture, operating system instance, platform data format, virtual machine, and host security configuration at the platform layer. Such strategies include the modified commodity operating system DÜPPEL [34], the multiple operating system rotational environment (MORE) [35], dynamic application rotation environment (DARE) [36], and self-cleansing intrusion tolerance (SCIT) [37].

NL-MTD dynamically changes parameters such as IP addresses, communication ports, network protocols, network topology, and routing paths at the network layer. Examples include end point route mutation (EPRM) [38], the reconnaissance deception system (RDS) [39], the dynamic backbone (DynaBone) strategy [40], and randomized intrusion-tolerant asynchronous services (RITAS) [41].

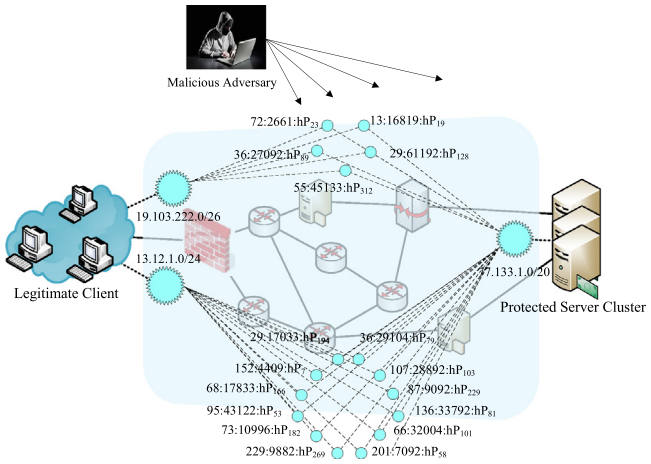

Fig. 5. Dynamic spatial MTD strategy (taking IP hopping as an example).

3.1.2. Classification by basic attributes

Spatial MTD strategies can be abstracted to dynamic, diverse, and redundant transformation of network vulnerabilities, and can be categorized as shuffle MTD (S-MTD), diversity MTD (D-MTD), and redundant MTD (R-MTD), as shown in Table 3.

S-MTD dynamically configures a network information system, such as by IP hopping [42], random host mutation [43], network topology reconfiguration [44], and virtual machine migration [45], randomizing configurations to increase the uncertainty of attackers. For instance, IP addresses in the communication link are dynamically changed in real time, making them difficult to accurately obtain, thus precluding attacks (Fig. 5).

D-MTD diversifies the configurations of network information systems, including servers, programming languages, operating systems, and hardware [46,47], providing alternatives with the same function but different structures, so as to improve resilience and fault tolerance and increase an attacker's time and energy cost. For instance, a protected server cluster might include Windows, Linux, and Unix operating systems, requiring an attacker to scan all variants to formulate an attack plan, which increases their spatiotemporal costs (Fig. 6).

R-MTD increases the redundancy of configurations of servers, hardware, operating systems, software, and services [48,49]. For example, with multiple protected server cluster components, once a cluster is attacked and destroyed, services can be migrated to another server cluster, thereby guaranteeing service availability (Fig. 7).

3.2. Temporal MTD strategies

Temporal MTD strategies focus on the timing of the implementation of an MTD strategy. These can be time-, event-, or

Table 3
Classification of basis attributes of spatial MTD strategies.

No.	Strategy	Switching parameters
1	S-MTD	Shuffling of system configurations, such as IP hopping, random host mutation, network topology reconfiguration, virtual machine migration
2	D-MTD	Diversity of system configurations, such as servers, programming languages, operating systems, hardware
3	R-MTD	Redundancy of system configurations, such as number of components for replicas of servers, hardware, operating systems, software, services

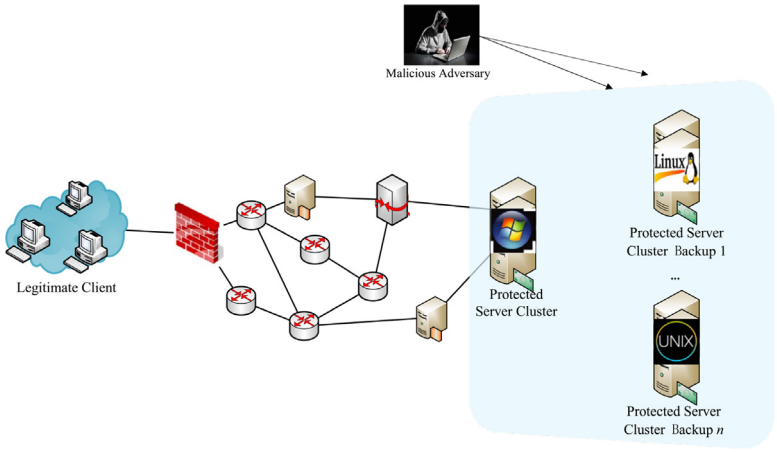

Fig. 6. Diversity spatial MTD strategy (taking operating system diversity as an example).

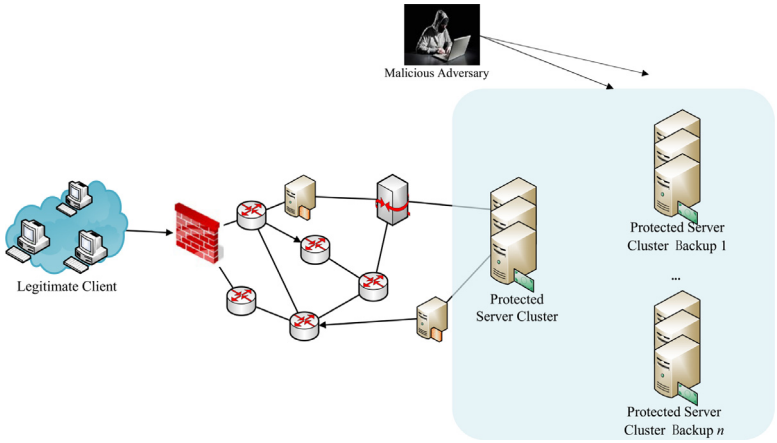

Fig. 7. Redundant MTD spatial strategy (taking server redundancy as an example).

hybrid-driven, represented by blue, red, and purple lines, respectively, in Fig. 8.

3.2.1. Time-driven temporal MTD strategies

Time-driven temporal MTD strategies predict possible cyber-attacks, and implement an MTD strategy at a set time. By changing the system parameters (e.g., IP address, port number, MAC address, network protocol, routing path), the attack surface can be changed to achieve active defense without interrupting network communication. This type of strategy is proactive, yet the selection of the time of change depends on prior experience and comes at a certain cost. Hence it may affect quality of service (QoS).

The key to a time-driven strategy is to determine the time interval of change, which can be random or uniform: (1) The uniform strategy predefines the time. Jafarian et al. [50] proposed OpenFlow Random Host Mutation (OF-RHM) based on software defined networking (SDN), with a 5-s time interval. Thompson et al. [51] proposed an MTD method for multi-OS migration, which intervals of 60 s and 5 min, depending on the scenario. Aydeger et al. [52] proposed a route mutation method for crossfire attacks, with time intervals of 5 s and 20 s to compare congested links. Although increasing the time interval helps alleviate link congestion, it can lead to communication delay of data packets; (2) The random strategy predefines the transfer time interval. Algin et al. [53] proposed a dynamic data scheduling scheme based on a randomized transfer time for selective jamming attacks of smart meter data collection, using time intervals of 15 s, 30 s, 60 s, and 120 s. Albanese et al. [54] proposed an identity virtualization-based MTD mechanism for ad hoc networks, with time intervals of [100, 105], [50, 55], [20, 25], and [10, 15].

Time-driven strategies ensure that any information obtained by the attacker expires quickly. Too long of a switching interval

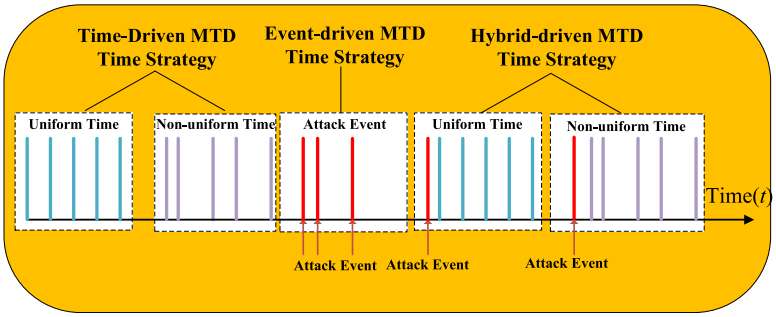

Fig. 8. Classification of temporal MTD strategies. . (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

gives an attacker enough time to scan and penetrate the system, leading to a certain damage to the system. Too short of an interval triggers time-driven strategies regardless of whether an attack is launched. To trigger an MTD strategy when the system is not under attack will waste defense resources and reduce system performance, which impacts QoS.

3.2.2. Event-driven temporal MTD strategies

The switching time interval of event-driven MTD strategies is variable, the attack surface is changed adaptively using a time function based on the attack event, and the strategy is triggered by external information such as security alarms and strategies. Different from time-driven strategies, they greatly reduce unnecessary overhead. However, they have an obvious lag in the response to attacks.

Debroy et al. [55] proposed an MTD mechanism based on virtual machine (VM) migration for denial-of-service (DoS) attacks, selecting the optimal strategy according to the cyberattack interarrival time function, i.e., the sum of the attacked and idle periods. Zhang et al. [56] maximized the mutation space by collaborative random end-point and routing mutation, and carried out detection of attackers at the same time. The MTD strategy was adjusted according to the results of detection to reduce system overhead. DeLoach et al. [57] proposed a model-driven MTD mechanism for enterprise network security, which triggers the MTD strategy based on attack data obtained by the intrusion detection system and security information and event management system (SIEMS). Tamba et al. [58] proposed an event-driven MTD mechanism to ensure the stability and communication load of physical information systems. Xu et al. [59] used in-band network telemetry (INT) to obtain the bottom network state, which triggered a random routing mutation strategy. Keromytis et al. [60] proposed a cloud security architecture, MEERKATS, that senses changes in the cloud and data environment based on distributed monitoring and detects state information and out-of-order behavior based on probabilistic anomaly-detection algorithms. Wu et al. [61] proposed an SDN-based port and address hopping technology for DDoS attacks, which dynamically detects SYN flood attacks based on an attack-detection model, and implemented a strategy of the server port and address-hopping module.

Event-driven strategies detect suspicious activities and use a time function based on a specific attack event or security alarm to trigger an MTD strategy, which can improve system security, given an effective time function and attack behavior prediction. Yet, such a method depends on the security detection tools.

3.2.3. Hybrid-driven temporal MTD strategies

Hybrid-driven temporal MTD strategies are both time- and event-driven. Huang et al. [62] proposed a server diversification-based rotation mode, using servers with the same function and different structures to transfer the attack surface. It can be triggered by an attack event or based on a random or fixed time interval. Kampanakis et al. [63] proposed an SDN-based MTD attack surface obfuscation model. The network parameters are randomized in a fixed time period to trigger the transfer of the attack surface, and an analysis engine collects real-time security events and evaluates potential attacks by analyzing existing attacks. Zangeneh et al. [64] proposed an MTD mechanism based on hybrid time- and event-based mutation, using a competitive Markov decision process (CMDP) to model the time-driven MTD strategy, and historical alert data to model the event-driven MTD strategy. The combination of these strategies enables defenders to efficiently and cost-effectively transfer the attack surface. Zhuang et al. [65] changed the MTD strategy configuration in a random time interval and analyzed current network configuration and functional security requirements based on a logical task model. The MTD strategy was implemented adaptively according to vulnerability scan results and risk indicators such as IDS alarms. Li et al. [66] implemented a two-level MTD strategy for IP hopping. Based on attack events, the temporal MTD strategy was adjusted in a "fast decreasing, slow increasing" manner. The IP hopping period was reduced when high-frequency attacks were detected and increased when low-frequency attacks or no attack were detected.

Time-driven MTD strategies are more proactive than event-driven strategies. However, they can lead to high defense costs. Table 4 describes different temporal MTD strategies, along with their pros and cons. The optimal temporal MTD strategy can be determined by integrating time- and event-driven strategies to balance system availability and security.

Various MTD strategies have been proposed for security threats at the data, platform, runtime environment, network, and software layers. Attacker–defender interaction is essentially a confrontation between attack and MTD strategies. The key to the MTD strategy is to change the transfer time and select the transfer attribute value in a limited space to achieve maximum payoffs. Most MTD studies have focused on strategy design and formulation, while ignoring decision-making. There is a lack of quantitative analysis methods and theoretical decision-making frameworks for the research of MTD decision-making.

Simple stacking of MTD strategies will greatly increase overhead. Therefore, some key issues concern how to: (1) balance network performance and security; (2) compromise network defense, operating costs, and expectations based on attack strengths; and (3) achieve optimal defense performance and maximize defense payoffs under moderate security conditions.

4. Status of MTD game decision-making methods

MTD decision-making does not mean formulating a new MTD strategy, but rather selecting the optimal strategy by analyzing

Table 4
Temporal MTD strategies and their pros and cons.

Strategy	Description	Pros	Cons
Time-driven	Can be divided into uniform and random time-driven strategies. It is an active method.	Non-detection defense, high difficulty of attack	Difficult to accurately determine timing
Event-driven	Triggered by external information such as specific security alarms and security strategies. MTD strategy is implemented adaptively	Targeted strategy and low cost	Defenses lag behind attacks, potentially creating security risks
Hybrid	Combination of above strategies	More reasonable decision process of MTD strategies	Difficult to balance security and availability

Table 5
Classification of studies on MTD game decision-making.

Category	Studies	Objective	Difference	Scenarios
Spatial	Manadhata et al.; Zhu et al.; Sengupta et al.	Select optimal strategy for configuration properties of MTD system	It focuses on guiding the defender to adopt the MTD defense strategy when dealing with network attacks. It mainly selects the optimal MTD defense strategy in a certain network state.	Network attack and defense confrontation scenario with discrete space and time
Temporal	Zhuang et al.; Clark et al.; Anwar et al.	Select optimal temporal strategy for MTD system to transition from current to new state	It focuses on guiding the defender when to adopt the MTD defense strategy, and focuses on the timing of selecting the MTD defense strategy based on the network status switch, so as to ensure that the defense information collected by the attacker is invalid, thus increasing the difficulty of successful attack.	Network attack and defense confrontation scenario with discrete space and continuous time
Spatiotemporal	Gao et al.; Wu et al.; Yang et al.	Select spatial MTD strategy for adoption at different times or periods; includes dimensions of time and space	It focuses on guiding the defenders to adopt what MTD defense strategy when facing the attack and defense confrontation of high-frequency, high-intensity and fast-paced network, and blocking the attack from the perspectives of time and space.	Network attack and defense confrontation scenario with continuous space and time
Bounded rationality	Azab et al.; Colbaugh et al.; Yoon et al.	Select MTD strategy under assumption of bounded rationality	It is from the perspective of participants. Considering the differences in cognitive abilities of both sides of the network attack and defense, how to more effectively implement MTD time and space strategies, constantly improve the cognitive ability of defense in the process of network attack and defense, so as to select the most effective MTD time or space strategies.	Network attack and defense confrontation scenario with discrete space and time, discrete space and continuous time, or continuous space and time

the influence of different attack and MTD strategies on attack and defense actions. Therefore, the quality of decision-making is particularly important to realize effective defense. When the attacker and defender have comparable technical levels, the quality of MTD decision-making will directly affect network attack and defense. When there is a large technical gap, the player with a lower technical level can reverse a disadvantage through precise and scientific decision-making.

The decision-making problems of temporal, spatial, spatiotemporal, and bounded rationality MTD strategies are the basic components of MTD decision-making research (Table 5). Each has its merits. The key premise of MTD is to maximize payoffs by selecting temporal, spatial, and spatiotemporal MTD strategies in a limited transformation space, and an appropriate MTD strategy driven by bounded rationality should be selected. We summarize representative studies on decision-making of spatial, temporal, spatiotemporal, and bounded rationality strategies.

4.1. Decision-making of spatial MTD strategies

To superimpose different spatial MTD strategies will increase the overhead of a network information system. Hence it is necessary to select appropriate MTD strategies depending on the network status, so as to balance performance and security.

The typical MTD decision-making process models the attacker–defender interaction using game models. Depending on the knowledge of both players, decision-making can be based on complete or incomplete information.

4.1.1. Decision-making based on complete information

Decision-making based on complete information has been studied using game models such as the Stackelberg and Markov games.

To balance security and system availability, Manadhata et al. [67] proposed an optimal software-layer MTD strategy for a two-player stochastic game and an attack surface measurement method. The optimal static and dynamic MTD strategies were determined by nonlinear and dynamic programming, respectively, while ensuring the availability of the system. Asher et al. [68] proposed a platform-level MTD decision-making method based on a complete information, static game model. A defense revenue model was constructed, and the attacker's ability was evaluated based on the reconnaissance ability and the number of usable exploits. Experimental results showed that increasing the migration rate and diversity of the platform reduced the probability of successful attacks. Alexander et al. [69] proposed probability-based dynamic single-node and graph-based dynamic multi-node game models, proved the existence of an equilibrium in a game based on a single-node information set, and analytically derived the multi-node game. Maleki et al. [70,71] proposed a Markov game-based MTD decision-making method, and introduced the concept of security capacity to evaluate the effectiveness of MTD strategies. The method's effectiveness was verified by analyzing the security of single- and multiple-target hiding strategies. Zhou et al. [72] proposed a multi-vNIC intelligent mutation technology for cloud service platforms. A dynamic game model was used to model client-side DNS cache attacks and a multi-vNIC intelligent mutation defense. An adaptive optimal defense strategy was generated based on reinforcement learning. This method is only

applicable to a certain type of MTD decision-making problem, and thus lacks good generalization ability. Eldosouky et al. [73] modeled cryptographic and key randomization MTD in wireless networks as a non-zero-sum stochastic game and proved the existence of a Nash equilibrium. The number of consecutive changes in the system was defined as the defense cost, and a decision-making algorithm based on a double-matrix game equilibrium was proposed, which effectively increased defense payoffs while ensuring key randomization. Zhou et al. [74] proposed a cost-effective MTD method for DDoS attacks based on a Markov game model, and a cost-effective cleaning algorithm to determine the optimal strategy. Experimental evaluation of the trade-off between effectiveness and cost showed that the method could effectively defend against DDoS attacks. The team [75,76] proposed a cost-effective MTD strategy, obtained the optimal strategy based on a trilateral game cost-effective shuffling (TCS) algorithm, and experimentally showed that the method mitigated DDoS attacks with an acceptable overhead.

Clark et al. [77] proposed a game-theoretic approach to IP address randomization in decoy-based cyber defense, which modeled the interaction between an attacker and a network of decoy nodes as a Stackelberg game. Simulation results showed that time-based games always have a pure-strategy Nash equilibrium, whose value depends on detection probability and cost, while the fingerprinting game has a mixed-strategy equilibrium. Feng et al. [78] proposed an MTD decision-making model based on a Stackelberg game. A real-time state feedback structure was introduced, and the optimal MTD strategy was obtained through a value iteration algorithm. The existence of an optimal static defense strategy was proved. The MTD strategy space was modeled as a directed graph, and the effects of parameters such as node degree, graph size, and switching cost on the strategy were discussed. For the placement of intrusion detection systems in the cloud, Sengupta et al. [79] proposed an IDS detection surface moving method, modeling the interaction between a cloud administrator and attacker as a Stackelberg game, whose equilibrium indicated the optimal IDS placement strategy. The results of a large-scale cloud-based experiment demonstrated the method's effectiveness and scalability. Niu et al. [80] modeled the interaction between an LTI system controller and adversary for a false data injection attack as a Stackelberg game, and analyzed the optimal attack strategies under single- and multi-stage cases. The optimal detection threshold of the controller was obtained by solving the convex optimization problem, and experiments showed that the method was superior to an attack detector with fixed parameters. For adaptive complex attackers, Li et al. [81] proposed an MTD decision-making model based on the Markov Stackelberg game, using a relative value iteration algorithm to determine the optimal strategy. Experiments showed that the method is significantly better than the Bayesian Stackelberg game strategy and uniform random strategy. Assuming that the attacker and defender had the ability to learn strategies in the SDN cloud, and the defender had complete observability, Chowdhary et al. [82] modeled the interaction between the attacker and defender as a zero-sum dynamic Markov game with payoffs based on common vulnerability scoring system (CVSS) metrics, vulnerability exploitation difficulty, and attack and defense costs. An optimal IP hopping decision algorithm based on deep Q-learning was proposed. Empirical evaluation showed that the method can effectively resist adaptive attacks and obtain higher defense payoffs than random strategies.

4.1.2. Decision-making based on incomplete information

Decision-making based on incomplete information is mainly studied based on Bayesian Stackelberg, stochastic, and signaling game models.

Cai et al. [83] proposed a method based on the MP2R model and used a general incomplete information game model to evaluate the effectiveness of MTD. The game selection method of dynamic software, dynamic platform, and IP hopping MTD strategies was analyzed, and the conditions for the presence of different game equilibrium strategies were presented. Zhu et al. [84] proposed a zero-sum multi-stage game-theoretic model based on feedback learning. The attacker–defender interaction was modeled based on the system's real-time data and observation information, and they analyzed the MTD strategy cost of the defender, attack cost of the attacker, and game equilibrium strategy. To model the migration of PL-MTD and the attacker–defender interaction of zero-day vulnerabilities, Winterrose et al. [85] proposed a dynamic game model based on incomplete information and compared the performance of S-MTD and D-MTD against adaptive adversaries. Experiments showed that to maximize D-MTD is more appropriate for short-term attacks. The authors did not provide the game equilibrium calculation method, and only studied the problem from the attacker's perspective, without considering the influence of random noises. Feng et al. [86] introduced cost and signaling strategies for strategic rational attackers and proposed a Bayesian Stackelberg game model to solve the subgame perfect equilibrium. Vadlamudi et al. [87] proposed a Bayesian Stackelberg game-based MTD decision-making method for Web applications, which can help defenders identify key system vulnerabilities and attacker types. Sengupta et al. [88] modeled MTD in Web applications as a repeated Bayesian Stackelberg game, introduced the MTD strategy cost to defense payoffs, and obtained the optimal MTD strategy by solving the Stackelberg equilibrium. Vulnerabilities were obtained based on the national vulnerability database, and attack and defense payoffs based on CVSS metrics. Experiments verified the robustness of the method. For reactive jamming attacks in the remote state estimation of networked control systems, Ding et al. [89] combined defense deception and transmission scheduling, and introduced a partially observable Markov decision process. An MTD method based on an incomplete information stochastic game was proposed, and the existence of an optimal strategy was proved. Multi-agent reinforcement learning was used to solve the optimal equilibrium strategy, which greatly reduced the accuracy of the attacker's remote state estimation.

Zhang et al. [90] proposed an incomplete information stochastic game to protect Web applications at the platform layer. The attacker and the defender dynamically adjusted the attack and defense payoff based on the set of historical attack and defense strategies and the distribution of strategy selections. The Nash-Q algorithm was used to select the optimal MTD strategy. The method has only one attack strategy, and cannot deal with multiple types of attacks. Kandoussi et al. [91] proposed a comprehensive defense system integrating VM migration and network deception at the cloud platform layer, modeling the attacker and defender based on incomplete information stochastic game theory and an attack graph. The potential attack path was determined based on the attack loss and cost, and a priority strategy was provided for node updates based on a Bayesian game. Colbaugh et al. [92] integrated incomplete information dynamic games and machine learning to predict the MTD strategy for adversarial attacks, effectively limiting its predictability, and verified the method in experiments on a large cybersecurity dataset. Sengupta et al. [93] proposed an MTD model based on Bayesian Stackelberg Markov games, and used multi-agent reinforcement learning to obtain the optimal MTD strategy. Under the premise of an unknown migration rate and payoff, a Bayesian Strong Stackelberg Q-learning (BSS-Q) method was proposed, which outperformed existing methods in Web and cloud network scenarios. For targets in a power system that are

prone to attacks, such as the host, network, and management, Zhao et al. [94] proposed two low-cost optimum proactive defense strategies based on a Bayesian game, which can effectively predict attack behavior and provide a targeted defense strategy. The method's effectiveness was verified on 27 attack models. Sengupta et al. [95] proposed MTDeep, a Bayesian Stackelberg game-based MTD framework for adversarial attacks in deep neural network information systems such as image classification. Test results on MNIST, Fashion-MNIST, and ImageNet showed that the method effectively improved image classification accuracy and somewhat reduced the rate of incorrect classification.

Sun et al. [96] proposed an optimal MTD decision-making method based on a signaling game, constructing the MTD strategy based on an induction signal. An equilibrium solution algorithm was proposed to obtain the optimal induction signal strategy. Considering the unavoidable misdetection defects of the defense detection system, a method to quantify the payoffs of the attack and defense strategy was proposed, and a refined Bayesian equilibrium algorithm and prior belief correction algorithm were presented. The method was verified by an example [97]. Chen et al. [98] proposed a method based on a signaling game to select the optimal PL-MTD strategy when the prior probability of the attacker type was known. Jiang et al. [99] proposed an optimal MTD strategy selection method based on a signaling game, where the MTD equilibrium strategy was solved based on a refined Bayesian equilibrium. The authors later proposed an optimal MTD strategy selection method based on a multi-stage Markov signaling game [100]. The distortion of the posterior probability update due to strategy switching was solved using a logistic map, and the optimal strategy selection algorithm was given. Chen et al. [101] proposed an optimal defense strategy selection method for spear-phishing attacks in industrial control systems based on a multi-stage signaling game, while considering defense capability and strategy cost. The Nash equilibrium of the model was analyzed based on numerical value payoffs. An example showed that the method effectively improved the efficiency of defense decision-making. Aydeger et al. [102] proposed a signaling game-based MTD strategy selection method for stealth link flooding attacks, and designed attack and defense strategies and payoffs. The best attack and defense responses and actions were selected based on an attacker–defender belief function. Results in the Mininet experimental environment in the SDN simulation tool showed that the method was significantly better than uniform time-driven random route mutation strategies. Rahman et al. [103,104] proposed a fingerprinting hopping method based on a signaling game for remote operating system fingerprinting attacks, and introduced a fingerprint confusion strategy. Results of pooling and separating equilibrium were obtained by analyzing the interaction between the fingerprint reader and the target system. The method reduced the defense overhead by 60%. While ensuring the communication overhead, it could effectively defend against fingerprinting attacks and reduce their probability of success (see Table 6).

4.2. Decision-making of temporal MTD strategies

A defender must determine the optimal temporal strategy to transfer to a new state, thereby destroying the attack information, making the information or progress of the attacker invalid, and ensuring high defense effectiveness and a low implementation cost. MTD aims to eliminate the asymmetric time advantage of the attacker. Factors such as the time interval between implementations of the MTD strategy, and the time required for MTD strategy implementation, attack implementation, and a successful attack, influence the effectiveness of MTD strategies.

The cost and cycle of the attacker–defender interaction change with the system configuration and attack–defense process. Successful implementation and payoff maximization depend on the time of the MTD strategy. MTD decision-making methods have been proposed in different cyberattack-defense scenarios, yet most studies focus on the sequential selection of MTD strategies, while simplifying or ignoring temporal MTD strategies. Current spatial MTD strategy selection methods cannot be simply and directly applied to temporal MTD strategy selection. Therefore, MTD research comprehensively considers temporal MTD strategies and attack time strategies, balances between system security and availability, and selects the optimal temporal MTD strategy based on the attacker–defender interaction.

Zhuang et al. [105] showed that, by defining the detection and attack surfaces based on spatial and temporal MTD strategies, the dynamic characteristics of MTD could be more effectively modeled, but provided no specific method. Clark et al. [106] proposed a decoy-based MTD method by which a computer network introduces a large number of virtual decoy nodes to prevent the location and targeting of real nodes. The node type was determined based on its response time to queries, and closed-form solutions for the expected time of detection were derived. Anwar et al. [107,108] proposed a VM migration timing strategy for a multi-tenant cloud based on game theory, presented the Nash equilibrium, and validated the model through numerical experiments. Navas [109] proposed an MTD timing strategy based on authenticated state synchronization (Auth-SYNC) to improve the resilience of the constrained Internet of Things (IoT), where temporal MTD strategies could be triggered based on the real-time clock or external events. Chen et al. [110] performed platform migration based on intrusion detection events and used a uniform time-driven MTD strategy to avoid missed detection, thereby achieving PL-MTD strategy migration with a hybrid-driven MTD. Ma et al. [111] proposed a uniform time-driven sequential platform migration strategy, uniform time-driven random platform migration strategy, and random time-driven random platform migration strategy for heterogeneous DMZ platforms. The optimal time strategy under different platform exposure times was determined by comparing the attack detection probability and defense payoff of the three strategies. Li et al. [112] proposed the optimal timing of MTD based on the Bayesian Stackelberg game, abstracted the MTD decision-making process into a general semi-Markov decision process, and obtained the optimal MTD strategy through value iteration.

Dijk et al. [113] proposed the FlipIt game for APTs, whose schematic diagram (Fig. 9) shows the switching of control of resources between the attacker and defender over time, where blue and red circles denote the defender and attacker, respectively. The defender has control at time $t = 0$. Different from most game models, the FlipIt game includes the defender, attacker, and resource, and players are allowed to control the resource at any time, at a certain cost. However, the actual control of the resource is not revealed before the players' actions. Thus, stealth is the game's primary feature. Each player seeks to maximize the control time of the resource while minimizing the cost. In the cyberattacker–defender interaction, both parties compete to control the resource (attack surface) to maximize their payoffs.

The FlipIt game has been widely used in security scenarios including targeted attack modeling, encryption key updates, password reset policies, and cloud auditing. Bowers et al. [114] studied the application of the FlipIt game in practical scenarios such as password reset policies, key rotation, VM refresh, and cloud auditing. Nochenson et al. [115] conducted a behavioral investigation matching human participants with computerized opponents in several rounds of the FlipIt game. Lee et al. [116] introduced a cybernetic approach to model competing malware

Table 6
Summary of decision-making of spatial MTD strategies methods.

Decision methods	Application scenario	MTD strategy	Attack technique	Game type	Advantage	Weakness
Decision-making based on complete information	Software system [67], cloud service platforms [72,79,82], wireless network [73], etc	REL-MTD [67], PL-MTD [68], etc.	DNS cache attack [72], Incorrect data injection attack [80], DDos attack [74], etc,	Stochastic game [67,73], Stackelberg game [77,78], Markov game [70,71], etc.	The network threat defense mechanism is more robust to ensure normal services for users.	The scenario generalization is weak, resulting in poor practicability of decision method and limitations of applicable scenarios.
Decision-making based on incomplete information	Web applications [87,88], cloud computing [91], power system [94], etc	REL-MTD [83], PL-MTD [91,98], NL-MTD [89], etc	Spear phishing attacks [101], Stealth link flooding attack [102], fingerprint identification attack [103,104], etc	Bayes Stackelberg game [86–88], signal game [96,97], etc	It effectively describes the characteristics of multi-stage, multi-state and incomplete information of network attack and defense	The attack type is relatively simple.

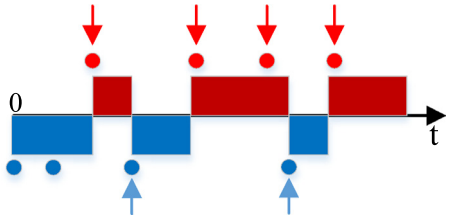

Fig. 9. The schematic diagram of FlipIt game. . (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

in the FlipIt game. Pawlick et al. [117] combined the FlipIt game and a signaling game to describe the interaction between an attacker, defender, and cloud-linked devices. Zhang et al. [118] investigated a game between a defender and a stealth attacker, which showed that a periodic defense strategy was the best response to non-adaptive adversaries. Laszka et al. [119] proposed the FlipThem game, a FlipIt game in which the attacker tries to destroy one or more of multiple resources. Feng et al. [120] introduced insider threats and stealth attacks in the FlipIt game, and studied a three-player leader–follower game model under asymmetric delayed feedback information. The sub-game perfect equilibria of the three-player game were obtained based on a previous study [121], which provided a reference for defense against advanced attacks and insider threats. The FlipIt game has recently been adopted to research MTD. Jones et al. [122] allowed system deformation by the defender so as to destroy the knowledge obtained by the attacker, and extended the FlipIt game to MTD, but did not use it for the MTD timing process.

The decision process of temporal MTD strategies is based on time- and event-driven MTD. A time-driven MTD strategy increases the difficulty of attack by randomly changing network elements, while an event-driven strategy determines defense timing and strategy based on network status and attack detection. The timeliness of a temporal MTD strategy greatly affects its effectiveness. Timeliness can affect system availability, and poor timeliness can lead to the failure of an MTD strategy. Therefore, MTD timing strategies have changed from a fixed to a random period. Although random-period MTD can make it somewhat more difficult for an attacker to obtain the MTD timing strategy, it is still difficult to effectively balance defense effectiveness and performance.

4.3. Decision-making of spatiotemporal MTD strategies

Decision-making of spatiotemporal MTD strategies has two dimensions, and is particularly important in the current high-frequency and fast-paced attack–defense process. Most studies focus on spatial MTD strategies, and decision models have been proposed based on various game models, mostly based on discrete-time multi-stage dynamic attacker–defender interactions. In actual cyberattack and defense, the attacker and defender often take actions with high frequency and intensity, i.e., with dynamic characteristics, and their decision-making needs cannot be met by the traditional multi-stage dynamic game. A mathematical model enabling the analysis of the dynamic attacker–defender interaction is needed. The mainstream method is based on differential games, and has not been applied to MTD.

A differential game is a continuous-time game model that analyzes non-cooperative conflict. It can analyze strategies with dynamic spatiotemporal changes and make continuous control decisions, and has been widely applied in missile interception and other fields. In network security, it has been studied in the fields of cognitive radio, cognitive networks, fog computing, and massive machine-type communication. Hao et al. [123] proposed a differential game approach to mitigate primary user emulation (PUE) attacks in cognitive radio networks. The Nash equilibrium was derived based on the capability of the attacker, sensing (attacking) capability of the secondary user, and power constraints. The method improved the availability of the cognitive channel and minimized the loss of PUE attacks. Feng et al. [124] modeled the objective function attack (OFA) attack–defense process based on a differential game, with a threat factor to measure the security level. The optimal defense strategy was obtained by proving the existence of the saddle point of the proposed model. An et al. [125] proposed an optimal intrusion response strategy in fog computing based on a differential game. By analyzing the attack intrusion path, the optimal attack and defense strategies were deduced, which effectively ensured the security of the fog computing cluster. Gao et al. [126] proposed a multi-attacker multi-defender game model based on a differential game for massive machine-type communication networks. The Hamilton function was introduced to solve the optimal strategy, and numerical simulation experiments were conducted.

Gao et al. [127] proposed a spatiotemporal interaction model for multi-attackers and multi-defenders based on a differential game. The saddle point equilibrium strategy was solved based on the Hamilton optimal control method, and a paralysis threshold was introduced to analyze the evolution of the attack and defense strategies. Wu et al. [128] proposed a zero-sum differential game model for attack–defense strategy analysis in IoT

networks. A Gauss–Seidel-like implicit finite-difference method was used to discretize continuous-time differential equations and iteratively solve for the optimal defense strategy. Huang et al. [129] proposed a network defense decision-making method based on a Markov differential game, depicting the randomness of network state transition based on Markov decision process, and the dynamic real-time nature of network defense decisions based on a differential game. Multi-stage equilibrium strategies were obtained based on dynamic programming. Mi et al. [130] proposed an optimal network defense strategy selection method based on a stochastic differential game, with Gaussian noise in the attack–defense process to introduce random interference. The Hamilton–Jacobi–Bellman (HJB) equation was used to obtain the equilibrium strategy.

Yang [131] et al. proposed a differential game-based repair strategy against lateral-movement APT, and established a node-level evolution model of the expected state. The Nash equilibrium was solved based on randomly generated attack and repair strategies. Wang et al. [132] applied differential game theory to analyze the antagonistic dynamics between an attacker and defender, and studied the black- and white-box game formulations. The evolution rules of the two games were analyzed through numerical simulations. He et al. [133] proposed a differential game-based IP hopping model for the Internet of Vehicles, in which a random IP address was generated based on a hash value and random numbers. The method adaptively adjusted a road side unit's IP hopping frequency according to the attack frequency, and effectively maximized the defense payoff. Sun et al. [134] proposed an optimal MTD strategy based on a differential game, constructed a network state evolution model, designed an open-loop Nash equilibrium algorithm, and verified the effectiveness of the method through numerical simulations.

4.4. Decision-making of bounded rationality MTD strategies

Neither the attacker nor defender is completely rational, and there are many constraints on their rationality. Hence research on bounded rationality MTD strategies is of great practical significance. Past studies have assumed complete rationality [135]. While considering the opponent's decision, a player seeks to maximize its payoff. The assumption of complete rationality is associated with many conditions that are difficult to achieve, such as perfect rational consciousness, recognition and judgment ability, memory and calculation ability, and analytical and reasoning ability. It is also assumed that every player knows how to maximize its payoff. If any of these conditions is not met, it is not complete rationality. Neither the attacker nor defender can fully grasp all the strategies and their payoffs. This leads to distortion of analysis and modeling results, affecting the applicability and practicability of MTD strategies.

The decision-making of bounded rationality MTD strategies is based either on evolutionary games or reinforcement learning.

4.4.1. Evolutionary game-based bounded rationality MTD decision-making

The evolutionary game is based on the principle of imperfect rationality, and through strategy revision and improvement, it gradually converges to the evolutionary stable strategy (ESS), thereby improving the reliability of decision-making. As a bounded rationality game, it models the behavior of a game player as an evolutionary process with adaptive learning. It has gained wide application in network security scenarios such as wireless sensor networks, cloud storage data center networks, smart grids, the IoT, and crowd-sensing networks.

Arora et al. [136] proposed an adaptive selection of cryptographic protocols in wireless sensor networks using evolutionary game theory, in which sensor nodes could adaptively adjust their defense strategies according to the attacker, and which had good robustness. Du et al. [137] proposed an incomplete information evolutionary game model based on enhanced cooperation for the strategic selection of misused detections in wireless sensor networks, where incomplete information was transformed by a Bayesian formula. The attack–defense process was modeled by the replicator dynamic equation, and a description of the evolutionary trajectory of the players over time was obtained, which provided moderate security and proactive defense in the form of support decisions. Abass et al. [138] carried out an evolutionary game theoretic analysis of APTs against cloud storage. APT games of a single storage device and multiple storage devices were modeled, and the influences of attack cycle, attack duration, attack cost, and defense cost on defensive effectiveness were analyzed through numerical simulations. Boudko et al. [139] proposed an evolutionary game model to ensure the confidentiality of an advanced metering infrastructure (AMI) in an intelligent IoT, which introduced learning capabilities in the behavior of both attackers and AMI nodes. The defender explored the space of strategies and selected the optimal set of solutions. Yang et al. [140] proposed a multi-stage asymmetric information attack and defense model based on evolutionary game theory, analyzed the attacker–defender interaction in different stages, and quantified the payoffs and costs of attack and defense strategies. The method was applied to a smart home, camera, and transportation. Ruan et al. [141] proposed an evolutionary game-based DoS-resistant authentication protocol parameter optimization model, which effectively solved the multi-level μ TESLA protocol buffer size selection problem and could effectively predict user behavior while reducing the defense cost. Most of the above studies were based on deterministic evolution strategies such as the replicator dynamic equation, which do not accurately describe the stochastic evolution characteristics of attack and defense strategies.

Azab et al. [142] proposed a smart MTD elastic system for Linux containers, which modeled the attacker-target container interaction as a game of a predator searching for prey. A host-based behavior-monitoring system seamlessly monitored containers for indications of intrusions and attacks, and run-time live-migration of Linux-containers was used to avoid attacks (predator) and failures. The effectiveness of the method was verified in the ACIS local cloud. Wang et al. [143] proposed a PL-MTD strategy selection method based on an evolutionary game, and analyzed the strategy evolution mechanism under the assumption of bounded rationality. The ESS was solved based on the replicator dynamic equation. For a Web server and host node, payoffs of attack and defense evolutionary strategies were experimentally compared. Colbaugh et al. [144,145] proposed an evolutionary game model based on incomplete attack–defense information for the problem of the same distribution of training and test data in machine learning. The unpredictability of the system was increased through real-time changing defense strategies. The effectiveness of the method was verified through examples of spam email filtering and network intrusion prevention. Bi et al. [146] proposed a multi-stage bounded rationality MTD strategy selection method combining evolutionary and signaling games. Multi-stage equilibrium strategies were obtained based on the replicator dynamic equation. Numerical simulations were carried out to obtain the strategy evolution in different stages. Shi et al. [147] proposed a three-party evolutionary game model of an array honeypot, including defenders, attackers, and legitimate users. The Jacobian matrix and equilibrium points were obtained by calculating the replicator dynamic, the eigenvalue matrix was obtained, and the ESS of array honeypot dynamic defense was obtained. Wang et al. [148] proposed a PL-MTD model based on a Markov evolutionary game for the selection of bounded rationality PL-MTD strategies, and verified the results through numerical simulation.

Table 7
Summary of decision-making of bounded rationality MTD strategies methods.

Decision methods	Application scenario	MTD strategy	Attack technique	Game type	Advantage	Weakness
Evolutionary game-based bounded rationality MTD decision-making	Wireless sensor [136,137], cloud storage environment [138], Internet of things [139], etc	NL-MTD [136,137], PL-MTD [143,148], etc.	APT attack [138], Dos attack [141], etc,	Evolutionary game [136], evolutionary search game [142], evolutionary signal game [146], etc.	It can effectively describe the evolution trajectory of equilibrium strategy.	Due to the lack of accuracy in payoffs calculation, it is impossible to describe the stochastic evolution characteristics of strategy effectively.
Reinforcement learning-based bounded rationality MTD decision-making	In-vehicle software-defined networking [155], Image classification system [149,150], etc	NL-MTD [151], etc	DDoS attack [151], Heartbleed attack [152], etc	Reinforcement learning [52,151], Deep reinforcement learning [155,156], etc	The strategy solving process is more adaptive and intelligent.	The intelligence characteristics of the attacker's decision cannot be fully considered.

4.4.2. Reinforcement learning-based bounded rationality MTD decision-making

Sengupta [149,150] proposed directions of MTD research in the field of artificial intelligence and security. MTD strategy can be applied to solve the security problems of artificial intelligence algorithms, such as image classification systems, and to enhance the security of multi-agent systems, such as reinforcement learning and deep reinforcement learning. Bounded rationality MTD strategy selection based on reinforcement learning is a typical application. Gao et al. [151] proposed an adaptive MTD strategy against DDoS attacks based on reinforcement learning. The payoffs were based on system security, performance, and defense efficiency, and the iterative attack and defense strategies were optimized based on Q-learning. The terminal information hopping strategy adaptively changed based on the environment to balance system performance and security. Zhu et al. [152] proposed an adaptive cyber defense method against the Heartbleed attack based on reinforcement learning. Adaptive iterative reinforcement learning algorithms were proposed for the cases of limited and continuous detection of the attacker. The convergence of the algorithm was analyzed, and its effectiveness was verified via numerical simulations. Tozer et al. [153] proposed a strategy selection method based on multi-objective reinforcement learning to minimize the attack surface and maximize the diversity of system configurations. The method's performance was compared with that of three other algorithms. Hu et al. [154] used Bayesian attack graphs to model the interactions between a network and a multi-stage attacker, and the defense problem was modeled as a partially observable Markov decision process. Thompson sampling was used to estimate transition probabilities, and reinforcement learning to choose optimal defense actions. The algorithm's performance was verified via numerical simulations based on real-world attacks. Yoon et al. [155] proposed a network slicing technology with multi-agent deep reinforcement learning to implement IP hopping for in-vehicle software-defined networking. The method determined the link bandwidth allocation and IP hopping frequency. Experiments showed that the method ensured the availability of services while minimizing system security vulnerabilities and defense costs. Eghtesad et al. [156] proposed an MTD strategy selection model based on a multi-agent partially observable Markov decision process, and proposed a multi-agent reinforcement learning framework based on deep Q-learning and the double oracle algorithm. The mixed strategy Nash equilibrium was solved to obtain the optimal MTD strategy. The payoff model was oversimplified, the attacker only considered control and sabotage behavior, and the defender only considered confidentiality and availability (see Table 7).

4.5. Shortcomings of current research

Limited by the game model's requirement of prior knowledge, game analysis methods need to master all or part of the information of offensive and defensive strategy, payoff calculation parameters and network system state in advance. If the above information cannot be mastered in advance, for example, in the face of zero-day security vulnerabilities, unknown attack (defense) strategies and network emergencies, the game analysis method can only rely on historical data and expert experience to make subjective assumptions, and the accuracy of the analysis cannot be guaranteed, which will weaken or even destroy the effectiveness of MTD game decisions.

Abstract modeling steps of MTD game decision method are complex, and currently there is a lack of high-quality generalized and automated modeling mechanisms and tools, and the quality and effect mainly depend on the ability and experience of researchers. In the face of heterogeneous complex network, attack and defense scenario of special alienated network, and large-scale attack and defense confrontation, the implementation speed and decision accuracy of game decision analysis are not enough to fully meet the realistic demand.

Most verification experiment of MTD game decision method are completed by simulation, which is less persuasive than real cases in the real world. And the comparative of different models and methods is weak, which is not conducive to analyzing their performance, function and innovation value. The main reasons are as follows:

(1) The network attack–defense experiments are often destructive and will affect network structure, network equipment or network service quality. And the uncontrollable risk of confrontation is high, the experimental cost is large. On the other hand, real case experiments generally require specific data such as attack behavior, defense measures, security losses, etc. It is difficult to collect data because the data is usually sensitivity, privacy and even confidentiality.

(2) The simulation experiment has the advantages of fast speed, convenient operation and low cost. It can quickly realize large-scale heterogeneous network experimental environment and multi-scenario attack–defense simulation, and conveniently collect experimental data for further analysis and research.

(3) When comparing the different models and methods, the experimental environment, test data, and comparison methods are all affected by many factors. For example, the sets of attack and defensive strategies, quantification methods of game payoffs, and experimental network structures in dissimilar models generally are completely different. These differences make it difficult to compare and analyze in the same instance.

5. Conclusion

5.1. Insights and lessons learned

Our analysis shows limitations in studies on MTD strategy selection based on game theory in terms of temporal, spatial, spatiotemporal, and bounded rationality MTD strategy selection:

(1) Complete information spatial MTD strategy selection models do not effectively model the dynamic stochastic characteristics of the attacker–defender interaction, and the spatial strategy payoff quantification generalizes poorly.

Most such studies are based on models such as stochastic, and Stackelberg games, which cannot effectively describe the dynamic and continuous characteristics of attacker–defender interaction. Single-stage models are usually based on matrix games, which cannot accurately describe the characteristics of single-stage attacker–defender interaction. Moreover, the defense cost is not considered, and is mostly based on historical data and expert experience. Hence there is a deviation between the payoff function and the actual payoff, causing poor generalization ability and an inability to ensure accurate decision results. It is not suitable for optimal spatial MTD strategy selection under different attacker–defender interactions;

(2) Incomplete information spatial MTD strategy selection models rely heavily on the prior probability, and the transfer probability is difficult to obtain and can easily fail.

Most studies are based on the probability distribution of an incomplete information Bayesian game model, which is converted to a complete information model using the classic Harsanyi transformation. The prior probability is based on the Bayesian model, which must meet the consistency assumption, which does not accord with the actual situation. Therefore, with the continuous progress of the attacker–defender interaction, the prior probability distribution of possible strategies under the condition of incomplete information will fail, which greatly reduces the effectiveness of strategy selection;

(3) The current temporal MTD game model has difficulty constructing the MTD strategy selection model and balancing the QoS and defense payoff.

There is a lack of a standard theoretical framework for temporal MTD strategy selection, which is a key factor in MTD effectiveness. Studies are mainly time-, event-, and hybrid-driven, and few incorporate game theory. Therefore, it is meaningful to integrate and systematize the temporal MTD decision process and build a solid game theory foundation;

(4) Existing spatiotemporal MTD game models cannot effectively describe the problems of hidden space–time and high-frequency confrontation.

Studies do not fully consider the adaptive adversarial ability of the attacker, and cannot capture the characteristics of stealth attacker–defender interaction. Although dynamic game models have been constructed, such as the Stackelberg, signaling, and Markov games, they are still essentially discrete multi-stage games, and cannot describe the continuous attacker–defender interaction. Spatiotemporal MTD strategy selection methods do not integrate decision-making of temporal and spatial elements. Hence their effectiveness and accuracy are poor;

(5) Existing MTD strategy selection models assume complete rationality, which is difficult to satisfy during an actual attacker–defender interaction, and whose limitations reduce the significance of research results. Most models are based on the traditional dynamic game model, which cannot accurately describe the set of attack and defense strategies and the dynamic change of the system runtime environment. Moreover, the current MTD decision-making model lacks a learning mechanism that fully describes the dynamic learning process and learning effects of attack and defense strategies, so the strategy evolution of the current MTD decision-making model has certain limitations.

(6) Most of the existing MTD game decision-making methods use the stochastic network model to study the real network, which are not suitable for large-scale heterogeneous complex networks.

Network information system has become a key social infrastructure, which is generally a large-scale and heterogeneous complex network. The basic assumptions of random networks are not in accordance with the actual situation. The Internet, World Wide Web, power grid, and the transportation network in the real world are not actually random, but are complex networks with scale-free, small world, node heterogeneity and so on characteristics. However, the existing game decision-making methods use the random network model for abstract description of large networks, assuming that the network nodes are homogeneous and the network links are random uniform distribution. On this basis, the attack–defense game analysis and decision algorithm design are realized. Because the influence of network structure characteristics is ignored, the existing methods are not suitable for scale-free networks, small-world networks and other types of complex networks, and the decision-making efficiency is limited.

Research has extended to bounded rationality MTD strategy selection, yet research on smart decision-making is still in the early stage. Reinforcement learning can be introduced on the basis of evolutionary games to build an intelligent evolutionary game system, which can be applied to temporal, spatial, and spatiotemporal MTD strategy selection. The temporal MTD strategy can integrate the FlipIt and evolutionary games, and can be applied to key switching and other quantum communication networks. The spatial MTD strategy can be based on integration of scholastic and evolutionary games, and applied to IP, 5G, and satellite communication networks. The spatiotemporal MTD strategy can be based on integration of differential and evolutionary games, and applied to high dynamic, real-time communication networks.

It is particularly feasible to integrate reinforcement learning with evolutionary games. An evolutionary game overcomes the limitation of reinforcement learning as a single-agent learning method and can incorporate multiple attackers and defenders, to construct three-, four-, and even multi-party methods. Reinforcement learning provides a Markov decision process, to extend the application scenario to multiple stages. The game payoff matrix restricts the implementation of MTD strategy selection models. Common fine-grained attack frameworks such as ATT&CK provide a good idea for payoff quantification. Moreover, the attack and defense knowledge plane of MTD can be established based on the knowledge graph, and the probability distribution derivation paradigm of risk transmission chain can be given on the basis of analyzing the threat transmission path. Through the design of the payoff function, it breaks through the problems of difficult design and poor generality of traditional evolutionary game payoff matrix. Then, the intelligent evolutionary learning mechanism is designed to solve the equilibrium strategy based on reinforcement learning, and the decision-making ability of MTD is enhanced through the balance of "exploration and utilization", which lays the foundation for the active suppression of unknown risks, so as to improve the pertinence and intelligence level of MTD decision-making.

With a rapidly increasing network structure and scale, it is urgent to study group MTD decisions in large-scale complex networks. The dynamic evolutionary game can be integrated with complex network control dynamics in decision-making schemes based on algorithms such as self-improvement learning and group dynamics. By exploring MTD strategy selection methods in uncertain and complex network environments, simulation platforms can be built for military, financial, and medical systems, and theoretical verification and practical implementation can be carried out on high-performance computing platforms.

5.2. Future research directions

MTD is a revolutionary technology against cyberattacks, and the focus of next-generation cybersecurity defense. Despite the achievements of existing research, problems remain.

(1) The timeliness of a temporal MTD strategy affects its effectiveness. While time- and event-driven strategies can somewhat increase the difficulty for the attacker to guess the strategy, it is still difficult to balance effectiveness and performance. Therefore, how to dynamically adjust them to minimize overhead and ensure effectiveness remains an important problem.

(2) As attack methods become more concealed and intelligent, it is difficult to effectively describe unknown attacks represented by APTs. There is currently no effective method to measure the hidden elements in the attacker–defender interaction. The accuracy of the description must be improved so as ensure the pertinence of MTD strategy selection [157]. Therefore, it is necessary to accurately model unknown attacks.

(3) The MTD decision process ensures the continuous, controllable, and manageable implementation of the MTD strategy. However, with the structural expansion of the defense system, there will be decision failures due to strategy conflicts [158]. Therefore, it is a challenge to choose an effective algorithm to ensure accurate and effective MTD decision results.

(4) To large-scale complex network attack and defense scenarios, because the existing research lacks considering the characteristics of complex network structure such as small world, scale-free, high aggregation, etc., the game analysis is inaccurate and the effectiveness of defense decision-making is weakened. Therefore, how to construct the MTD game model and decision algorithm for complex networks is an urgent problem.

In the future, comprehensively considering the characteristics of complex network structure and network attack–defense behavior, we can combine complex network theory with evolutionary game and differential game methods to study defense decision-making [159]. Based on the network evolution game model, the evolution analysis of complex network security state can be achieved. According to the analysis of attack–defense confrontation and the change of network security state, then the attack and defense strategy description and income calculation are realized, and finally we can design better game equilibrium solution and decision algorithm.

MTD aims to break the asymmetry between attackers and defenders via innovative defense methods, novel strategy selection mechanisms, and optimized implementation. The continuous emergence of novel technologies and integration of different disciplines provide new development directions and ideas for MTD strategy selection. Through the integration of deep learning, reinforcement learning, knowledge graph, complex network and other theories and technologies, it is expected to improve the automation degree of MTD game decision, decision completion speed and effectiveness of decision results. With continuous progress in MTD research, it will continue to play an important role in cybersecurity.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

We thank all the reviewers for their valuable comments. This work was supported by the National Key Research and Development Program of China (Grant No. 2017YFB0801904).

References

[1] J. Tan, H. Zhang, C. Lei, et al., Research progress on moving target defense for SDN, Chin. J. Netw. Inf. Secur. 4 (7) (2018) 1–12.
[2] The ENISA Threat Landscape 2022 (ETL) Report, https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape.
[3] M. Zhu, A.H. Anwar, Z. Wan, et al., Game-theoretic and machine learning-based approaches for defensive deception: A survey, 2021, arXiv preprint arXiv:2101.10121.
[4] L. Zhang, V.L.L. Thing, Three decades of deception techniques in active cyber defense-retrospect and outlook, Comput. Secur. 106 (2021) 102288.
[5] J. Pawlick, E. Colbert, Q. Zhu, A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy, ACM Comput. Surv. 52 (4) (2019) 1–28.
[6] J.H. Cho, D.P. Sharma, H. Alavizadeh, et al., Toward proactive, adaptive defense: A survey on moving target defense, IEEE Commun. Surv. Tutor. 22 (1) (2020) 709–745.
[7] G. Cai, B. Wang, W. Hu, et al., Moving target defense: state of the art and characteristics, Front. Inf. Technol. Electron. Eng. 17 (11) (2016) 1122–1153.
[8] S. Sengupta, A. Chowdhary, A. Sabur, et al., A survey of moving target defenses for network security, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1909–1941.
[9] Rui Zhuang, Scott A. DeLoach, Xinming Ou, Towards a theory of moving target defense, in: Moving Target Defense, 2014.
[10] G. Cai, B. Wang, T. Wang, et al., Research and development of moving target defense technology, J. Comput. Res. Dev. 53 (5) (2016) 968–987.
[11] S. Forrest, A. Somayaji, D. Ackley, Building diverse computer systems, in: Proceedings of the Sixth Workshop on Hot Topics in Operating Systems, IEEE, 1997, pp. 67–72.
[12] Networking and Information Technology Research and Development, National Cyber Leap Year Summit 2009: Co-Chairs' Report, 2009, Online report.
[13] Cybersecurity Game-Change Research & Development Recommendations. NITRD CSIA IWG[EB/OL].
[14] Report on Implementing the Federal Cybersecurity Research and Development Strategy.
[15] W. Zhang, Game Theory and Information Economics, 2004.
[16] X. Liang, Y. Xiao, Game theory for network security, IEEE Commun. Surv. Tutor. 15 (1) (2012) 472–486.
[17] S. Yang, Y. Zhang, C. Wu, Attack-defense quantification based on game-theory, 2019, arXiv preprint arXiv:1902.10439.
[18] B.C. Ward, S.R. Gomez, R. Skowyra, et al., Survey of Cyber Moving Targets Second Edition, MIT Lincoln Laboratory, Lexington United States, 2018.
[19] H. Marco-Gisbert, I. Ripoll Ripoll, Address space layout randomization next generation, Appl. Sci. 9 (14) (2019) 2928.
[20] C. Kil, J. Jun, C. Bookholt, et al., Address space layout permutation (ASLP): Towards fine-grained randomization of commodity software, in: 2006 22nd Annual Computer Security Applications Conference (ACSAC'06), IEEE, 2006, pp. 339–348.
[21] V. Iyer, A. Kanitkar, P. Dasgupta, et al., Preventing overflow attacks by memory randomization, in: 2010 IEEE 21st International Symposium on Software Reliability Engineering, IEEE, 2010, pp. 339–347.
[22] A. Tang, S. Sethumadhavan, S. Stolfo, Heisenbyte: Thwarting memory disclosure attacks using destructive code reads, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 256–267.
[23] G. Christou, G. Vasiliadis, V. Papaefstathiou, et al., On architectural support for instruction set randomization, ACM Trans. Archit. Code Optim. (TACO) 17 (4) (2020) 1–26.
[24] X. Jiang, H.J. Wangz, D. Xu, et al., Randsys: Thwarting code injection attacks with system service interface randomization, in: 2007 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007), IEEE, 2007, pp. 209–218.
[25] E.G. Barrantes, D.H. Ackley, S. Forrest, et al., Randomized instruction set emulation, ACM Trans. Inf. Syst. Secur. 8 (1) (2005) 3–40.
[26] Z. Liang, B. Liang, L. Li, et al., Against code injection with system call randomization, in: 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, Vol. 1, IEEE, 2009, pp. 584–587.

[27] C. Zhang, T. Wei, Z. Chen, et al., Practical control flow integrity and randomization for binary executables, in: 2013 IEEE Symposium on Security and Privacy, IEEE, 2013, pp. 559–573.
[28] A.J. O'Donnell, H. Sethu, On achieving software diversity for improved network security using distributed coloring algorithms, in: Proceedings of the 11th ACM Conference on Computer and Communications Security, 2004, pp. 121–131.
[29] C. Le Goues, T.V. Nguyen, S. Forrest, et al., Genprog: A generic method for automatic software repair, IEEE Trans. Softw. Eng. 38 (1) (2011) 54–72.
[30] P.E. Ammann, J.C. Knight, Data diversity: An approach to software fault tolerance, IEEE Trans. Comput. 37 (4) (1988) 418–425.
[31] A. Nguyen-Tuong, D. Evans, J.C. Knight, et al., Security through redundant data diversity, in: 2008 IEEE International Conference on Dependable Systems and Networks with FTCS and DCC, DSN, IEEE, 2008, pp. 187–196.
[32] C. Cadar, P. Akritidis, M. Costa, et al., Data Randomization, Technical Report TR-2008-120, Microsoft Research, 2008, Cited on, 2008.
[33] E. Pattuk, M. Kantarcioglu, Z. Lin, et al., Preventing cryptographic key leakage in cloud virtual machines, in: 23rd {USENIX} Security Symposium ({USENIX} Security 14), 2014, pp. 703–718.
[34] Y. Zhang, M.K. Reiter, Düppel: Retrofitting commodity operating systems to mitigate cache side channels in the cloud, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, 2013, pp. 827–838.
[35] M. Thompson, N. Evans, V. Kisekka, Multiple OS rotational environment an implemented moving target defense, in: 2014 7th International Symposium on Resilient Control Systems, ISRCS, IEEE, 2014, pp. 1–6.
[36] M. Thompson, M. Mendolla, M. Muggler, et al., Dynamic application rotation environment for moving target defense, in: 2016 Resilience Week, RWS, IEEE, 2016, pp. 17–26.
[37] A.K. Bangalore, A.K. Sood, Securing web servers using self cleansing intrusion tolerance (SCIT), in: 2009 Second International Conference on Dependability, IEEE, 2009, pp. 60–65.
[38] U. Rauf, F. Gillani, E. Al-Shaer, et al., Formal approach for resilient reachability based on end-system route agility, in: Proceedings of the 2016 ACM Workshop on Moving Target Defense, 2016, pp. 117–127.
[39] S. Achleitner, T. La Porta, P. McDaniel, et al., Cyber deception: Virtual networks to defend insider reconnaissance, in: Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, 2016, pp. 57–68.
[40] J.D. Touch, G.G. Finn, Y.S. Wang, et al., DynaBone: dynamic defense using multi-layer internet overlays, in: Proceedings DARPA Information Survivability Conference and Exposition, Vol. 2, IEEE, 2003, pp. 271–276.
[41] H. Moniz, N.F. Neves, M. Correia, et al., Randomized intrusion-tolerant asynchronous services, in: International Conference on Dependable Systems and Networks (DSN'06), IEEE, 2006, pp. 568–577.
[42] S.Y. Chang, Y. Park, B.B.A. Babu, Fast ip hopping randomization to secure hop-by-hop access in sdn, IEEE Trans. Netw. Serv. Manag. 16 (1) (2018) 308–320.
[43] E. Al-Shaer, Q. Duan, J.H. Jafarian, Random host mutation for moving target defense, in: International Conference on Security and Privacy in Communication Systems, Springer, Berlin, Heidelberg, 2012, pp. 310–327.
[44] Z. Gu, J. Zhang, Y. Ji, et al., Network topology reconfiguration for FSO-based fronthaul/backhaul in 5G+ wireless networks, IEEE Access 6 (2018) 69426–69437.
[45] K. Karthikeyan, R. Sunder, K. Shankar, et al., Energy consumption analysis of virtual machine migration in cloud using hybrid swarm optimization (ABC–BA), J. Supercomput. 76 (5) (2020) 3374–3390.
[46] J. Wu, Analysis on diversity, randomness, and dynameicity, in: Cyberspace Mimic Defense, Springer, Cham, 2020, pp. 159–205.
[47] X. Yang, J. Hu, Y. Ji, et al., Design of a metasurface antenna with pattern diversity, IEEE Antennas Wirel. Propag. Lett. (2020).
[48] H. Hu, J. Wu, Z. Wang, et al., Mimic defense: a designed-in cybersecurity defense framework, IET Inf. Secur. 12 (3) (2017) 226–237.
[49] Y. Wang, J. Wu, Y. Guo, et al., Scientific workflow execution system based on mimic defense in the cloud environment, Front. Inf. Technol. Electron. Eng. 19 (12) (2018) 1522–1536.
[50] J.H. Jafarian, E. Al-Shaer, Q. Duan, Openflow random host mutation: transparent moving target defense using software defined networking, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, 2012, pp. 127–132.
[51] M. Thompson, N. Evans, V. Kisekka, Multiple OS rotational environment an implemented moving target defense, in: 2014 7th International Symposium on Resilient Control Systems, ISRCS, IEEE, 2014, pp. 1–6.
[52] A. Aydeger, N. Saputro, K. Akkaya, et al., Mitigating crossfire attacks using SDN-based moving target defense, in: 2016 IEEE 41st Conference on Local Computer Networks, LCN, IEEE, 2016, pp. 627–630.
[53] R. Algin, H.O. Tan, K. Akkaya, Mitigating selective jamming attacks in smart meter data collection using moving target defense, in: Proceedings of the 13th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 2017, pp. 1–8.
[54] M. Albanese, A. De Benedictis, S. Jajodia, et al., A moving target defense mechanism for manets based on identity virtualization, in: 2013 IEEE Conference on Communications and Network Security, CNS, IEEE, 2013, pp. 278–286.
[55] S. Debroy, P. Calyam, M. Nguyen, et al., Frequency-minimal moving target defense using software-defined networking, in: 2016 International Conference on Computing, Networking and Communications, ICNC, IEEE, 2016, pp. 1–6.
[56] H. Zhang, C. Lei, D. Chang, et al., Network moving target defense technique based on collaborative mutation, Comput. Secur. 70 (2017) 51–71.
[57] S.A. DeLoach, X. Ou, R. Zhuang, et al., Model-driven, moving-target defense for enterprise network security, in: Models@ Run. Time, Springer, Cham, 2014, pp. 137–161.
[58] T.A. Tamba, B. Hu, Y.Y. Nazaruddin, On event-triggered implementation of moving target defense control, IFAC-PapersOnLine 53 (2) (2020) 3539–3544.
[59] X. Xu, H. Hu, H. Zhang, et al., Random routing defense method based on deep deterministic policy gradient, J. Commun. 42 (6) (2021) 41–51.
[60] A.D. Keromytis, R. Geambasu, S. Sethumadhavan, et al., The meerkats cloud security architecture, in: 2012 32nd International Conference on Distributed Computing Systems Workshops, IEEE, 2012, pp. 446–450.
[61] H. Wu, T. Chen, A DDoS defense method based on port and address hopping in SDN, Cyberspace Secur. 1 (8) (2020) 4.
[62] Y. Huang, A.K. Ghosh, Introducing diversity and uncertainty to create moving attack surfaces for web services, in: Moving Target Defense, Springer, New York, NY, 2011, pp. 131–151.
[63] P. Kampanakis, H. Perros, T. Beyene, SDN-based solutions for moving target defense network protection, in: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, IEEE, 2014, pp. 1–6.
[64] V. Zangeneh, M. Shajari, A cost-sensitive move selection strategy for moving target defense, Comput. Secur. 75 (2018) 72–91.
[65] R. Zhuang, S. Zhang, S.A. DeLoach, et al., Simulation-based approaches to studying effectiveness of moving-target network defense, in: National Symposium on Moving Target Research, 2012, p. 246.
[66] Z. Li, J. Tan, R. Hu, et al., Moving target defense method based on double address hopping, Netinfo Secur. 21 (2) (2021) 24–33.
[67] P.K. Manadhata, Game theoretic approaches to attack surface shifting, in: Moving Target Defense II, Springer, New York, NY, 2013, pp. 1–13.
[68] N. Ben-Asher, J. Morris-King, B. Thompson, et al., Attacker skill defender strategies and the effectiveness of migration-based moving target defense in cyber systems, in: Proc. 11th Int. Conf. Cyber Warfare Security, ICCWS, 2016, p. 21.
[69] A.V. Outkin, B.K. Eames, S.T. Jones, et al., A Framework for Analysis of Attacker-Defender Interaction in Cyber Systems, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2016.
[70] M.H. Valizadeh, H. Maleki, W. Koch, et al., Markov modeling of moving target defense games, IACR Cryptol. ePrint Arch. (2016).
[71] H. Maleki, S. Valizadeh, W. Koch, et al., Markov modeling of moving target defense games, in: Proceedings of the 2016 ACM Workshop on Moving Target Defense, 2016, pp. 81–92.
[72] Z. Zhou, C. Xu, T. Ma, et al., Multi-vNIC intelligent mutation: A moving target defense to thwart client-side DNS cache attack, in: ICC 2020-2020 IEEE International Conference on Communications, ICC, IEEE, 2020, pp. 1–6.
[73] A.R. Eldosouky, W. Saad, D. Niyato, Single controller stochastic games for optimized moving target defense, in: 2016 IEEE International Conference on Communications, ICC, IEEE, 2016, pp. 1–6.
[74] Y. Zhou, G. Cheng, S. Jiang, et al., A cost-effective shuffling method against DDoS attacks using Moving Target Defense, in: Proceedings of the 6th ACM Workshop on Moving Target Defense, 2019, pp. 57–66.
[75] Z. Chen, G. Chen, Moving target defense technology using Stackelberg-Markov asymmetrical trilateral game model, Chinese J. Comput. 43 (03) (2020) 512–525.
[76] Y. Zhou, G. Cheng, S. Jiang, et al., Cost-effective moving target defense against DDoS attacks using trilateral game and multi-objective Markov decision processes, Comput. Secur. 97 (2020) 101976.
[77] A. Clark, K. Sun, L. Bushnell, et al., A game-theoretic approach to IP address randomization in decoy-based cyber defense, in: International Conference on Decision and Game Theory for Security, Springer, Cham, 2015, pp. 3–21.
[78] X. Feng, Z. Zheng, P. Mohapatra, et al., A stackelberg game and markov modeling of moving target defense, in: International Conference on Decision and Game Theory for Security, Springer, Cham, 2017, pp. 315–335.
[79] S. Sengupta, A. Chowdhary, D. Huang, et al., Moving target defense for the placement of intrusion detection systems in the cloud, in: International Conference on Decision and Game Theory for Security, Springer, Cham, 2018, pp. 326–345.

[80] L. Niu, A. Clark, A framework for joint attack detection and control under false data injection, in: International Conference on Decision and Game Theory for Security, Springer, Cham, 2019, pp. 352–363.
[81] H. Li, W. Shen, Z. Zheng, Spatial–temporal moving target defense: A markov stackelberg game model, 2020, arXiv preprint arXiv:2002.10390.
[82] A. Chowdhary, D. Huang, A. Sabur, et al., SDN-based Moving Target Defense using Multi-agent Reinforcement Learning.
[83] G. Cai, B. Wang, Q. Xing, Game theoretic analysis for the mechanism of moving target defense, Front. Inf. Technol. Electron. Eng. 18 (12) (2017).
[84] Q. Zhu, T. Başar, Game-theoretic approach to feedback-driven multi-stage moving target defense, in: International Conference on Decision and Game Theory for Security, Springer, Cham, 2013, pp. 246–263.
[85] M.L. Winterrose, K.M. Carter, N. Wagner, et al., Adaptive attacker strategy development against moving target cyber defenses, in: Advances in Cyber Security Analytics and Decision Systems, Springer, Cham, 2020, pp. 1–14.
[86] X. Feng, Z. Zheng, D. Cansever, et al., A signaling game model for moving target defense, in: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, IEEE, 2017, pp. 1–9.
[87] S.G. Vadlamudi, S. Sengupta, M. Taguinod, et al., Moving target defense for web applications using bayesian stackelberg games, in: Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems, 2016, pp. 1377–1378.
[88] S. Sengupta, S.G. Vadlamudi, S. Kambhampati, et al., A game theoretic approach to strategy generation for moving target defense in web applications, in: AAMAS, 2017, pp. 178–186.
[89] K. Ding, X. Ren, D.E. Quevedo, et al., Defensive deception against reactive jamming attacks in remote state estimation, Automatica 113 (2020) 108680.
[90] H. Zhang, K. Zheng, X. Wang, et al., Strategy selection for moving target defense in incomplete information game, Comput. Mater. Contin. 62 (2) (2020) 763–786.
[91] E.M. Kandoussi, M. Hanini, I. El Mir, et al., Toward an integrated dynamic defense system for strategic detecting attacks in cloud networks using stochastic game, Telecommun. Syst. 73 (3) (2020) 397–417.
[92] R. Colbaugh, K. Glass, Predictability-oriented defense against adaptive adversaries, in: 2012 IEEE International Conference on Systems, Man, and Cybernetics, SMC, IEEE, 2012, pp. 2721–2727.
[93] S. Sengupta, S. Kambhampati, Multi-agent reinforcement learning in bayesian stackelberg markov games for adaptive moving target defense, 2020, arXiv preprint arXiv:2007.10457.
[94] J. Zhao, X. Zhang, F. Di, et al., Exploring the optimum proactive defense strategy for the power systems from an attack perspective, Secur. Commun. Netw. 2021 (2021).
[95] S. Sengupta, T. Chakraborti, S. Kambhampati, Mtdeep: boosting the security of deep neural nets against adversarial attacks with moving target defense, in: Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence, 2018.
[96] Y. Sun, W. Ji, J. Weng, Selection of defensive optimal strategy for moving target signal game, J. Front. Comput. Sci. Technol. 14 (9) (2020) 1510–1520.
[97] Y. Sun, W. Ji, J. Weng, et al., Selection of optimal strategy for moving target defense based on signal game, in: Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, 2020, pp. 28–32.
[98] T. Chen, G. Wang, R. Ma, et al., Platform dynamic defense strategies based on signaling game[J/OL], J. Chongqing Univ. Posts Telecommun. (Nat. Sci.) 1-9.
[99] L. Jiang, H. Zhang, J. Wang, Optimal strategy selection method for moving target defense based on signaling game, J. Commun. 40 (6) (2019) 128–137.
[100] L. Jiang, H. Zhang, J. Wang, A Markov signaling game-theoretic approach to moving target defense strategy selection, Acta Electron. Sin. 49 (3) (2021) 527–535.
[101] X. Chen, X. Liu, L. Zhang, et al., Optimal defense strategy selection for spear-phishing attack based on a multistage signaling game, IEEE Access 7 (2019) 19907–19921.
[102] A. Aydeger, M.H. Manshaei, M.A. Rahman, et al., Strategic defense against stealthy link flooding attacks: A signaling game approach, IEEE Trans. Netw. Sci. Eng. 8 (1) (2021) 751–764.
[103] M.A. Rahman, M.G.M.M. Hasan, M.H. Manshaei, et al., A game-theoretic analysis to defend against remote operating system fingerprinting, J. Inf. Secur. Appl. 52 (2020) 102456.
[104] M.A. Rahman, M.H. Manshaei, E. Al-Shaer, A game-theoretic approach for deceiving remote operating system fingerprinting, in: 2013 IEEE Conference on Communications and Network Security, CNS, IEEE, 2013, pp. 73–81.
[105] R. Zhuang, S.A. DeLoach, X. Ou, Towards a theory of moving target defense, in: Proceedings of the First ACM Workshop on Moving Target Defense, 2014, pp. 31–40.
[106] A. Clark, K. Sun, R. Poovendran, Effectiveness of IP address randomization in decoy-based moving target defense, in: 52nd IEEE Conference on Decision and Control, IEEE, 2013, pp. 678–685.
[107] A.H. Anwar, G. Atia, M. Guirguis, A game-theoretic framework for the virtual machines migration timing problem, IEEE Trans. Cloud Comput. (2019).
[108] A.H. Anwar, G. Atia, M. Guirguis, It's time to migrate! A game-theoretic framework for protecting a multi-tenant cloud against collocation attacks, in: 2018 IEEE 11th International Conference on Cloud Computing, CLOUD, IEEE, 2018, pp. 725–731.
[109] R.E. Navas, Improving the Resilience of the Constrained Internet of Things: A Moving Target Defense Approach, Ecole nationale supérieure Mines-Télécom Atlantique, 2020.
[110] T. Chen, R. Ma, G. Wang, et al., Dynamic defense strategy for platform based on event-driven and timing migration, Comput. Eng. 45 (9) (2019) 105–111.
[111] R. Ma, T. Chen, G. Wang, et al., Dynamic defense active migration strategy for heterogeneous platforms of DMZ, Fire Control Command Control 44 (03) (2019) 1–8+22.
[112] H. Li, Z. Zheng, Optimal timing of moving target defense: A Stackelberg game model, in: MILCOM 2019-2019 IEEE Military Communications Conference, MILCOM, IEEE, 2019, pp. 1–6.
[113] M.V. Dijk, A. Juels, A. Oprea, et al., FlipIt: The game of stealthy takeover, J. Cryptol. 26 (4) (2013) 655–713.
[114] K.D. Bowers, M.V. Dijk, R. Griffin, et al., Defending against the unknown enemy: Applying FL I PIT to system security, in: Introduction to Statistics for the Behavioral Sciences. Saunders, 2009.
[115] A. Nochenson, J. Grossklags, A behavioral investigation of the FlipIt game, in: Proceedings of the 12th Workshop on the Economics of Information Security, WEIS, 2013, p. 93.
[116] P. Lee, A. Clark, B. Alomair, L. Bushnell, R. Poovendran, A host takeover game model for competing malware, in: Proceedings of the IEEE Conference on Decision and Control, Osaka, Japan, 2015, pp. 4523–4530.
[117] J. Pawlick, S. Farhang, 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, 2015, pp. 289–308.
[118] M. Zhang, Z. Zheng, N.B. Shroff, Stealthy attacks and observable defenses: A game theoretic model under strict resource constraints, in: Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP), Atlanta, GA, USA, 2014, pp. 813–817.
[119] A. Laszka, G. Horvath, M. Felegyhazi, L. Buttyan, Flipthem: Modeling targeted attacks with flipit for multiple resources, in: Decision and Game Theory for Security, in: LNCS, Springer, 2014, pp. 175–194.
[120] X. Feng, Z. Zheng, D. Cansever, et al., Stealthy attacks with insider information: A game theoretic model with asymmetric feedback, in: MILCOM 2016-2016 IEEE Military Communications Conference, IEEE, 2016, pp. 277–282.
[121] X. Feng, Z. Zheng, P. Hu, et al., Stealthy attacks meets insider threats: A three-player game model, in: MILCOM 2015-2015 IEEE Military Communications Conference, IEEE, 2015, pp. 25–30.
[122] S. Jones, A. Outkin, J. Gearhart, J. Hobbs, J. Siirola, C. Phillips, S. Verzi, D. Tauritz, S. Mulder, A. Naugle, Evaluating Moving Target Defense with Pladd, Technical report, Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), 2015.
[123] D. Hao, K. Sakurai, A differential game approach to mitigating primary user emulation attacks in cognitive radio networks, in: 2012 IEEE 26th International Conference on Advanced Information Networking and Applications, IEEE, 2012, pp. 495–502, http://www.nitrd.gov/pubs/CSIA_IWG_Cybersecurity_GameChange_RD_Recommendations_20100513.pdf.
[124] G. Feng, J. Lin, Q. Zhao, et al., A differential game based approach against objective function attack in cognitive networks, Chin. J. Electron. 27 (4) (2018) 879–888.
[125] X. An, F. Lin, S. Xu, et al., A novel differential game model-based intrusion response strategy in fog computing, Secur. Commun. Netw. 2018 (2018).
[126] Q. Gao, H. Wu, J. Zhang, et al., Multi-attacker multi-defender interaction in mMTC networks via differential game, in: 2020 IEEE/CIC International Conference on Communications in China, ICCC, IEEE, 2020, pp. 1250–1255.
[127] Q. Gao, H. Wu, Y. Zhang, et al., Differential game-based analysis of multi-attacker multi-defender interaction, Sci. China Inf. Sci. 64 (12) (2021) 1–13.
[128] H. Wu, Q. Gao, X. Tao, et al., Differential game approach for attack-defense strategy analysis in internet of things networks, IEEE Internet Things J. (2021).
[129] S. Huang, H. Zhang, J. Wang, et al., Markov differential game for network defense decision-making method, IEEE Access 6 (2018) 39621–39634.
[130] Y. Mi, H. Zhang, H. Hu, et al., Optimal network defense strategy selection method: A stochastic differential game model, Secur. Commun. Netw. 2021 (2021).

[131] L.X. Yang, P. Li, Y. Zhang, et al., Effective repair strategy against advanced persistent threat: A differential game approach, IEEE Trans. Inf. Forensics Secur. 14 (7) (2018) 1713–1728.
[132] S. Wang, Y. Pu, H. Shi, et al., A differential game view of antagonistic dynamics for cybersecurity, Comput. Netw. 200 (2021) 108494.
[133] Y. He, M. Zhang, X. Yang, et al., The intelligent offense and defense mechanism of internet of vehicles based on the differential game-IP hopping, IEEE Access 8 (2020) 115217–115227.
[134] Y. Sun, W. Ji, J. Weng, et al., Optimal strategy of moving target defense based on differential game, J. Comput. Res. Dev. 58 (8) (2021) 1789–1800.
[135] W. Ye, S. Fan, Evolutionary snowdrift game with rational selection based on radical evaluation, Appl. Math. Comput. 294 (2017) 310–317.
[136] S. Arora, P. Singh, A.J. Gupta, Adaptive selection of cryptographic protocols in wireless sensor networks using evolutionary game theory, Procedia Comput. Sci. 78 (2016) 358–366.
[137] Y. Du, J. Xia, J. Ma, et al., An optimal decision method for intrusion detection system in wireless sensor networks with enhanced cooperation mechanism, IEEE Access 9 (2021) 69498–69512.
[138] A.A.A. Abass, L. Xiao, N.B. Mandayam, et al., Evolutionary game theoretic analysis of advanced persistent threats against cloud storage, IEEE Access 5 (2017) 8482–8491.
[139] S. Boudko, P. Aursand, H. Abie, Evolutionary game for confidentiality in IoT-enabled smart grids, Information 11 (12) (2020) 582.
[140] Y. Yang, B. Che, Y. Zeng, et al., MAIAD: a multistage asymmetric information attack and defense model based on evolutionary game theory, Symmetry 11 (2) (2019) 215.
[141] N. Ruan, L. Gao, H. Zhu, et al., Toward optimal dos-resistant authentication in crowdsensing networks via evolutionary game, in: 2016 IEEE 36th International Conference on Distributed Computing Systems, ICDCS, IEEE, 2016, pp. 364–373.
[142] M. Azab, B.M. Mokhtar, A.S. Abed, et al., Smart moving target defense for linux container resiliency, in: 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, CIC, IEEE, 2016, pp. 122–130.
[143] Z. Wang, G. Wang, T. Chen, et al., Platform dynamic defense evolution game model and state migration strategy, J. Air Force Eng. Univ. (Nat. Sci. Ed.) 21 (3) (2020) 85–92.
[144] R. Colbaugh, K. Glass, Moving target defense for adaptive adversaries, in: 2013 IEEE International Conference on Intelligence and Security Informatics, IEEE, 2013, pp. 50–55.
[145] K. Glass, R. Colbaugh, Moving Target Defense for Adaptive Adversaries, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2013.
[146] W. Bi, H. Lin, L. Zhang, Moving target defense decision-making algorithm based on multi-stage evolutionary signal game model, J. Comput. Appl. (2021).
[147] L. Shi, X. Wang, H. Hou, Research on optimization of array honeypot defense strategies based on evolutionary game theory, Mathematics 9 (8) (2021) 805.
[148] G. Wang, Z. Wang, E. Zhang, et al., Markov evolutionary game model and migration strategies for multi-stage platform dynamic defense, Acta Armamentarii 42 (8) (2021) 1690–1697.
[149] S. Sengupta, Moving target defense: a symbiotic framework for AI & security, in: Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems, 2017, pp. 1861–1862.
[150] S. Sengupta, Moving Target Defense: A Symbiotic Framework for AI & Security (Doctoral Consortium), 2017.
[151] C. Gao, Y. Wang, Reinforcement learning based self-adaptive moving target defense against DDoS attacks, J. Phys. Conf. Ser. 1812 (1) (2021) 012039, IOP Publishing.
[152] M. Zhu, Z. Hu, P. Liu, Reinforcement learning algorithms for adaptive cyber defense against Heartbleed, in: Proceedings of the First ACM Workshop on Moving Target Defense, 2014, pp. 51–58.
[153] B. Tozer, T. Mazzuchi, S. Sarkani, Optimizing attack surface and configuration diversity using multi-objective reinforcement learning, in: 2015 Ieee 14th International Conference on Machine Learning and Applications (Icmla), IEEE, 2015, pp. 144–149.
[154] Z. Hu, M. Zhu, P. Liu, Adaptive cyber defense against multi-stage attacks using learning-based POMDP, ACM Trans. Priv. Secur. 24 (1) (2020) 1–25.
[155] S. Yoon, J.H. Cho, D.S. Kim, et al., Moving target defense for in-vehicle software-defined networking: IP shuffling in network slicing with multiagent deep reinforcement learning, in: Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II, Vol. 11413, International Society for Optics and Photonics, 2020, p. 114131U.
[156] T. Eghtesad, Y. Vorobeychik, A. Laszka, Deep reinforcement learning based adaptive moving target defense, 2019, arXiv preprint arXiv:1911.11972.
[157] H. Zhang, J. Tan, X. Liu, S. Huang, H. Hu, Y. Zhang, Cybersecurity threat assessment integrating qualitative differential and evolutionary games, IEEE Trans. Netw. Serv. Manag. 19 (3) (2022) 3425–3437.
[158] J. Tan, H. Jin, H. Hu, R. Hu, H. Zhang, H.W. Zhang, WF-MTD: Evolutionary decision method for moving target defense based on wright-fisher process, IEEE Trans. Dependable Secure Comput. http://dx.doi.org/10.1109/TDSC.2022.3232537.
[159] H. Zhang, Y. Mi, X. Liu, Y. Zhang, J. Wang, J. Tan, A differential game approach for real-time security defense decision in scale-free networks, Comput. Netw. (2023).