applied sciences

MDPI

Review

A Survey on Moving Target Defense: Intelligently Affordable, Optimized and Self-Adaptive

Rongbo Sun, Yuefei Zhu, Jinlong Fei * and Xingyu Chen

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China; satoshi626@163.com (R.S.); yfzhu17@sina.com (Y.Z.); heimda11r@foxmail.com (X.C.)
* Correspondence: feijinlong_2021@163.com

Abstract: Represented by reactive security defense mechanisms, cyber defense possesses a static, reactive, and deterministic nature, with overwhelmingly high costs to defend against ever-changing attackers. To change this situation, researchers have proposed moving target defense (MTD), which introduces the concept of an attack surface to define cyber defense in a brand-new manner, aiming to provide a dynamic, continuous, and proactive defense mechanism. With the increasing use of machine learning in networking, researchers have discovered that MTD techniques based on machine learning can provide omni-bearing defense capabilities and reduce defense costs at multiple levels. However, research in this area remains incomplete and fragmented, and significant progress is yet to be made in constructing a defense mechanism that is both robust and available. Therefore, we conducted a comprehensive survey on MTD research, summarizing the background, design mechanisms, and shortcomings of MTD, as well as relevant features of intelligent MTD that are designed to overcome these limitations. We aim to provide researchers seeking the future development of MTD with insight into building an intelligently affordable, optimized, and self-adaptive defense mechanism.

Keywords: moving target defense; cyber security; affordable defense; self-adaptive defense; intelligent defense

Citation: Sun, R.; Zhu, Y.; Fei, J.; Chen, X. A Survey on Moving Target Defense: Intelligently Affordable, Optimized and Self-Adaptive. *Appl. Sci.* **2023**, *13*, 5367. https://doi.org/10.3390/app13095367

Academic Editors: Luis Javier García Villalba and Ki-Hyun Jung

Received: 30 March 2023
Revised: 21 April 2023
Accepted: 24 April 2023
Published: 25 April 2023

1. Introduction

1.1. Motive

To use a Chinese idiom to paraphrase the idea of moving target defense (MTD), *transferring flowers to wood* is the most appropriate one, which refers to covertly grafting the branch of a flowering tree onto another flowering tree so that no one can tell what kind of flowering tree it was before. Likewise, the method that defenders constantly and dynamically use to shift the set of attributes that can be exploited by attackers to confuse them coincides with the idea behind this idiom. In a more concise and direct manner, a target can be defined as an entity or asset that is susceptible to exploitation by malicious adversaries, such as an application, computer, or system. MTD refers to a set of techniques that involves altering the properties or configurations of a target randomly and regularly or increasing its uncertainty and unpredictability, with the primary objective of enhancing the security defenses of the target while preserving its fundamental functionality.

The concept of MTD arose from the reality that traditional cyber defense strategies focus on reinforcing the defense system, but this approach inevitably exposes information to attackers once the system is fortified. To counter this disadvantage, researchers proposed MTD as a revolutionary game-changing technique to address the growing complexity and variability of cyber-attacks. Unlike traditional defense strategies, which seek to harden and create an impenetrable system, MTD focuses on increasing the system's resilience by constantly shifting the attack surface, as shown in Figure 1. This makes it more challenging and costly for attackers to exploit vulnerabilities while limiting the time that the vulnerability is exposed. By implementing MTD, organizations can reduce the likelihood of successful attacks and increase their ability of responding effectively against cyber threats.

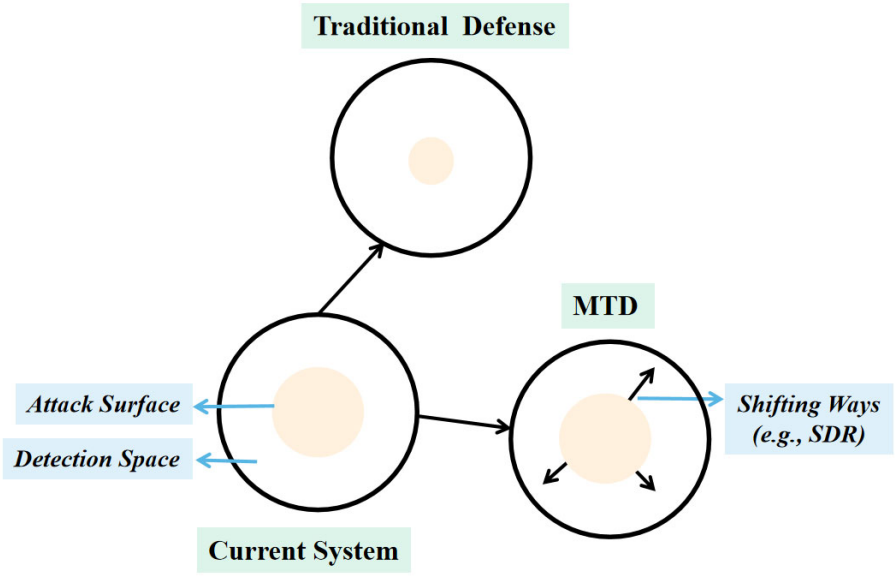

Figure 1. The differences between traditional defense and MTD working on a system.

In recent years, numerous MTD techniques have been proposed in response to the shortcomings of traditional cyber defense. Notably, the field of intelligent MTD has garnered significant attention and has become a subject of considerable interest in MTD research due to the extraordinary performance of machine learning algorithms in processing complex, massive, and high-dimension data in many tasks and have shown more accurate and collegiate performance in many complex problems [1] compared to traditional decision-making methods.

However, research on intelligent MTD remains incomplete and lacks systematic summary investigations. While nearly 3000 papers have been published since 2018 on proposed MTD techniques, intelligent MTD research remains relatively scattered without being firmly integrated, with each researcher focusing on their own field. This situation stands in contrast to other intelligent techniques that have undergone comprehensive research and integration. As a result, research on intelligent MTD is currently inefficient and fragmented. The main challenges for intelligent MTD can be listed as follows.

- The current state of intelligent MTD has not yet achieved a unified and comprehensive system. For instance, when classifying existing intelligent MTD techniques by applying them into five layers (network layer, platform layer, runtime environment layer, software layer, and data layer), it was observed that most of these techniques were primarily focused on the network layer, with little attention paid to other layers. This lack of attention to multi-layer protection was inconsistent with the continued development of a defense system for more than ten years.
- Diverse intelligent MTD techniques require a systematic organization to facilitate researchers' comprehension of the evolution and trends of intelligent MTD. Such an organization is expected to contribute significantly to the development of intelligent MTD. Specifically, after organizing these techniques, researchers can gain insights into one of the emerging trends *toward self-adaptive* as intelligent MTD is organized. They can comprehend that this trend frequently employs machine learning (ML) algorithms that are deformed by reinforcement learning (RL). We believe such a systematic organization provides an opportunity for researchers to advance their research alongside the development of related MTD techniques.

Based on the above-mentioned issues, we have provided our solution in this exhaustive survey. In contrast to traditional surveys of MTD, this survey aims to present the latest trends in MTD: how to move toward affordable, optimized, and self-adaptive MTD in

the context of intelligence. We present our insights and perspectives for the provision of researchers looking for future trends in MTD development.

1.2. Survey Methodology

We used the thesis database (Scopus database, occasionally assisted by the Web of Science) and specific keywords (such as moving target defense, machine learning, etc.) to search and determine an extensive range of the literature review papers (LRPs) that were initially related [2]. One most straightforward way to achieve this is to filter the papers' date (we have been looking for papers for nearly 20 years), publishing platform, field, and so on with the filter that comes with the database, including journal articles and conference papers. By browsing abstracts, keywords, and objective statements of pieces of the literature, we could determine their relevance. Then, the results of rough reading based on inductive coding and of intensive reading based on co-occurrence analysis were presented. The papers were selected based on three main criteria: whether they (i) provided new machine learning techniques or ideas on moving target defense, (ii) had a high degree of completion and reproducibility, and (iii) had the ability to meet the demands of affordability, optimization, and self-adaptation.

We initially collected around 150 published papers with relevant keywords in the thesis database, in addition to many online articles, with each paper carefully reviewed and summarized. Then, we analyzed around 80 papers in this survey based on the selection criteria mentioned above. Additionally, by then, we had come up with a system flow of what our survey should be similar to, as shown in Figure 2.

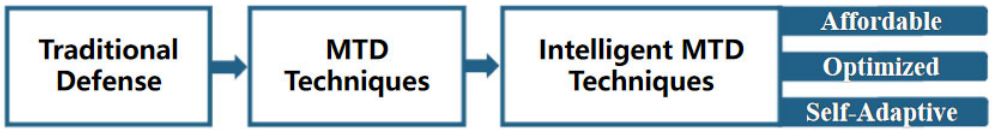

Figure 2. The systematic flow of our survey.

The selected papers were then grouped into three categories: (i) MTD-related techniques, (ii) intelligent MTD-related techniques, and (iii) surveys that concentrated on MTD development. It needs to be noted that these three categories were not mutually exclusive. We believe all the papers selected were state-of-the-art at that moment. We selected them to follow our systematic flow.

- Papers in (i) were put forward because their defense methods showed better effectiveness than corresponding traditional defense or their defense methods could be improved into intelligent MTD techniques and be compared with the latter ones.
- Papers in (ii) were put forward because their defense methods could achieve more significance than previous ones. We collected these papers and summarized three categories of them, *towards affordable*, *towards optimized*, and *towards self-adapting*, respectively. Or we could also regard them as development trends of intelligent MTD based on their commonalities. We analyzed what these papers had achieved and what they had not accomplished to approximately represent the status quo of the entire category.
- Papers in (iii) demonstrated different categories of MTD techniques, and we classified them into various levels, which helped us to comprehend the development of MTD in a more comprehensive way.

1.3. Comparison with Existing MTD Surveys

We selected several surveys that had completed investigations of MTD since 2013 for comparison, chiefly aiming at the main concept, mechanism, and classification of MTD techniques and intelligent MTD techniques, and insights and future development recommendations on MTD, as shown in Table 1.

Table 1. Summary of related works.

Refs.	Year	MTD Mechanism	Intelligent MTD Introduction	Intelligent MTD Traits	Intelligent MTD Development Trend	Insights
Okhravi et al. [3,4]	2013, 2018	Five layers	-	-	-	From passive defense into proactive defense
Cai et al. [5]	2016	Three layers	-	-	-	Function-and-movement model
Lei et al. [6]	2018	Four layers	√	Coarsely	Coarsely	From proactive defense into reactive defense
Zheng et al. [7]	2019	Three layers	Coarsely	Coarsely	-	The perspective of architectural structure
Sengupta et al. [8]	2019	Five attack surface shifting ways	Coarsely	Coarsely	-	A simple and yet general notion of defense
Cho et al. [9]	2020	SDR	√	Partially	Coarsely	Toward proactive, adaptive defense
Sun et al. [10]	2020	GT-related	GT-related MLs	-	-	Optimized defense behaviors
Our survey	-	SDR/Five layers	√	√	√	Intelligently affordable, optimized and self-adaptive defense

The earliest investigation of MTD-related techniques appeared in 2013, when MIT Lincoln Laboratory published a technical report that provided an exhaustive survey of MTD [3] and, within five years, a significantly expanded and updated version was released [4]. The main contribution of these two surveys is that the first survey was the first to classify MTD into five layers based on what MTD moved: dynamic data layer, dynamic software layer, dynamic runtime environment layer, dynamic platform layer, and dynamic network layer. The second survey gave an exhaustive list of MTD techniques in each category and the types of attacks based on each category of MTD techniques.

In 2016, Cai et al. [5] adopted a revolutionary classification method to classify MTD techniques: three implementation layers, including software, the running platform, and the physical network. This classification covered all kinds of examples in the literature on MTD techniques at that time, but this survey did not provide a comprehensive summary in terms of the combination of MTD techniques. The three-layer classification method was not widely used due to its limitation in classification, and most of the MTD techniques are still classified based on the five-layer classification method mentioned above.

In 2018, Lei et al. [6] conducted extensive investigations in the areas of strategies generation, restructuring the implementation and performance evaluation of MTD, among which the classification methods are based on multiple criteria: theory (e.g., game theory, machine learning, and genetic algorithms), technology (e.g., transformation or restructuring of system configurations), and purpose. For this reason, one may need a more consistent classification to obtain a clear depiction of the overall trends in MTD research and to easily gain insights from existing MTD methods.

In 2019, Zheng et al. [7] published an overview of a survey on the technical architecture of MTD based on the application, operating system, and network levels. As the title suggests, this survey focused mainly on an architectural analysis of MTD techniques, such as software diversification, addressing space layout randomization, instruction set randomization, and IP randomization.

In the same year, Sengupta et al. [8] conducted a survey of defensive MTD tools, techniques, and strategies, from which the designation of key actions, the implementation of MTD, and the evaluation of the effectiveness of MTD are all covered in this survey. However, some critical aspects of the implementation layer and MTD portfolio are missing from its classification. This is the unity that is generally lacking in MTD surveys.

Cho et al. [9] 2020 presented a comprehensive survey of MTD techniques covering all the relevant aspects that MTD techniques may involve: essential layers, design principles of MTD techniques, MTD classification, common attacks, key methods, important algorithms,

metrics, evaluation methods, and application areas. Remarkably, this survey discussed the pros and cons of each aspect of MTD investigated in detail.

Meanwhile, Sun et al. [10] focused on the game-theoretic decision-making approaches of MTD and systematically introduced the application scenarios of combining MTD with four different game-theoretic models (static game, signal game, Markov game, differential game, and evolutionary game) with some new perspectives and interpretations of game-theoretic MTD research, and proposed a direction for future development.

The surveys above do not provide a more detailed description of the development of intelligent MTD, which leads to insufficient analysis and guidance facing the intelligent network world. This is what we are trying to introduce: the development trend of intelligent MTD, as well as the shortcomings and prospects of intelligent MTD at the current stage of development. We are committed to discussing more technical details and helping researchers to obtain more detailed knowledge of the future development of MTD as much as possible.

1.4. Key Contributions

The main contribution of this paper is the presentation of a detailed and comprehensive account of the research and development process of intelligent MTD. Our work provides MTD-related researchers with the following new perspectives:

- We conducted a thorough survey on MTD, as shown in Figure 3. We analyzed the development and deficiencies of MTD techniques, highlighting the emergence of reinforced MTD techniques such as intelligent MTD and SDN-based MTD. Then, we focused on techniques related to intelligent MTD, categorizing them based on their characteristics towards *affordable*, *optimized*, and *self-adaptive*, and formed a systematic organization, aiming to provide researchers with a more intuitive understanding of current intelligent MTD techniques.
- During our research, we introduced a new classification method for MTD techniques, SDR/Five layers, which aligns more closely with existing MTD development. This approach has practical significance and offers a more detailed classification for all the MTD techniques proposed so far.
- We discussed the practical conclusions that could be obtained from our survey and identify existing limitations. From these insights, we offer suggestions for future developments in intelligent MTD techniques.

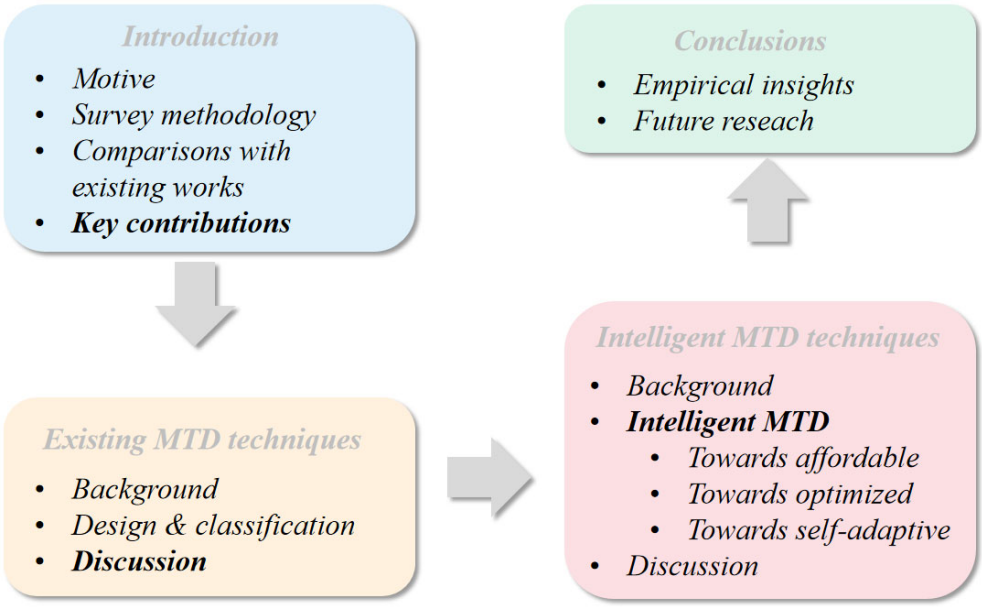

Figure 3. Structure of our survey.

2. MTD Techniques

2.1. Background

To have the principles of MTD thoroughly comprehended, it is essential to understand its background. The concept of MTD was first proposed in 2009 as a response to the shortcomings of reactive security defense mechanisms, which were primarily based on techniques such as authentication, access control, information encryption, intrusion detection, vulnerability scanning, and virus prevention. While these measures offered a degree of security, they proved inadequate due to the increasing automation and diversification of attacks. Furthermore, the complexity of modern networking environments places an overwhelming burden on network administrators, who may overlook even minor issues that could lead to serious security risks. In general, the following are key features that differentiate traditional cyber defense mechanisms from MTD:

- Traditional defenses aim to enhance the defense capabilities of static facilities and minimize their vulnerabilities' exposure. In contrast, MTD concentrates on dynamically shifting the attack surface [3] to increase resilience.
- Traditional defenses often focus on monitoring, detecting, preventing, and remediating attacks on static infrastructure. MTD emphasizes faster and more comprehensive attack detection and timely responses to mitigate potential damages.
- Traditional defenses rely on known attack patterns for defense and may be limited in addressing emerging or novel threats. MTD seeks to proactively address such unpredictable attacks through its dynamic nature.
- Unlike traditional defense mechanisms, which operate in a fixed dimension, MTD adapts and changes constantly to protect against attacks on ever-changing systems. This approach significantly limits attackers' research time and ability to penetrate compromised systems.

While general defense mechanisms aim to improve system stability, their rigid nature makes it challenging to ensure long-term fortification against the rapidly evolving techniques employed by attackers. In contrast, MTD prioritizes affordable, service-oriented defense [3] to meet three core development points:

- Minimizing defense costs (e.g., system deployment overhead)
- Maximizing service availability for users
- Maintaining the required defense security levels

Although MTD is built on the architecture of general defense, it aims to minimize deployment overhead by adopting existing security mechanisms as its base. Introducing new security measures requires intensive analysis and patching efforts quintessentially, which can be time-consuming and impractical. MTD aims to preserve affordability in individual system deployments while maintaining its fundamental principle of providing cost-effective defense, i.e., *affordable defense*.

2.2. Design and Classification

The basic design principle of MTD centers around three key points.

2.2.1. What to Move

By dynamically shifting attack surfaces, MTD techniques confuse attackers who rely on fixed system configurations to execute an attack. As a collection of resource attributes (shown in Table 2) in a system that could be used by an attacker to execute an attack, the attack surface can be exploited to confuse the attacker by dynamically changing these configurations. To facilitate the enumeration of joint attack surfaces, they can be classified hierarchically based on their level of existence. This classification leads to the first way of classifying MTD techniques, which includes the network layer, platform layer, runtime environment layer, software layer, and data layer [3].

Table 2. Attack surfaces most often utilized.

The Attack Surfaces Often Utilized in Recent Years (Since '18)		
Network L.	❑IP address/Port [11–23]	❑Route/Network topology [24–28]
Platform L.	❑Virtual Machines [29–33]	❑Proxies [34]
Rt. Env. L.	❑Operation Systems [35–37]	
Software L.	❑Software [38–42]	
Data L.	❑Instruction sets [43,44]	❑Codes [45,46]

Various MTD techniques can disrupt the attacker's resource reconnaissance and vulnerability detection. By continuously shifting the attack surface, MTD techniques hinder an attackers' ability to locate and access target hosts, forcing them to continuously chase the target. This not only increases the attacker's cost but also eliminates their temporal advantage and information asymmetry advantage over defenders. The result is a more resilient defense mechanism that can adapt to ever-evolving threats.

Research on MTD has primarily focused on the network layer for several key reasons. Firstly, designing defense mechanisms at the network layer is more in line with MTD's pursuit of affordable defense due to its small size, low resource consumption, and ease of operation. Secondly, narrowing the focus to a specific layer, such as the network layer, allows for more targeted study and development.

Nevertheless, it is important to note that MTD has been in development for over a decade, and thus, the current top-heavy research situation does not fully represent the breadth and depth of MTD as a cyber defense mechanism.

2.2.2. How to Move

By seeking ways to shift attack surfaces to increase unpredictability and uncertainty, MTD techniques can lead to information failure for attackers. Cho et al. [9] classified the shifting of attack surfaces into shuffling, diversity, and redundancy (SDR), as well as hybrid techniques based on a mixture of these two or three, as shown in Figure 4.

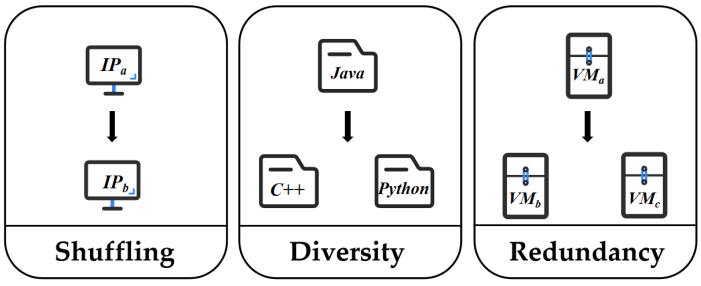

Figure 4. SDR examples.

- Shuffling

Shuffling involves randomizing or rearranging system configurations. IP hopping [11] is a common shuffling method that constantly changes the host's IP address to evade scanning by attackers. Shuffling does not require building new security techniques. Instead, it builds on existing ones, and is, therefore, less burdensome in terms of development costs and resource consumption, is easy to operate, and is highly compatible. However, because shuffling relies on the quality of existing techniques, its effectiveness may be limited if those techniques are not sufficiently robust against attacks.

- Diversity

Diversity means alternating between different components that can achieve the same system functionality. For example, if a program is programmed in Python, the same functionality can be achieved in C++. Diversity builds on existing defense techniques and

has similar advantages and disadvantages to shuffling. However, it also incurs additional defense costs due to the need to prepare extra systems or components.

- Redundancy

Redundancy refers to the preparation of multiple copies of a system or network component to ensure that the new copy can be replaced at any time if the original system or component is attacked, disabling the original attack process. It is worth noting that redundancy requires higher service availability for users than the previous two techniques. Therefore, quality measurement of redundancy is usually accomplished by evaluating the system's Quality of Service (QoS). In addition, if redundancy is not performed correctly, it provides a more significant opportunity for an attacker to execute an attack on a larger attack surface (e.g., another server to attack or another path to the target) than a system that does not use redundancy.

- Hybrid

Hybrid combines two or three of the above methods. While enhancing security, the benefits of each of the three methods can be taken into account, such as improving QoS while keeping the overhead low, but what cannot be overlooked is that hybrid presents a larger attack surface than individual methods and requires an additional overhead when combining multiple methods into a single solution.

We have presented the two mainstream classifications of MTD techniques based on what to move and how to move, respectively. We believe that these two categories can cover almost all the MTD techniques that have been proposed so far. Based on this idea, we introduced a combination of these two methods to form a new classification method called SDR/Five layers, as shown in Table 3. The features of this are precisely explained in this table.

Table 3. SDR/Five layers for MTD techniques.

Categories	Typical Techniques					Features
	Network L.	Platform L.	Ex. Env. L.	Software L.	Data L.	
Shuffling	IP hopping [11]	VM migration [29]	OS rotation [35]	Software rearrangement [39]	Keys rotation [40]	These techniques own a low burden in terms of development costs and resource consumption, ease of operation and high compatibility. Security is highly dependent on the quality of existing techniques.
Diversity	Diverse network configurations [46]	Multi-Dockers [47]	Diverse OSes [37]	Diverse software [42]	Diverse codes [45]	Broadly similar to shuffling techniques, they also result in sacrificing additional defense costs due to the need to prepare different systems or components.
Redundancy	Honeypot [48]	OS redundancy [30]	OS redundancy [35]	Software components redundancy [41]	-	The service availability requirements for users are higher than the above two kinds of techniques, and it is easier to extend the attack surface if they are not executed correctly.

2.2.3. When to Move

MTD techniques need to determine when to update the current state of the MTD system to maximize the invalidation of the relevant resource information obtained by an attacker. The conditions for triggering updates can be divided into fixed-time triggering [6] and ad hoc event triggering.

- Fixed-time triggering: MTD techniques periodically shift the attack surface at fixed intervals. Setting the triggering interval requires a technique-specific analysis, but for

each technique, researchers need to find the right triggering point. If the interval is too long, attackers have enough time to penetrate the system and launch an attack. If it is too short, the MTD mechanism is triggered frequently, leading to wasted resources and degraded performance. Additionally, frequent triggering of MTD can significantly degrade the QoS and users' experience.

As a result, self-adaptive MTD techniques based on ad hoc event triggering are becoming increasingly favored. These techniques can effectively avoid the problems associated with selecting fixed intervals. By adapting to changes in the system or network environment, self-adaptive MTD techniques can ensure optimal defense mechanisms that minimize the likelihood of successful attacks while maintaining high QoS and user usage satisfaction.

- Ad hoc event triggering: MTD shifts the attack surface when the system detects an attacker's access or a precursor to an attack. Self-adaptive MTD adopts this approach, and its main challenge is accurately predicting attacks that can trigger MTD effectively.

Machine learning can be a helpful tool in addressing this challenge by assisting in the achievement of the self-adaptive triggering of MTD. By analyzing patterns in system behavior, machine learning algorithms can identify potential threats and predict future attacks more accurately than traditional rule-based systems. In Section 3, we further discuss how machine learning can be leveraged to improve the effectiveness of self-adaptive MTD techniques.

2.3. Discussion

Based on our survey, we have recognized some development trends and challenges for existing MTD techniques.

2.3.1. Systematic Development

As mentioned above, MTD techniques are classified into two categories based on *what to move* and *how to move*, but these techniques are generally independently proposed by different researchers and have not yet formed a complete system. We cannot ignore that the overlapping use of various independently proposed MTD techniques may cause unforeseen conflicts. Therefore, it is urgent and significant in the future that work is conducted to analyze the system or network attributes affected by various MTD techniques, evaluate whether different MTD techniques can be utilized integrally, and establish a complete and available MTD system.

2.3.2. Integration with Existing Security Defense Mechanisms

MTD defends attackers by shifting the attack surface, but by its nature, this defense mechanism cannot cover the vulnerability of the system itself. For instance, software randomization [38–40] (classified as Shuffling/Software layer), a common MTD technique, does not eliminate the existence of vulnerabilities in software. Attackers are still capable of performing vulnerability attacks on specific targets through exploiting mining, buffer overflow, and other methods. We can expect that, with software randomization, different users have different binary codes and, thus, cannot perform attacks on other targets using the same approach.

Another example is instruction set randomization [43,44] (classified as Shuffling/Data layer). Although it can prevent attackers from inserting binary instructions into the target program to execute an attack successfully, the vulnerability of the target program is also not eliminated, and well-designed worms and viruses can still break through the defense of instruction set randomization.

Therefore, we need to clarify the idea that in order to achieve a genuine defense winning, MTD must be integrated with existing security defense mechanisms. Existing network security defenses such as firewalls, intrusion detection systems, and anti-virus systems have been deployed in the network with network topology and a configuration that is relatively

fixed, while introducing MTD into them changes the existing network configuration, thus potentially leading to increased resource consumption, reduced network availability, and possible mutual interference with existing network security defense techniques.

We believe that MTD must be implemented appropriately without affecting existing network operations and must adapt to existing network infrastructure, network services, and network protocols. The development trend of MTD needs to integrate better with existing network security protection technology and be embedded better into the existing network.

2.3.3. Combination with New Techniques

How to maintain the vitality of MTD is our concern, and we believe that as a defense framework concept rather than a defense mechanism that needs to be built from scratch, MTD can be very compatible with emerging techniques. We attach great importance to the combination of MTD with new techniques, which is also why we conducted this survey: we are concerned about how MTD is progressing further down the road of new techniques, especially machine learning.

Undoubtedly, the future of MTD is not just about machine learning. We have noticed that MTD has been combined with many other types of emerging techniques to achieve better active defense effects, such as:

- SDN-based MTD

MTD tends to change the existing network configuration and, therefore, usually causes the degradation of network service availability. For example, while IP address hopping can interfere with attackers' scanning and intrusion to some extent, it may cause the failure of the entire network communication, whereas a software-defined network (SDN) can fundamentally change the network structure, giving the central controller the ability to regulate the entire network globally [49]. Therefore, IP address hopping in SDN [50] could minimize the impact of moving target defense techniques on the entire network.

- MTD-applied cloud computing

Cloud computing has been widely adopted to process massive traffic data. Many large data centers have utilized cloud computing to provide convenient services due to highly centralized data and services, which is precisely the reason why cloud services are in demand of high-level defense mechanisms to protect these highly centralized data and services. Favorably, the combination of MTD with cloud computing outstandingly improves the proactive defense capability of cloud servers [51] and ensures the security of cloud services [52].

2.3.4. Challenges for Existing MTD Techniques

Based on our survey, we identified several issues that require improvement in some existing MTD techniques, including:

- Large resource consumption and high defense costs (we have highlighted this issue several times during the introduction of SDR).
- For example, in the face of the attacker's scanning, the existing MTD's countermeasure is to perform IP hopping when scanning behavior is detected, and their representative techniques include but are not limited to OF-RHM [11], SEHT [12], DDS [13], and NATD [14]. Their common problem is a lack of accuracy and efficiency in identifying attack manners, the waste of resources caused by untargeted hops, and a lack of integration with the affordable defense pursued by MTD.
- They have an incapability of balancing multi-constraints (e.g., costs, security performance, and service availability).
- For instance, routing randomization has been proven to be an effective method against eavesdropping attacks. Currently, representative routing randomization techniques include but are not limited to: RRM [53], AE-RRM [50], AT-RRM [54], and SSO-RM [55]. However, RRM and AE-RRM implement random transformations only on the routes

of data transmission between nodes, without considering different attack behaviors and protecting network QoS under such circumstances. As for AT-RRM and SSO-RM, they can dynamically adjust transformation strategies to some extent, but their protection effectiveness for QoS is still unsatisfactory, and they fail to consider the varying demands of different applications for latency and bandwidth. Besides, all of their packets' granularity is too coarse, making it easy for attackers to intercept continuous data packets and render the defense ineffective.

- Relatively fixed defense strategies (easy to be reconnoitered and recognized by attackers).

An example is the ASLR [56] deployed in Unix systems. It performs well in defending against buffer overflow vulnerabilities by randomly selecting the base address of the stack at runtime. This means that the location of each variable in memory is uncertain, making it difficult for attackers to exploit these vulnerabilities. However, ASLR is vulnerable to BROP attacks [57], which can exploit the fact that the parent process retains the same address space layout when forking a child's process. This example illustrates that fixed defense strategies are vulnerable to countermeasures applied by attackers. Therefore, there is no easy way for MTD to achieve long-term defense success.

Although MTD is confronted with many challenges, its idea that transitioning from passiveness to activeness and affordable defense is the future trend of cyber security means it has broad application prospects in many fields. With the help of machine learning, MTD research has met a brave new world. In Section 3, we introduce the intelligent MTD techniques and how these three problems are improved (and demonstrate specific feasible solutions to the three examples mentioned above).

3. Intelligent MTD Techniques

3.1. Background

As we have mentioned above, MTD gradually reveals its shortcomings and deficiencies in the continuous development of both cyber-attack and defense, and existing MTD cannot undertake a plethora of defense tasks satisfactorily.

With an improvement in computer hardware and the advent of the big data era, machine learning theories and techniques [58,59] are becoming increasingly heated, and their application areas are expanding. Machine learning-related techniques have demonstrated excellent processing capabilities for complex, massive, and high-dimension data in many tasks and have shown more accurate and collegiate performance in many complex problems compared to traditional decision-making methods, which makes machine learning considered a strategic technology, leading a new round of technological and industrial revolutions.

Thereby, MTD, based on machine learning, enables systems to capture evolving attack patterns with high scalability and applicability. However, since machine learning requires a large amount of data for training to ensure a certain level of prediction accuracy, insufficient data can result in reduced performance despite high levels of overhead and complexity. Moreover, it is of great importance to ensure that sufficient computational power is available in the environment where MTD is deployed, as resource-constrained environments may be unable to afford it.

3.2. Intelligent MTD Techniques

It has been found that machine learning algorithms can be considered in terms of affordability and other aspects to diminish the shortcomings of existing MTD techniques or help existing MTD systems set up better protection mechanisms. As mentioned in Section 2.3.4, machine learning can help accomplish three challenges of MTD (in red points) as mentioned above (in blue points) (Table 4):

Table 4. Challenges of MTD and accomplishments of machine learning.

• Large resource consumption and high defense costs • The incapability of balancing multi-constraints • Relatively fixed defense strategies		• Towards affordable • Towards optimized • Towards self-adaptive

Instead of applying the classification method of SDR/Five layers, we decided to expand the above three points to introduce intelligent MTD techniques. We did not introduce intelligent MTD techniques in the traditional way mainly out of two considerations. Firstly, we are more interested in exploring how machine learning algorithms can help address the problems that arise from existing MTD approaches: as such, a recapitulation owns more practicability and usefulness (Table 5). Secondly, the development of intelligent MTD techniques is uneven across all levels of the five layers [9]. Hence, it is not a favorable way to categorize intelligent MTD techniques according to SDR/Five layers for the introduction.

Table 5. Common machine learning algorithms applied for intelligent MTD techniques.

Towards affordable	CNN [19]	DL [39]	RL [34]
Towards optimized	RL [60–68]		
Towards self-adaptive	DL [69]	CNN [19]	Neuro-evolution [14]
	Clustering [48]	RL [36]	RNN [70]

3.2.1. Towards Affordable

One of the primary goals of MTD is to provide an affordable defense. This refers to reducing resource costs in deploying the techniques, which includes both deployment costs and system overhead. Deployment cost determines the economic threshold for users to adopt the technology, while system overhead affects the QoS and users' experience of the deployed system.

Currently, MTD techniques pursue high-precision and high-accuracy security defense effectiveness, which requires a substantial increase in data samples. Processing these data requires better hardware support, resulting in high-intensity hardware dependency and difficulties in promoting applications. On top of that, the deployment of MTD inevitably occupies storage and computational resources, especially self-adaptive MTD, which requires collecting data samples for sensing attacks and, thus, occupying network channel resources.

In this way, how to reduce the deployment cost and system overhead has become one of the most pressing issues in the development of MTD. The use of machine learning algorithms, such as Neural Network Compression [71], to reduce resource costs has been achieved in other areas, such as data processing [72], image recognition [73], and speech recognition [74], which can efficiently process large amounts of data and retain key features to improve computational efficiency [75,76]. Drawing on this, an increasing number of MTD techniques have started to utilize machine learning algorithms to improve defense performance while reducing resource costs.

After recapitulation, we found that the existing intelligent MTD came *towards affordable* for defense mainly from the following points:

- New MTD methods are designed to reduce the high overhead of existing methods

Vikram et al. [39] found that the CAPTCHA approach traditionally used to defend against web bot attacks such as XRumer, Magic Submitter, and SENuke generates a significant system overhead and reduces system availability. To address this, they designed a new MTD technique that intelligently randomized HTML elements to counter web bot attacks without affecting normal users. After analysis, they categorized the system overhead into page load time (PLT) and page size. To reduce the system overhead, they designed

an intelligent randomization algorithm to ensure that only a small number of characters needed to be added from the original string for each element, which ensured that the PLT increase overhead was less than 0.2 s in all cases, and the average page size increase was only 0.103 KB. This technique was evaluated to prevent all web bot attacks successfully with relatively low overhead while ensuring users' experience and system QoS.

As a feasible solution to the IP hopping issue proposed in Section 2.3.4. Xu et al. [19] proposed a CNN-based adaptive IP hopping approach to defending against scanning attacks. To achieve lightweight defense, they first compressed the CNN detector deployed in the control plane using deep compression techniques to reduce its storage and computational resource usage, improve its forward computational efficiency, and release its dependence on GPU computation cards in its usage phase. Second, they changed the attack-aware data samples from network data streams to stream table data to reduce the network channel resource occupation. Experiments showed that the hopping frequency of their proposed method was lower than other methods [11–14,77], significantly reducing the system overhead.

- Methods are designed to minimize the additional overhead when triggering MTD

Wang et al. [68] proposed an MTD approach for minimizing long-term system costs for DDoS attacks and covert channel attacks. The authors argued that MTD imposes an overhead on currently running applications in the system when dynamically shifting the attack surface; therefore, determining the optimal triggering time for MTD can minimize this additional overhead. The authors modeled this problem as an update reward process in reinforcement learning and proposed an optimal algorithm to determine the correct time to trigger MTD and avoid the additional burden of invalid triggering, thus minimizing long-term cost rates.

Designing an inappropriate interval to trigger MTD cannot afford to balance system security and system overhead, so the trend in intelligent MTD development is *towards self-adaptive*. Our investigation shows that most self-adaptive MTD has achieved better results in reducing the additional overhead when triggering MTD.

It should be noted that the techniques we listed were optimized regarding system overhead, so we could assume that, in the future, self-adaptive MTD techniques are also likely to address affordability.

3.2.2. Towards Optimized

Towards optimization is about finding the most effective and counter-measurable defense for a defense system, given multiple conditional constraints, which include the attacker's possible attack behavior, the system's security, the system's overhead, the system's QoS, the users' experience, etc. The current popular technique is to use machine learning to find the best defense strategy solution for the MTD system facing a known attacker.

Developing and evaluating cyber-attack and defense game strategies is a hot research topic. To maximize the impact of MTD, defenders must strategically choose when and what changes to make while considering their systems' characteristics and the activities observed by adversaries. Finding the best strategy for MTD is a significant challenge, especially when facing resourceful and determined adversaries who can react to defenders' actions. The game-theoretic approaches [10], such as the classical game model (static game, signal game), Markov game model, differential game model, and evolutionary game model, can be used to extend MTD techniques due to their flexibility in problem formulations to reflect various scenarios in most domains.

Reinforcement learning is a good match for this. Reinforcement learning [78] is a learning process in which the learner must discover which actions yield the most lucrative payoffs without being told what action to take under incomplete information conditions. This process is beneficial for assisting cyber attackers and defenders in playing and choosing the optimal strategy.

The study of generalized optimal strategy-solving methods revolves around the following procedures:

1. To clarify the attackers' and defenders' knowledge about each other and to build a game model (such as the Stackelberg game based on incomplete information and a zero-sum game or a general-sum game according to the actual situation);
2. To consider different reinforcement learning practical scenarios that can be applied to advance the game process and reach game equilibrium finally, e.g., Bayesian-Stackelberg equilibrium;
3. To select the most efficient sets of strategies and consider them as optimized strategies for the MTD system (as shown in Figure 5).

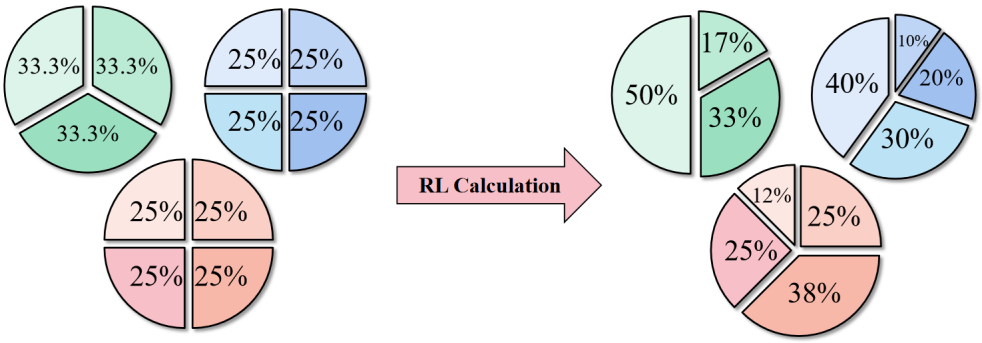

Figure 5. Diagram of optimization for multi-MTD methods.

In the actual game of cyber-attack and defense, we need to take many factors [79] into consideration, including but not limited to the following factors shown in Table 6:

Table 6. Factors commonly considered in GT-MTD.

Factors	Explanations
Actual participants	Is there only one attacker and one defender? Realistic situations are likely to face multiple agents.
Rationality profile	Perfect rationality or bounded rationality.
Environment	The environment includes knowledge about the opponent. In most cases, the attacker has the advantage in this respect and has much more incomplete information about the defender.
Play order	In most cases, the order is leader-follower (Stackelberg game), but there are also cases where cards can be played simultaneously, depending on the actual situation.
Available strategies	We cannot exhaust all possible types of attacks in the same game, nor can we deploy all possible MTD mechanisms in the same system.
Revenue measurement	For the defender, the revenue design is more complex, including but not limited to system security, system overhead, system QoS, and users' experience.

We show the development of research in intelligent MTD solutions step by step with examples of research results in recent years, and summarize them in Table 7.

- Defensive strategy solutions considering specific types of attacks

In the first place, we focused on strategic solutions for specific attacks.

As a feasible solution to the routing randomization issue proposed in Section 2.3.4, Xu et al. [27] introduced the Deep Deterministic Policy Gradient (DDPG), a deep reinforcement learning algorithm, into routing randomization against eavesdropping attacks. With the superior performance of DDPG in learning from complex environments and high-dimensional data, they generated randomized routing schemes that met both security and

QoS requirements based on real-time network states. Additionally, they utilized a P4 network architecture to deploy randomized routing schemes and achieved finer packet-level granularity for randomized routing.

Zhu et al. [62] proposed two iterative reinforcement learning algorithms to determine an ideal defense strategy against heart bleed attacks, especially when the information about the attacker is unknown or limited. They used Markov chains and stochastic stability in their algorithms by introducing adaptive, robust reinforcement learning capabilities. They showed that their approach could provide near-optimal defense strategies.

How can the defense be adjusted if the attacker's strategy keeps changing? Furthermore, how can the system security and system performance be balanced with limited system resources? Gao et al. in [63] established a cyber-attack and defense game model for specific DDoS attacks and proposed an adaptive strategy for MTD, which adaptively adjusted the defense strategy according to changes in environmental conditions. It also balanced system security and system performance by adjusting parameters to adapt to changes in environmental conditions.

Similarly, Anshuman et al. [64] focused on adversarial machine-learning attacks. Adversarial machine learning has become the latest threat in speech recognition and image recognition, which is becoming accessible to people in their daily lives. The authors proposed a moving target defense approach to defending against adversarial machine learning, but instead of proposing a machine learning algorithm to counter such adversarial algorithms, they proposed a switching scheme between machine learning algorithms to defend against adversarial attacks, which is derived from the Stackelberg equilibrium of the game.

Farchi et al. [67] proposed a strategic selection method based on a machine learning algorithm to defend against adversarial machine learning. They helped the defender implement multiple learners using a game-theoretic approach, which learned and computed the policy space separately and applied possible dominant policies accordingly. Otherwise, it applied Nash-stable policies to solve the optimal policy finally. Through practical applications, the authors concluded that the method could reduce the effectiveness of adversarial attacks on machine learning attacks.

- Defensive strategy solutions considering generalized types of attacks

Next, let us consider generalized attack defense types, i.e., we are vaguer about the specific attack and defense methods and focus further on how to enhance this simulation game to be more generalized for application in the face of real situations [80].

Tozer et al. [66] proposed a multi-objective reinforcement learning algorithm to minimize the attack surface of the system, mainly including the components, interfaces, and communication channels of the system. The configuration diversity was obtained by solving the optimal policy. They designed a system to generate a multi-objective Markov decision process, used three different multi-objective reinforcement learning algorithms to learn a set of optimal policies, and compared the resultant benefits, concluding that the multi-objective time-difference post-state algorithm could obtain optimal solutions.

Huang et al. [65] mentioned that in a multi-stage MTD game, both the attacker and the defender can use reinforcement feedback learning to attack through the risk assessment of the attack, system configuration, and adjustment of the system configuration leading to a shift in the attack surface, thus continuing to influence the risk assessment results and reaching a cycle until equilibrium. The point of reaching equilibrium is that neither the attacker nor the defender can further enhance their gains by picking other actions. This iterative convergence process from evaluation to policy adjustment is called generalized policy iteration and is a common policy solution in reinforcement learning dynamic planning.

As can be seen, the above study has not yet considered the order of play between the defender and the network adversary and is simply understood as a general simultaneous play situation. However, this is inconsistent with most actual cyber-attack and defense situations. Usually, leader-follower games are the common way of cyber-attack and defense games. In addition, the author's dismissal of incomplete information about rational

adversaries makes the whole theory out of practice, but we must admit that all practice requires the continuous evolution of the theory to be successful.

Taha Eghtesad et al. [60] proposed a multi-intelligent partially observable MTD Markov decision process model and formulated a two-person general sum game between the adversary and the defender. Based on the established adaptive MTD model, the authors proposed a multi-intelligent reinforcement learning framework based on a dual-prophecy machine algorithm to guarantee the convergence of strategies for both attackers and defenders to solve the game problem.

Sailik Sengupta et al. [61] proposed to model MTD as a leader-follower game between a multi-intelligent defender and a networked adversary by designing a Bayesian Stackelberg Markov game model that could model the uncertainty of attacker types and the nuances of the MTD system. On the algorithmic side, the authors applied the Bayesian Strong Stackelberg Q-learning method: an algorithm that learns the best movement strategy for the BSMG in a reasonable amount of time through interactions. We can learn that the latest intelligent MTD solutions have converged the best strategies in incomplete information.

Table 7. Our survey on recent MTD optimization research.

Ref.	RL Method	Attack	Participants	Rationality	Environment	Order
Zhu et al. [62]	Iterative RL	Heart bleed	Single-agent	Perfect	Unknown/Incomplete	Stackelberg
Gao et al. [63]	Basic RL	DDoS	Single-agent	Perfect	Known	-
Anshuman et al. [64]	-	Adversarial attacks	Single-agent	Perfect	Known	Stackelberg
Xu et al. [27]	DDPG	Eavesdropping attacks	Single-agent	Perfect	Known	-
Farchi et al. [67]	Multi-learner RL	Adversarial attacks	Multi-agent	Perfect	Known	Stackelberg
Tozer et al. [66]	Multi-object RL	GENERALIZED	Multi-agent	Perfect	Known	-
Huang et al. [65]	RLHF	GENERALIZED	Single agent	Perfect	Partially observable	-
Taha et al. [60]	Double oracle	GENERALIZED	Multi-agent	Bounded	Partially observable	Stackelberg
Sengupta et al. [61]	Q-Learning	GENERALIZED	Multi-agent	Bounded	Unknown/Incomplete	Bayesian Stackelberg

3.2.3. Towards Self-Adaptive

Next, we present intelligent MTD techniques *towards self-adaptive* in two ways. Summary has been shown in Table 8.

The first is when it is appropriate to trigger MTD. If the triggering time interval is fixed, we need to consider: if the triggering time interval is too long if the attacker has enough time to penetrate the system and launch an attack; if the interval is too short, if the MTD mechanism will be triggered frequently, which wastes resources and reduce performance, and significantly reduces QoS. Therefore, ad hoc event triggering is preferred.

Secondly, in the face of various attacks, how can we use relatively fixed defense strategies to counteract them? How can we determine which defense strategy is most effective in defending against these attacks? Relatively fixed defense strategies are easily recognized by attackers, while attack strategies change rapidly. Therefore, the way to trigger fixed defense strategies cannot keep up with evolving attack methods.

We note that various MTD techniques have been developed in the direction *towards self-adaptive*, i.e., the defense system can automatically adapt to the behavioral characteristics of the attacker and adjust defense strategy according to the behavioral characteristics of the attack, configure transformation information, and trigger transformation actions in a targeted manner. We can understand that most of the self-adaptive MTD techniques should ensure affordability and optimization.

Since self-adaptive MTD techniques require deploying a sensing engine to sense the attack behavior and the constant collection of data samples used to sense the attack, equipping machine learning algorithms to construct a sensing engine is a mainstream approach for researchers designing self-adaptive MTD techniques. After investigation, we found that existing intelligent MTD techniques are mainly self-adaptive from the following points.

- Self-adaptation empowered by machine learning

Song et al. [69] proposed a self-adaptive MTD that could generate multiple new models in depth after deployment to detect and defend against adversarial examples collaboratively. Post-deployment quasi-secret deep models proposed in this paper significantly increased the bar for attackers constructing compelling adversarial examples. They also applied serial data fusion with an early stopping technique in order to reduce the inference time by up to five times while maintaining sensing and defense performance.

In Section 3.2.1, we presented how Xu et al. [19] proposed an adaptive IP hopping approach that not only performed a lightweight implementation in terms of system cost but also accomplished the adaptive processing of attacks. Their approach consists of a lightweight Convolutional Neural Network detector composed of three convolutional modules and a judgment module to sense scanning attacks and provide a CNN-based three-stage jumping strategy to achieve self-adaptation, which allows the MTD system to optimize its behavior in real-time according to the attacks.

- Self-adaptation empowered by machine learning with legacy defense mechanisms

As a feasible solution to the relatively fixed defense strategies issue proposed in Section 2.3.4. Smith et al. [14] held the belief that although used as a defense mechanism, untimely triggered MTD could also be disruptive to ordinary users. For example, when IP addresses were dynamically changed, IP address resolution using DNS caching before performing any communication was no longer effective. The authors noted that MTD deployment could be triggered by using lightweight intrusion detection, which they proposed to use as an intrusion detection mechanism to help MTD become adaptive. They proposed an approach called the Neuro-evolution of Augmented Topologies, which generated sparse topologies by building packet-based detectors that could manipulate topologies in real time to accomplish the self-adaptive functionality.

Fraunholz et al. [48] proposed a machine learning-based approach for dynamic honeypot configuration, deployment, and maintenance. By identifying network entities (machines and devices), these entities were further analyzed and clustered, and finally, honeypots were intelligently deployed in the network based on the clustering. Through machine learning, the honeypot system it deployed owned two characteristics: first, it was hybrid, i.e., low-interaction honeypots and high-interaction honeypots were deployed in a mixed manner, with low-interaction honeypots responsible for redirecting attack traffic to high-interaction honeypots and high-interaction honeypots emulating operating systems and network services; second, it was adaptive, i.e., the system could intelligently record and analyze intruder activities and take measures to protect the network based on analysis results. These honeypots did not require configuration and maintenance and were, therefore, a significant advantage of honeypot technology in modern network security.

- Self-adaptation empowered by machine learning with game theories

Colbaugh et al. [36] proposed a self-adaptive MTD technique aimed at mitigating the ability of the adversary to understand defense mechanisms. They modeled the adversary's adaptability through the learner's feature space to make adversarial predictions and trigger self-adaptive MTD. These methods are based on game theory and machine learning and are applicable to problems of practical size and complexity. They also utilized reinforcement learning [81] to model the co-evolutionary relationship between attackers and defenders to derive optimal defense strategies for MTD that are difficult to reverse.

Sengupta et al. [70] proposed a self-adaptive MTD method MTDeep, which focused on adversarial attacks on DNNs. In MTDeep, the input images are randomly classified, and a network is selected from a collection of networks based on a policy generated through game-theoretic reasoning. The interaction between image classification systems can be modeled as a repeated Bayesian game using MTDeep (i.e., the set of DNNs) and its users (i.e., adversarial and legitimate). The configuration space of the defenders is the set of DNNs that are trained for the same task but are not affected by the same attacks. The Stackelberg equilibrium of the game provides the optimal switching strategy for MTDeep to

reduce the adversarial modification of images leading to misclassification and guaranteeing the high classification accuracy of the system.

Table 8. Our survey on recent MTD self-adaptation researches.

Ref.	ML Method	Taxonomy	Affordability	Optimization
Song et al. [69]	DL	ML-based	-	√
Xu et al. [19]	CNN		√	√
Smith et al. [14]	Neuro-evolution	ML + defense mechanism-based	√	-
Fraunholz et al. [48]	Clustering		-	√
Colbaugh et al. [36]	RL	ML + GT-based	-	√
Sengupta et al. [70]	DNN		-	√

3.3. Discussion

Machine learning-based MTD allows systems to capture evolving attack patterns with high scalability and applicability and has become the mainstream research direction for current MTD techniques. With the guideline of complementing the shortcomings of traditional MTD techniques, we divided the research direction of intelligent MTD into three major points: *towards affordable*, *towards optimized*, and *towards self-adaptive*. Among them, towards self-adaptive is the most advanced and effective technology orientation for MTD and shares the features of towards affordable and towards optimized. Combined with the survey, we demonstrated the following main points with Table 9.

- When introducing machine learning to address existing MTD problems, it is important to ensure the two fit together seamlessly. Achieving optimal results requires a rigorous validation process. Machine learning often requires large amounts of data for training, which can introduce additional overhead and complexity. In addition, many machine learning algorithms rely on high-performance GPU computing cards and occupy significant storage space. In addition, inefficient machine learning algorithms can also pose processing efficiency issues, so sufficient computing power must be provided in the environment where MTD is deployed.
- In addition, existing intelligent MTD research has focused on optimized solutions that specify attack defense types, and these have shown promising results in real-world cyber-attack and defense scenarios. However, they are only applicable to specific scenarios and may be limited in practical situations where attack defense types change rapidly. In contrast, generalized attack types can model the real world more closely and take more factors into account. However, when information about rational adversaries is incomplete, these models may yield sub-optimal strategies in sequential settings. Furthermore, existing efforts to learn defense policies in sequential settings are either unpopular or neglect the strategic nature of the adversary due to scalability issues caused by incomplete information.
- At last, self-adaptive MTD solves various problems caused by manual decision-making regarding MTD trigger intervals and balances security and resource costs. It can also extract features for optimal defense strategy selection in the face of new attack methods. However, the design of the engine for sensing attack behavior and analyzing attack features is complicated. The continuous collection of data samples is required to sense attacks, and the adaptive effect heavily depends on the algorithm and sensing engine.

Table 9. Summary of intelligent MTD techniques.

	Towards Affordable	Towards Optimized	Towards Self-Adaptive
Main ideas	• To reduce the high overhead of legacy methods • To minimize the additional triggering of overhead	• Solutions considering specific types of attacks • Solutions considering generalized types of attacks	• ML • ML + defense mechanisms • ML + GT
Merits and demerits	• Efficaciously processing large data to improve defense efficiency • Rendering additional overhead and inefficient algorithms can also cause problems in processing efficiency	• Helping defenders respond to attacks with optimal defense strategies • Easy-to-generate sub-optimal strategies in solution	• Balancing security and resource costs to respond to attacks with optimized defense strategies • Sophisticated sesing and analysis of attack behavior and traits
Challenges	• To minimize the additional overhead from ML • To increase the computational power of ML algorithms	• Scalability problems considering incomplete information in real cases	• Necessary to ensure the high-level capability of sensing attacks

4. Conclusions

4.1. Empirical Insights

- MTD aims to enhance security by shifting the attack surface rather than eliminating all vulnerabilities in system components. This represents a departure from traditional security goals, which have focused on eliminating vulnerabilities entirely. With the addition of machine learning, MTD can provide an affordable, optimized, and self-adaptive defense mechanism that enhances system security without requiring the replacement of existing techniques. By actively guiding this development trend, we can further balance the relationship between defense costs, system security, and system availability in multiple dimensions, enabling MTD to move toward large-scale applications.
- Defense measures are not mutually exclusive, and MTD is actively seeking to integrate with existing security defense mechanisms. However, it is crucial to consider how introducing MTD may alter the existing network configuration, which is often relatively fixed when existing network security defense measures are in place. This change can increase resource consumption, reduce network availability, and potentially interfere with existing network security defenses, ultimately reducing overall defense capability.
- To leverage existing techniques and maximize the effectiveness and efficiency of MTD, it is significant to combine MTD with other emerging techniques such as SDN, cloud computing, and machine learning to achieve better active defense. By using different types of MTD that can be tailored to specific application domains, we can enhance the overall defense capability of MTD.
- While game-theoretic MTD approaches are commonly utilized in MTD strategy selection research, the emergence of machine learning has shown that relevant algorithms can be considered to address the affordability, self-adaptation, and other limitations of existing MTD techniques [82]. Machine learning can also help construct better protection mechanisms for existing MTD systems.
- In our survey, we did not present MTD techniques measurement metrics due to our focus on MTD and intelligent development, but this does not mean that measurement metrics are unimportant. Many MTD techniques have applied MTD-related metrics to assess the effectiveness of their own techniques. Unfortunately, these evaluation metrics differ among different MTDs, making it difficult to integrate various techniques effectively. Several quantitative metrics have been proposed to assist in uniformly assessing MTD techniques, but they have only had limited success. We believe that researchers should continue striving to develop a universal metric that covers all

aspects of cyber-attacks and defense to facilitate the convergence of MTD techniques as much as possible.

4.2. Future Research

- We propose the establishment of a more comprehensive coverage of MTD classifications in future work. In our survey, we introduced the SDR/Five layers MTD classification by what to move and how to move, but we did not combine it with when to move to cover more comprehensive MTD techniques. It is necessary to develop a classification that can comprehensively include multidimensional MTD attributes to help researchers better understand and develop MTD techniques.
- Security, performability, and affordability are important indicators when measuring the effectiveness of MTD techniques. While MTD improves system security, it may also hinder service availability to average users. In future research, we suggest exploring finer granularity to develop affordable MTD solutions that meet the average users' needs. Notably, most existing MTD approaches do not provide highly lightweight distributed solutions. Therefore, we recommend building more lightweight MTD techniques in the future to enable the higher widespread deployment and application of MTDs.
- Comprehending the attacker's behavior or system security situation is crucial in enabling defenders to make optimal decisions. However, there are many factors to consider for practical application, and extrapolation can easily lead to sub-optimal strategies. To address this, MTD should explore a wider range of practical scenarios with reinforcement learning to help defenders solve more difficult adversaries.
- We believe that the concepts and techniques of self-adaptive MTD are not yet mature, and therefore, more self-adaptive MTD mechanisms need to be developed. In terms of triggering MTD operations, we need to balance the bi-directional costs of triggering and security by considering factors such as system vulnerability or attack pattern/strength. This requires advanced detection or learning capabilities from defenders.
- The advancement of intelligent MTD techniques cannot be achieved without the support of big data and high-performance hardware. Therefore, future intelligent MTD researchers should consider constructing larger sample datasets and forming systematic sample databases for training machine learning algorithms and improving accuracy and generalization ability. Using hardware devices with higher computing performance can also enhance training efficiency and the real-time decision-making of MTD.
- Deceptive defense [83] ideas have emerged in recent years, and combining deceptive defense methods with MTD could be a future research trend. There is already a trend of combining deceptive defense with intelligence [81], where deceptive defense provides misleading information by actively exposing false intelligence of the protected system, thus allowing the attacker to move the attack in the direction of favoring the defender by actively creating and reinforcing the observation and identification of deceptive information.

Author Contributions: Conceptualization, R.S. and Y.Z.; methodology, R.S. and J.F.; investigation, R.S. and X.C.; writing—original draft preparation, R.S.; writing—review and editing, R.S., Y.Z. and J.F.; supervision, J.F.; funding acquisition, J.F. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is supported by the Key JCJQ Program of China, grant number 2020-JCJQ-ZD-021-00 and 2020-JCJQ-ZD-024-12. The authors would like to acknowledge them.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: No new data were created.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bland, J.A.; Petty, M.D.; Whitaker, T.S.; Maxwell, K.P.; Cantrell, W.A. Machine learning cyberattack and defense strategies. *Comput. Secur.* **2020**, *92*, 101738. [CrossRef]
2. Wee, B.V.; Banister, D. How to Write a Literature Review Paper? *Transport. Rev.* **2016**, *36*, 278–288. [CrossRef]
3. Okhravi, H.; Rabe, M.; Leonard, W.; Hobson, T.; Bigelow; Streilein, W. *Survey of Cyber Moving Targets*; Technical Report, 1166; MIT Lincoln Laboratory: Lexington, MA, USA, 2013.
4. Ward, B.; Gomez, S.; Skowyra, R.; Bigelow, D.; Martin, J.; Okhravi, H. *Survey of Cyber Moving Targets*, 2nd ed.; Technical Report, 1228; MIT Lincoln Laboratory: Lexington, MA, USA, 2018.
5. Cai, G.L.; Wang, B.S.; Hu, W.; Wang, T.Z. Moving target defense: State of the art and characteristics. *Front. Inf. Technol. Electron. Eng.* **2016**, *17*, 1122–1153. [CrossRef]
6. Lei, C.; Zhang, H.-Q.; Tan, J.-L.; Zhang, Y.-C.; Liu, X.-H. Moving target defense techniques: A survey. *Secur. Commun. Netw.* **2018**, 3759626. [CrossRef]
7. Zheng, J.; Namin, A.S. A survey on the moving target defense strategies: An architectural perspective. *J. Comput. Sci. Technol.* **2019**, *34*, 207–233. [CrossRef]
8. Sengupta, S.; Chowdhary, A.; Sabur, A.; Huang, D.; Alshamrani, A.; Kambhampati, S. A survey of moving target defenses for network security. *arXiv* **2019**, arXiv:1905.00964. [CrossRef]
9. Cho, J.-H.; Yoon, S.; Kim, D.S. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 709–745. [CrossRef]
10. Sun, Y.; Ji, W.; Weng, J.; Zhao, B. Overview on MTD based on game theory. *MATEC Web Conf.* **2020**, *309*, 02012. [CrossRef]
11. Jafarian, J.H.; Al-Shaer, E.; Duan, Q. 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, New York, NY, USA, 13 August 2012; pp. 127–132.
12. Lei, C.; Zhang, H.; Ma, D.; Yang, Y. Network Moving Target Defense Technique Based on Self-Adaptive End-Point Hopping. *Arab. J. Sci. Eng.* **2017**, *42*, 3249–3262. [CrossRef]
13. Miao, L.; Hu, H.; Cheng, G. The Design and Implementation of a Dynamic IP Defense System Accelerated by Vector Packet Processing. In Proceedings of the International Conference on Industrial Control Network and System Engineering Research, New York, NY, USA, 15–16 March 2019; pp. 64–69.
14. Smith, R.J.; Zincir-Heywood, A.N.; Heywood, M.I.; Jacobs, J.T. Initiating a Moving Target Cyber Defense with a Real-Time Neuro-Evolutionary Detector. In Proceedings of the 2016 on Genetic and Evolutionary Computation Conference Companion, New York, NY, USA, 20–24 July 2016; pp. 1095–1102.
15. Al-Shaer, E.; Duan, Q.; Jafarian, J.H. Random host mutation for moving target defense. In *Security and Privacy in Communication Networks, 8th International ICST Conference, SecureComm 2012, Padua, Italy, 3–5 September 2012*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 106.
16. Antonatos, S.; Akritidis, P.; Markatos, E.P.; Anagnostakis, K.G. Defending against Hitlist Worms Using Network Address Space Randomization. In Proceedings of the 2005 ACM Workshop on Rapid Malcode, Computer Networks, New York, NY, USA, 11 November 2005; pp. 3471–3490.
17. Kewley, D.; Fink, R.; Lowry, J.; Dean, M. Dynamic Approaches to Thwart Adversary Intelligence Gathering. In Proceedings of the DARPA Information Survivability Conference and exposition II (DISCEX), Anaheim, CA, USA, 12–14 June 2001; Volume 1, pp. 176–185.
18. Sharma, D.P.; Kim, D.S.; Yoon, S.; Lim, H.; Cho, J.; Moore, T.J. FRVM: Flexible Random Virtual IP Multiplexing in Software-Defined Networks. In Proceedings of the IEEE TrustCom, New York, NY, USA, 1–3 August 2018; pp. 579–587.
19. Xu, X.; Hu, H.; Liu, Y.; Zhang, H.; Chang, D. An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector. *Secur. Commun. Netw.* **2021**, *2021*, 8848473. [CrossRef]
20. Luo, Y.B.; Wang, B.S.; Wang, X.F.; Hu, X.F.; Cai, G.L.; Sun, H. RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 263–270.
21. Carroll, T.E.; Crouse, M.; Fulp, E.W.; Berenhaut, K.S. Analysis of Network Address Shuffling as a Moving Target Defense. In Proceedings of the IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 701–706.
22. MacFarland, D.C.; Shue, C.A. The SDN shuffle: Creating a Moving-Target Defense Using Host-Based Software-Defined Networking. In Proceedings of the 2nd ACM Workshop on Moving Target Defense (MTD), Denver, CO, USA, 12 October 2015; pp. 37–41.
23. Kampanakis, P.; Perros, H.; Beyene, T. SDN-Based Solutions for Moving Target Defense Network Protection. In Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Sydney, NSW, Australia, 19 June 2014; pp. 1–6.
24. Achleitner, S.; Porta, T.L.; McDaniel, P.; Sugrim, S.; Krishnamurthy, S.V.; Chadha, R. Deceiving network reconnaissance using SDN-based virtual topologies. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 1098–1112. [CrossRef]

25. Achleitner, S.; La Porta, T.; McDaniel, P.; Sugrim, S.; Krishnamurthy, S.V.; Chadha, R. Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. In Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, New York, NY, USA, 28 October 2016; pp. 57–68.
26. Hong, J.B.; Yoon, S.; Lim, H.; Kim, D.S. Optimized Network Reconfiguration for Software Defined Networks Using Shuffle-Based Online MTD. In Proceedings of the IEEE Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 26–29 September 2017.
27. Xu, X.; Hu, H.; Liu, Y.; Tan, J.; Zhang, H.; Song, H. Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack. *Digit. Commun. Netw.* **2022**, *8*, 373–387. [CrossRef]
28. Trassare, S.T.; Beverly, R.; Alderson, D. A Technique for Network Topology Deception. In Proceedings of the MILCOM 2013—2013 IEEE Military Communications Conference, San Diego, CA, USA, 18–20 November 2013; pp. 1795–1800.
29. Hong, J.B.; Enoch, S.Y.; Kim, D.S.; Nhlabatsi, A.; Fetais, N.; Khan, K.M. Dynamic security metrics for measuring the effectiveness of moving target defense techniques. *Comput. Secur.* **2018**, *79*, 33–52. [CrossRef]
30. Danev, B.; Masti, R.; Karame, G.; Capkun, S. Enabling Secure VM-vTPM Migration in Private Clouds. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC), New York, NY, USA, 5–9 December 2011; pp. 187–196.
31. Zhang, Y.; Li, M.; Bai, K.; Yu, M.; Zang, W. Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds. In Proceedings of the IFIP International Information Security Conference, Heraklion, Greece, 4–6 June 2012; pp. 388–399.
32. Penner, T.; Guirguis, M. Combating the Bandits in the Cloud: A Moving Target Defense Approach. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 14–17 May 2017; pp. 411–420.
33. Peng, W.; Li, F.; Huang, C.-T.; Zou, X. A Moving Target Defense Strategy for Cloud-Based Services with Heterogeneous and Dynamic Attack Surfaces. In Proceedings of the IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 804–809.
34. Jia, Q.; Sun, K.; Stavrou, A. Motag: Moving Target Defense against Internet Denial of Service Attacks. In Proceedings of the 22nd International Conference on Computer Communications and Networks (ICCCN), Nassau, Bahamas, 30 July–2 August 2013; pp. 1–9.
35. Thompson, M.; Evans, N.; Kisekka, V. Multiple OS Rotational Environment an Implemented Moving Target Defense. In Proceedings of the 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 August 2014; pp. 1–6.
36. Colbaugh, R.; Glass, K. Predictability-Oriented Defense against Adaptive Adversaries. In Proceedings of the 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, Republic of Korea, 14–17 October 2012; pp. 2721–2727.
37. Huang, Y.; Ghosh, A.K.; Bracewell, T.; Mastropietro, B. A Security Evaluation of a Novel Resilient Web Serving Architecture: Lessons Learned Through Industry/Academia Collaboration. In Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Chicago, IL, USA, 28 June–1 July 2010; pp. 188–193.
38. Jackson, T.; Salamat, B.; Homescu, A.; Manivannan, K.; Wagner, G.; Gal, A.; Brunthaler, S.; Wimmer, C.; Franz, M. Compiler-generated software diversity. In *Moving Target Defense*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 77–98.
39. Vikram, S.; Yang, C.; Gu, G. Nomad: Towards Nonintrusive Moving-Target Defense against Web Bots. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, 14–16 October 2013; pp. 55–63.
40. Casola, V.; Benedictis, A.D.; Albanese, M. A Moving Target Defense Approach for Protecting Resource-Constrained Distributed Devices. In Proceedings of the IEEE 14th International Conference on Information Reuse Integration (IRI), San Francisco, CA, USA, 14–16 August 2013; pp. 22–29.
41. Yuan, E.; Malek, S.; Schmerl, B.; Garlan, D.; Gennari, J. Architecture-Based Self-Protecting Software Systems. In Proceedings of the 9th International ACM SIGSOFT Conference on Quality of Software Architectures, New York, NY, USA, 17–21 June 2013; pp. 33–42.
42. Larsen, P.; Homescu, A.; Brunthaler, S.; Franz, M. SoK: Automated Software Diversity. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 276–291.
43. Kc, G.S.; Keromytis, A.D.; Prevelakis, V. Countering Code-Injection Attacks with Instruction-Set Randomization. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), New York, NY, USA, 27–30 October 2003; pp. 272–280.
44. Portokalidis, G.; Keromytis, A.D. Global ISR: Toward a Comprehensive Defense against Unauthorized Code Execution. In *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*; Springer: New York, NY, USA, 2011; pp. 49–76.
45. Azab, M.; Hassan, R.; Eltoweissy, M. Chameleonsoft: A Moving Target Defense System. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, FL, USA, 15–18 October 2011; pp. 241–250.
46. Kohli, T. An Efficient Threat Detection Framework for Docker Containers using AppArmor Profile and Clair Vulnerability Scanning Tool. Master's Thesis, National College of Ireland, Dublin, Ireland, 2022.
47. Okhravi, H.; Comella, A.; Robinson, E.; Haines, J. Creating a cyber moving target for critical infrastructure applications using platform diversity. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 30–39. [CrossRef]
48. Fraunholz, D.; Zimmermann, M.; Schotten, H.D. An Adaptive Honeypot Configuration, Deployment and Maintenance Strategy. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 19–22 February 2017; pp. 53–57.

49. Debroy, S.; Calyam, P.; Nguyen, M.; Neupane, R.L.; Mukherjee, B.; Eeralla, A.K.; Salah, K. Frequency-minimal utility-maximal moving target defense against DDoS in SDN-based systems. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 890–903. [CrossRef]
50. Aseeri, A.; Netjinda, N.; Hewett, R. Alleviating Eavesdropping Attacks in Software-Defined Networking Data Plane. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research, New York, NY, USA, 4–6 April 2017; pp. 1–8.
51. Li, Y.; Dai, R.; Zhang, J. Morphing Communications of Cyber-Physical Systems Towards Moving-Target Defense. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 592–598.
52. Torquato, M.; Vieira, M. Moving target defense in cloud computing: A systematic mapping study. *Comput. Secur.* **2020**, *92*, 101742. [CrossRef]
53. Duan, Q.; Al-Shaer, E.; Jafarian, H. Efficient Random Route Mutation Considering Flow and Network Constraints. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, 14–16 October 2013; pp. 260–268.
54. Liu, J.; Zhang, H.; Guo, Z. A defense mechanism of random routing mutation in SDN. *IEICE Trans. Inf. Syst.* **2017**, *100*, 1046–1054. [CrossRef]
55. Zhou, Z.; Xu, C.; Kuang, X. An Efficient and Agile Spatio-Temporal Route Mutation Moving Target Defense Mechanism. In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
56. Ganz, J.; Peisert, S. ASLR: How Robust Is the Randomness? In Proceedings of the 2017 IEEE Cybersecurity Development (SecDev), Cambridge, MA, USA, 24–26 September 2017; pp. 34–41.
57. Bittau, A.; Belay, A.; Mashtizadeh, A.; Mazières, D.; Boneh, D. Hacking Blind. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 227–242.
58. Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*; MIT Press: Cambridge, MA, USA, 2016.
59. LeCun, Y.; Bengio, Y.; Hinton, G. Deep Learning. *Nature* **2015**, *521*, 436–444. [CrossRef]
60. Eghtesad, T.; Vorobeychik, Y.; Laszka, A. Adversarial Deep Reinforcement Learning based Adaptive Moving Target Defense. In *Decision and Game Theory for Security*; GameSec 2020; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2020.
61. Sengupta, S.; Kambhampati, S. Multi-agent Reinforcement Learning in Bayesian Stackelberg Markov Games for Adaptive Moving Target Defense. *arXiv* **2007**, arXiv:2007.10457.
62. Zhu, M.; Hu, Z.; Liu, P. Reinforcement Learning Algorithms for Adaptive Cyber Defense against Heartbleed. In Proceedings of the 1st ACM Workshop on Moving Target Defense (MTD), New York, NY, USA, 7 November 2014; pp. 51–58.
63. Gao, C.; Wang, Y. Reinforcement learning based self-adaptive moving target defense against DDoS attacks. *J. Phys. Conf. Ser.* **2021**, *1812*, 012039. [CrossRef]
64. Chhabra, A.; Mohapatra, P. Moving Target Defense against Adversarial Machine Learning. In Proceedings of the 8th ACM Workshop on Moving Target Defense (MTD '21), Virtual Event, Republic of Korea, 15 November 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 29–30.
65. Huang, Y.; Huang, L.; Zhu, Q. Reinforcement Learning for feedback-enabled cyber resilience. *Annu. Surv. Control* **2022**, *53*, 273–295. [CrossRef]
66. Tozer, B.; Mazzuchi, T.; Sarkani, S. Optimizing Attack Surface and Configuration Diversity Using Multi-Objective Reinforcement Learning. In Proceedings of the IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 9–11 December 2015; pp. 144–149.
67. Farchi, E.; Shehory, O.; Barash, G. Defending via strategic ML selection. *arXiv* **2019**, arXiv:1904.00737.
68. Wang, H.; Li, F.; Chen, S. Towards Cost-Effective Moving Target Defense against DDoS and Covert Channel Attacks. In Proceedings of the 2016 ACM Workshop on Moving Target Defense (MTD '16), Vienna, Austria, 24 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 15–25.
69. Song, Q.; Yan, Z.; Tan, R. Moving target defense for deep visual sensing against adversarial examples. *arXiv* **2019**, arXiv:1905.13148.
70. Sengupta, S.; Chakraborti, T.; Kambhampati, S. MTDeep–Boosting the Security of Deep Neural Nets against Adversarial Attacks with Moving Target Defense. In Proceedings of the 10th International Conference on Decision and Game Theory for Security, GameSec 2019, Stockholm, Sweden, 30 October–1 November 2019; pp. 479–491.
71. Soliman, H.S. Neural Network Model for Compressing/Decompressing Image/Acoustic Data Files. U.S. Patent No. 6,608,924, 19 August 2003.
72. Wang, Z.; Liu, M.; Cheng, Y.; Wang, R. Robustly Fitting and Forecasting Dynamical Data with Electromagnetically Coupled Artificial Neural Network: A Data Compression Method. *IEEE Trans. Neural Netw.* **2007**, *28*, 1397–1410. [CrossRef] [PubMed]
73. Cui, W.; Jiang, F.; Gao, X.; Tao, W.; Zhao, D. Deep Neural Network Based Sparse Measurement Matrix for Image Compressed Sensing. In Proceedings of the 2018 25th IEEE International Conference on Image Processing (ICIP), Athens, Greece, 7–10 October 2018; pp. 3883–3887.
74. Hourri, S.; Nikolov, N.S.; Kharroubi, J. Convolutional neural network vectors for speaker recognition. *Int. J. Speech Technol.* **2021**, *24*, 389–400. [CrossRef]
75. Song, H.; Mao, H.; Dally, W.J. Deep Compression: Compressing Deep Neural Network with Pruning, Trained Quantization and Huffman Coding. *arXiv* **2015**, arXiv:1510.00149.
76. Tung, F.; Mori, G. Deep Neural Network Compression by In-Parallel Pruning-Quantization. *IEEE Trans. Pattern Anal. Mach. Intell.* **2020**, *42*, 568–579. [CrossRef] [PubMed]

77. Duohe, M.; Lei, C.; Wang, L.; Zhang, H.; Xu, Z.; Li, M. A Self-adaptive Hopping Approach of Moving Target Defense to thwart Scanning Attacks. In Proceedings of the International Conference on Information, Communications and Signal Processing, Singapore, 29 November–2 December 2016.
78. Sutton, R.S.; Barto, A.G. *Reinforcement Learning: An Introduction*, 2nd ed.; Massachusetts Institute of Technology: Cambridge, MA, USA, 2018.
79. Pawlick, J.; Colbert, E.; Zhu, Q. A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. *ACM Comput. Surv.* **2020**, *52*, 82. [CrossRef]
80. Tan, J.; Zhang, H.; Zhang, H. Optimal temporospatial strategy selection approach to moving target defense: A FlipIt differential game model. *Comput. Secur.* **2021**, *108*, 102342. [CrossRef]
81. Colbaugh, R.; Glass, K. Moving target defense for adaptive adversaries. In Proceedings of the IEEE International Conference on Intelligence and Security Informatics, Seattle, WA, USA, 4–7 June 2013; pp. 50–55.
82. Wang, S.; Wang, J.; Pei, Q.; Tang, G.; Wang, Y.; Liu, X. Active deception defense method based on dynamic camouflage network. *J. Commun.* **2020**, *41*, 97–111.
83. Kumari, S.; Yadav, R.J.; Namasudra, S.; Hsu, C. Intelligent deception techniques against adversarial attack on the industrial system. *Int. J. Intell. Syst.* **2021**, *36*, 2412–2437. [CrossRef]