Revisiting a Probabilistic Moving Target Defense Strategy to Handle Attacks Against Network Nodes with Multiple Resources

Jamil Ahmad Kassem[1](✉), Helena Rifà-Pous[1], and Joaquin Garcia-Alfaro[2]

[1] Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Center for Cybersecurity Research of Catalonia (CYBERCAT), Barcelona, Spain
jahmadkassem@uoc.edu
[2] SAMOVAR, Télécom SudParis Institut Polytechnique de Paris, 91120 Palaiseau, France
https://www.uoc.edu, https://www.telecom-sudparis.eu

Abstract. Traditional cyber defense strategies rely on a linear approach that involves detecting threats, selecting defenses, and mitigating attacks; yet, they struggle with emerging, unrecognized, and advanced threats. In search of a more robust solution, researchers have explored innovative strategies to maintain cybersecurity in a network without prior knowledge of the adversary or the specific attack being executed. One such strategy is known as Moving Target Defense (MTD). Leveraging Bayesian Stackelberg game theory, we establish optimal strategies for the defender and adversary, showcasing how the defender can reduce costs by steering attacks away from higher criticality nodes. This approach helps the defender implement a novel MTD logic model for either diversion or minimization of the attack damages. We use simulation results to show how our approach surpasses previous strategies. Our approach offers improvements in managing a multitude of resources. The new approach, while not addressing the known drawbacks, lays the foundation for more advanced MTD models that can incorporate a more detailed representation of system resources.

Keywords: Cybersecurity · Moving target defense · Cyber defense · Game theory · Logic model

1 Introduction

Cybersecurity is a complex issue when adversaries possess some knowledge of the system and can bypass the system's defense mechanisms. To address these advanced attacks, the scientific literature has introduced new approaches to handle security during such attacks. Progress beyond the use of different technologies involves implementing innovative security approaches that hinder attacks rather than simply halting them. One such approach is Moving Target Defense (MTD).

MTD finds its origins in older applications, such as the radio frequency hopping techniques used during World War II to thwart interception. This core concept has transitioned seamlessly into the digital age, with the rise of the internet in the 1990s prompted the development of MTD techniques for securing digital communication [7,9,26] and to address cyber-resilience issues associated with critical systems [25]. MTD operates without requiring prior knowledge of the adversary, relying solely on information about the expected attack type [33].

Moving Target Defense MTD strategies aim to enhance the resilience of the system by increasing the uncertainty of attackers, such as dynamically changing IP addresses. These periodic changes reduce the likelihood of successful attacks [11]. Despite growing interest in MTD, limitations exist, particularly in creating lightweight adaptive mechanisms against rational adversaries. MTD also incurs high costs in prolonged attacks. Furthermore, some MTD methods confuse attackers, broader network targeting attacks can diminish their effectiveness [8,27].

Based on the work of Mizrak [20], strategic approaches in cybersecurity emphasize cost-oriented optimization, where the defender aims to minimize overall costs. In our work, we build on Mizrak's findings and propose a mathematical model as a foundational approach to managing a cybersecurity system, specifically using MTD. This model serves as a basis for more advanced studies that address the handling of multiple resources and simultaneous attacks. A more complex model incorporates a detailed representation of resource criticality and accounts for multiple adversaries or attack vectors. The primary objective is to minimize the defender's costs, whether the system is under attack or not.

Our work leverages game theory, a branch of mathematics concerned with the analysis of strategic interactions between rational agents [1]. Formally, a game is defined as an interaction between players governed by a set of rules that specify the actions available to each player and the resulting outcomes for all possible combinations of actions [15]. In the context of MTD, game theory is used to investigate the strategic decision-making processes of two players with conflicting objectives [17]. These decisions are based on mathematical models (utility functions) that quantify the potential gains and losses associated with each action. Both players act rationally, seeking to minimize losses or maximize gains through their chosen strategies.

This paper is a preliminary outline of this work which was presented in study [2] and builds on previous work [8] to propose a new mathematical model for a defender-adversary game. The model considers multiple adversary strategies and focuses on resource protection by a defender who relocates resources to thwart attacks. This approach minimizes cost and attack impact, especially for interconnected and crucial resources. The development of our model, which constitutes the main contribution of this paper, follows a structured methodology outlined in the following list:

- Introduce a model for a system consisting of multiple nodes and resources.
- Define a multi-target defense strategy for the defender.
- Establish a game-theoretic strategy for the defender.

- Define the gains for the two players in the game.
- Solve the problem and develop a general solution.
- Perform numerical comparisons between the new strategy and the related work.

The paper is organized as follows. Section 2 surveys related work. Section 3 presents our method and some analytic results. Section 4 provides the best scenarios for the adversary and the defender. Section 5 provides numerical results. Section 6 concludes the paper.

2 Related Work

A wide range of methodologies for implementing deception in cyber defense have been tested [12]. Deception plays a crucial role in safeguarding networks by redirecting adversarial attacks towards less critical components. Notable technologies include contributions from Borders *et al.* [3], where fake network terminals are used to deceive attacks into unfruitful results. In addition, Onaolapo [21] and Lazarov [19] propose the creation of synthetic data to attract adversaries and protect resources, and Rrushi *et al.* [24] propose the use of decoy network interfaces to lure malicious software running on the system.

In a similar vein, MTD contributions employ various models such as game theory, heuristic models (*e.g.*, genetic), and machine learning to implement the different aspects of MTD, such as determining when to implement changes and which parts to modify [5]. MTD can be activated using triggers based on time or events. Time-based triggers are activated at specific intervals, while event-based triggers wait for certain trigger events before activation [6,23,30]. Time- and event-based triggers can be used concurrently [16,31,32], creating a hybrid activation mechanism. Although robust, all of these mechanisms share the drawback of being one-dimensional (handling a singular entity). Consequently, advanced attackers operating beyond a single attack model still pose a significant threat to systems that model them with a single threat model. Furthermore, combining different MTD models is not a straightforward process [29].

Yoon *et al.* [28] develop an MTD approach over programmable networks via Software Defined Networking (SDN) techniques using a three-tier attack graph. This attack graph uses a topology-dependent model as the basis for the MTD implementation. Asset-aware MTD offers an adaptive and scalable security solution. By integrating the topology-dependent attack graph with SDN, the impact of MTD on the system can be reduced. The attack graph evaluates exploitability considering the path leading to vulnerabilities. In the paper, the prediction of the attack path of the defender employs three main approaches: brute force, forward, and backward propagation. Incorporating deception alongside MTD can enhance the effectiveness of the previous approach. Although MTD is effective, using deception would benefit both security and cost for the defender.

In the work of Feng *et al.* [8], a game-theoretic model is proposed that incorporates MTD and deception to protect resources. The authors operate under the assumption that the adversary has more knowledge about the defender than vice versa. The system consists of multiple nodes that might be housing a resource. The defender can change the position of the resource, to deceive the adversary into failed attacks. The adversary, on the other hand, studies the system to select the node that is most probable to contain the resource. This interaction forms a two-player game between the adversary and the defender, each striving to maximize gains while minimizing losses. Leveraging the adversary's prior knowledge, the defender employs fake communication to deceive the adversary into targeting nodes less likely to contain the resource. Upon receiving feedback, the adversary must discern whether it is deception or accurate information. The study shows how, when implemented correctly, deception decreases the cost of defense. However, the previous work does not discuss having multiple resources and attacks. Furthermore, some attacks, such as Denial of Service (DoS), may affect the node functionality as a whole and, in this case, multiple resources. In such cases, switching resources may not impede the attack and could potentially result in unnecessary sacrificing of system resources.

Jia *et al.* [14] introduce a proxy switching MTD that helps against DOS attacks. Nonmalicious nodes are assigned to secure, noncompromised proxies. After an attack, nodes undergo continuous shuffling among proxies until malicious insider nodes are identified. Wright *et al.* [27] extend the work of [14] by proposing a new pay-off model for both adversaries and defenders. Their study introduces four additional strategies for the proxy switching defense system. The results demonstrate the efficacy of proactive defense for the defender, while adversaries in this scenario tend to target proxies with a higher number of nodes.

Although previous research has made significant progress in implementing MTD [4] and new defense technologies, we identified shortcomings at the micro-level of the networks under consideration. Specifically, resources within the network are treated as a single entity rather than as separate manageable entities. Since most networks contain multiple resources, using a single-entity model would place these resources at a higher risk. More specifically, since resources are often correlated, separating them would reduce the efficiency of the model (see Sect. 5). Effective resource management becomes crucial when adversaries have prior knowledge of the system and can target resources regardless of the number of nodes associated with the proxy. Furthermore, the defender can leverage the knowledge of the adversary as a defensive strategy. Building upon these observations, this paper introduces a model for the defender to manage multiple resources within a network. This allows the defender to minimize defense costs and the impact of attacks. Additionally, the defender can use the adversary's knowledge as a weapon to protect the resources in the system. In this paper, we do not consider quantifying the criticality of resources and consider that the defender uses an already established mathematical representation of value [13].

3 Our Approach

In this section, we describe our two-player model. Section 3.1 describes the model and the benefits for the two players. Section 3.2 describes the strategy that the defender is undertaking to maintain the security of the network nodes. A table of key variables used throughout this paper is presented in Table 1.

Table 1. Table of symbols and meaning as used in the paper

Symbol	Meaning
π	Adversary strategy
n	Number of nodes
m	Number of resources
c_a	Adversary total attack cost
c_m	Defender resource migration cost
i	Index for resources
k	Index for nodes
R	Set of resources
r_i	resource i
$T_c(k)$	Criticality of node k
$\alpha(i, k)$	Probability of moving r_i to node k
$\mathbb{C}(k)$	Defense cost if node k is attacked

3.1 Moving Target Defense Model

In this work, we introduce a novel MTD model comprised of two fundamental elements, nodes and resources. We define a network with n interconnected nodes (where $n > 1$) and m essential resources (where $m > 1$). These resources represent critical system components that provide vital services for network operation. We envision resources as functionalities offered by applications or services. An example of a resource could be an HTML service that grants access to specific websites hosted on the system. The nodes, on the other hand, function as containers for these resources. These nodes can be physical devices such as computers, microcontrollers, or any other electronic device capable of running the resources. The nodes are interconnected, allowing the free movement of resources between them. This model provides a framework for analyzing and understanding the behavior of networks where resources are dynamically managed and migrated across interconnected processing units.

Our model incorporates two intelligent agents, an adversary, and a defender. These agents operate with opposing objectives, seeking to maximize their respective utilities within the system. The defender, responsible for system control, prioritizes minimizing the overall cost of the system. In contrast, the adversary acts with malicious intent, with the aim of inflicting the greatest possible damage to the system.

The cost incurred by the defender agent comprises two components, defense cost and attack impact cost. The defense cost encapsulates the expenses associated with implementing the defender's strategy, as elaborated in Sect. 3.2. The

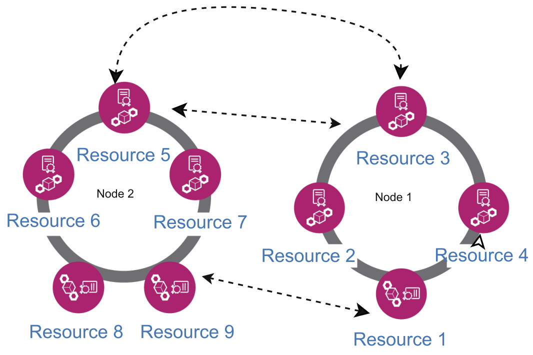


Fig. 1. Dynamic two node model with nine resources mobility

attack impact cost represents the damage inflicted by the attack of the adversary. Both agents are primarily concerned with the resources of the system.

The adversary adopts a strategic approach, crafting its attack strategy based on the anticipated utility gained from targeting specific nodes. The adversary can utilize attacks such as Denial-of-Service to disable a node. However, the adversary also incurs a cost associated with the launch of the attack. Therefore, the adversary's total utility is calculated as the difference between the expected benefit from a successful attack and the cost of carrying it out. This cost-benefit analysis guides the adversary's selection of targets, shaping its overall attack strategy.

The defender strategy involves resource protection through node relocation, allowing multiple resources to reside within a single node (as depicted in Fig. 1). The defender strategically distributes resources between nodes, ensuring that all nodes possess similar total criticality. By doing so, the defender removes the incentive for the adversary to attack a specific node and minimizes the maximum possible cost.

Assumptions. As mentioned above, adversaries and defenders have a set of prior knowledge on which to base their strategy. In the following, we outline the assumptions that we have made about the knowledge that the two agents have. We categorize the assumptions into two groups depending on what is known and what is hidden.

What the Adversary Knows:

- The number of resources and the number of nodes available to the defender.
- The strategy used by the defender. In this case, MTD.
- Probabilistic positions of the resources.
- The cost associated with implementing an attack.

What the Adversary Does Not Know:

- The exact location of the resources.
- How the defender implements MTD.

What the Defender Knows:

- An estimation of the attack cost by analyzing network complexity, threat intelligence, attack vectors, and resource investment (time, skills, tools)
- Total knowledge of the system's composition, including nodes and resources.
- The adversary's decision-making process regarding attacks.

What the Defender Does Not Know:

- The timing of the adversary's planned attacks.

Due to limited knowledge, both agents use probabilities in their strategies. The adversary uses past observations to predict the location of the resources. Under conditions of limited mutual knowledge, agents can converge on strategies that optimize their individual outcomes while remaining acceptable. This point of convergence, where both agents achieve a stable and mutually agreeable outcome, corresponds to the concept of an equilibrium state in game theory.

To sum up, the system comprises the following key components:

- A defender agent that tries to decrease defense and attack impact cost.
- An adversary agent that tries to cause the highest attack damage.
- m resources that are freely movable between nodes at a given cost.
- n interconnected nodes, each capable of containing multiple resources.
- The impact of the attack depends on the number of resources in the attacked node.

3.2 Resource Moving Strategy

The defender employs an MTD strategy to protect the system by relocating resources between nodes, thereby complicating the adversary's efforts. The defender, through the knowledge that the adversary is familiar with the system, proceeds to move resources between nodes. Consequently, the adversary gains the ability to anticipate the defender's movements and formulate a corresponding attack plan. The model operates as a two-player game known as a Bayesian Stackelberg game [22]. Bayesian Stackelberg is one of the classical models of game theory that tries to establish realistic strategies for the players where the leader chooses their action by anticipating the follower's response while taking into account uncertainty in the follower's preferences and adjusting them accordingly.

We establish the existence of a set of resources denoted as R within the system, which are the primary concern for both the defender and the adversary. This set of resources is denoted as $R = \{r_1, r_2, \ ...\ r_m\}$. We suppose that the adversary, through insider nodes or eavesdropping techniques, can form a probabilistic model of the position of the i^{th} resource r_i throughout the network. We normalize the values around the cost of resources. Specifically, we represent all variables as a factor of resource cost.

The adversary formulates an attack binary strategy [Eq. (1)], denoted π, considering both the expected gain of the attack and the associated cost of the attack. The expected gain depends on the resources affected, with attacks capable of targeting multiple resources in the k^{th} node, where k is the index of the attacked node.

$$\pi = \begin{cases} 1, & \text{attack cost} < \text{ expected gain of the attack} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

Before an attack is conducted, the initial step for the adversary is to establish a positional probability representation highlighting the optimum node for attacking. To illustrate the probabilities for the resources, we construct a matrix A where $\alpha(i,k)$ is the probability that the resource r_i is in node k, as shown in Matrix (2).

$$A = \begin{pmatrix} \alpha(1,1) & \alpha(2,1) & \dots & \alpha(m,1) \\ \alpha(1,2) & \alpha(2,2) & \dots & \alpha(m,2) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(1,n) & \alpha(2,n) & \dots & \alpha(m,n) \end{pmatrix} \tag{2}$$

note that $\sum_{k=1}^{n} \alpha(i,k) = 1$. For each node k, the adversary can find the impact of the attack, denoted by T_c, as the sum of the elements of the row k in the matrix A multiplied by the cost of each resource. Since the model is normalized to the cost of resources, we replace that value with 1 to form the impact of the attack as $T_c(k) = \sum_{i=1}^{m} \alpha(i,k)$. Let $U_a(k)$ be the expected gain of the adversary, that is, the utility function if the attack is targeting node k. We define the utility of the adversary in Eq. (3).

$$U_a(k) = (T_c(k) - c_a) \cdot \pi \tag{3}$$

where c_a designates the cost of attack for the adversary.

The defender similarly establishes an A matrix to define the implementation of MTD. Let $\mathbb{C}(k)$ be the expected cost incurred by the defender to implement the defense strategy. Then, we define the cost for the defender in Eq. (4).

$$\mathbb{C}(k) = (T_c(k) \cdot \pi) + c_m \sum_{i=1}^{m} (1 - \alpha(i, Position(i)))^2 \tag{4}$$

where c_m is the cost of movement for the defender. $Position(i)$ denotes the current location of r_i before any action by the defender is taken. Since the defender uses a uniform approach to move resources and all resources are of equal importance, moving resources incurs the same cost for the defender. The cost of moving resources only differs between different networks and setups of the system. Given the discrete nature of the model, the probability of resource movement is computed as one minus the probability of not moving the resource. As such, $1 - \alpha(i, Position(i))$ is the probability that r_i will be relocated.

The cost of the defender, as shown in Eq. (4), is formed from the expected loss due to an attack and the cost of the defender's strategy. In this context, the defender reallocates system resources to generate a state that minimizes the adversary's utility. Similarly, the adversary targets the node with the highest criticality (*i.e.*, highest $T_c(k)$). Although our cost model resembles the one presented in [8], we focus on the defender's management of multiple resources. We consider the squared value of the probability of moving a resource, $1 - \alpha(i, Position(i))$ to accentuate the impact of moving a single resource, as opposed to dividing the movement between multiple resources. Moving a single resource would cause this resource to become frequently unavailable. Since resources in R are critical, this scenario could bring the entire system to a halt while waiting for the unavailable resource to resume normal functionality. Consequently, it is more advantageous for the defender to move multiple resources.

4 Optimum Scenario

In this section, we discuss the defender's preferred MTD strategy. In Sect. 4.1 we present the two defender methodologies and illustrate them using two use-case examples. In the subsequent Sect. 4.2 we apply the methodologies introduced in Sect. 4.1 to find the general solution for the scenarios defined by the adversary's intent of attacking or not. In Sect. 4.3 we discuss the scenarios and highlight some important remarks.

4.1 Matrix Derivation

Building on the model presented in Sect. 3.1, the defender strategy is defined by two constraints. The first constraint is concerned with minimizing the probability of moving nodes; intuitively, a higher α for a particular resource signifies a lower probability of the defender needing to move that resource. The second constraint that the defender tries to minimize is the impact of the attack on all nodes *i.e.*, $T_c(k)$. This optimization problem can be seen as a variation of the subset sum problem [18], this problem consists of a set of numbers A which is divided into a selection of numbers that add up to a specific target value. In this case, the set in question is the probability matrix A, and the sum is each row with a value determined by the scenarios taken by the defender.

This section explores the two key constraints considered by the defender, which can be mathematically represented by the matrix A. The first constraint aims to minimize the probability of movement. This can be achieved by maximizing the maximum value α within each column of matrix A. The second constraint focuses on minimizing the overall impact of the attack. This translates into minimizing the sum of the elements in a row in matrix A. A lower sum across a row indicates a reduced cumulative impact of potential attacks targeting that specific resource type.

Consider an example involving five resources and three nodes (*i.e.*, $m = 5$ and $n = 3$). The defender's goals are to minimize $T_c(k)$ and maximize $\alpha(i, postion(i))$. Each column of the matrix corresponds to a resource, while each row corresponds to a node.

In the initial step, we consider a set-up where resources are equally divided among all nodes as shown in matrix A shown below. By evenly dividing resources across all nodes, the defender minimizes the maximum possible attack cost.

$$A = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

Minimizing Movement, First Approach. In this step, the goal of the defender is to minimize the probability of movement without changing $T_c(k)$. To accomplish this goal, the defender has the flexibility to interchange resources between nodes. At this stage, the model shares some similarities with the resource allocation model defined in [10]. In the context of matrix A, the movement cost is inversely proportional to the highest value in each column. To adhere to the constraint of not altering $T_c(k)$, the defender can subtract from one column and add to another; in this case, the subtracted and added value is $\frac{1}{3}$. Specifically, the defender takes two columns i_1 and i_2 and two rows k_1 and k_2 to carry out the operation. We move the values to the set $\{\alpha(i_1, k_1),\ \alpha(i_1, k_2),\ \alpha(i_2, k_1),\ \alpha(i_2, i_2)\}$. The new values of α after the operation are $\{\alpha(i_1, k_1) + \frac{1}{3}, \alpha(i_1, k_2) - \frac{1}{3}, \alpha(i_2, k_1) - \frac{1}{3}, \alpha(i_2, i_2) + \frac{1}{3}\}$. The defender repeats the same operation with different pairs of i and k, in this case for three pairs of resources, to decrease the probability of resource movement and maintain the same maximum T_c over all nodes. We illustrate this iterative approach in the following matrices:

$$A = \begin{pmatrix} \frac{2}{3} & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{3} & \frac{2}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 1 & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 1 & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & \frac{2}{3} & 0 \\ 0 & 1 & 0 & 0 & \frac{2}{3} \\ 0 & 0 & 1 & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

Minimizing Movement, Second Approach. The result matrix obtained from the last step minimizes the cost of movement for the defender, but the squared cost of movement, *i.e.*, $(1 - \alpha)^2$, can be further decreased. To this end, the cost of movement is divided across multiple resources instead of focusing on one resource. To achieve this, the defender for each node (row) sums all probabilities and divides them equally between resources. Note that this action is taken only with maximum α values, *i.e.*, when a row has more than one maximum α value. Our objective is to maximize the maximum values for each column. Applying the previous step, we get the final matrix. In the last step, we reorganize the matrix for organizational purposes.

$$A=\begin{pmatrix}\frac{5}{6} & 0 & 0 & \frac{5}{6} & 0\\ 0 & \frac{5}{6} & 0 & 0 & \frac{5}{6}\\ \frac{1}{6} & \frac{1}{6} & 1 & \frac{1}{6} & \frac{1}{6}\end{pmatrix}\rightarrow\begin{pmatrix}\frac{5}{6} & \frac{5}{6} & 0 & 0 & 0\\ 0 & 0 & \frac{5}{6} & \frac{5}{6} & 0\\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 1\end{pmatrix}$$

4.2 Defender Preferred Strategy

By employing the methodology of Sect. 4.1, we can establish a novel mathematical model and propose the corresponding general solution for the defender. Given that the adversary prefers to attack node k with the highest $T_c(k)$, and considering that the maximum cannot be less than the average, it follows that $T_c(k) \geq \frac{m}{n}$. Taking into account the adversary attack strategy described in Eq. (1), we differentiate three different scenarios: attack, optimized attack, and no attack.

Attack Scenario. This scenario is the general solution for the example in Sect. 4.1. If condition $c_a < T_c(k)$ holds, the adversary will opt to launch an attack. If $c_a < \frac{m}{n}$, the defender is unable to allocate r_i to nodes in a way that prevents an attack. To minimize costs, the defender should aim to minimize $T_c(k)$ while simultaneously maximizing $\alpha(i, Position(i))$. However, to reach an initial solution, the defender prioritizes minimizing $T_c(k)$ over maximizing $\alpha(i, Position(i))$. Consequently, the defender establishes the cost shown in Eq. (5).

$$\mathbb{C}(k)=\sum_{i=1}^{m}\alpha(i,k)+c_m\sum_{i=1}^{m}(1-\alpha(i,Position(i)))^2 \tag{5}$$

The minimum value of $T_c(k)$ can be achieved by equally dividing resources over nodes (*i.e.*, $T_c(k)=\frac{m}{n}$). After defining $T_c(k)$, the defender proceeds to maximize the value of $\alpha(i, Position(i))$, which leads to the matrix in Matrix (6). The upper left and lower right cells in Matrix (6) are repeated $\lceil\frac{m}{n}\rceil$ times.

$$A=\left[\overbrace{\begin{matrix}\frac{m}{n\lceil\frac{m}{n}\rceil}\cdot\boldsymbol{I}^{\lceil\frac{m}{n}\rceil}_{m \bmod n} & \boldsymbol{0}_{(m-\lceil\frac{m}{n}\rceil m \bmod n)\times(m \bmod n)}\\ \frac{1}{n\lceil\frac{m}{n}\rceil}\cdot\boldsymbol{1}_{(\lceil\frac{m}{n}\rceil m \bmod n)\times(n-m \bmod n)} & \boldsymbol{I}^{m-\lceil\frac{m}{n}\rceil}_{m \bmod n}\end{matrix}}^{m}\right]\left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\}n \tag{6}$$

where $\boldsymbol{I}^x_y$ designates an identity matrix of size y that is repeated x times *i.e.*, $\boldsymbol{I}^x=\boldsymbol{I}|\boldsymbol{I}\ldots\boldsymbol{I}$. We designate $\lfloor\frac{m}{n}\rfloor$ as the round-down value of $\frac{m}{n}$ and $\lceil\frac{m}{n}\rceil$ as round-up. From Matrix (6) the expected attack impact is $\frac{m}{n}$. The matrix also shows that $\lfloor\frac{m}{n}\rfloor(n-m \bmod n)$ resources do not move, while $(m \bmod n)\lceil\frac{m}{n}\rceil$ resources have a $\frac{m}{n\lceil\frac{m}{n}\rceil}$ probability of not moving. We update $\mathbb{C}(k)$ with the calculated value as shown in Eq. (7).

$$\mathbb{C}(k)=\frac{m}{n}+c_m(m \bmod n)\lceil\frac{m}{n}\rceil(1-\frac{m}{n\lceil\frac{m}{n}\rceil})^2 \tag{7}$$

Optimized Attack Scenario. The previous scenario can be further improved mathematically while maintaining that the adversary will attack. $\mathbb{C}(k)$ can be further decreased by increasing $T_c(k)$ beyond $\frac{m}{n}$ in favor of decreasing the cost of moving nodes. we designate δ as the amount of increase of the attack impact in favor of decreasing the probability of moving resources. We form the optimization problem $\mathbb{C}(k) = \frac{m}{n} + \delta(m \bmod n)\lceil\frac{m}{n}\rceil + c_m(m \bmod n)\lceil\frac{m}{n}\rceil(1 - \frac{m}{n\lceil\frac{m}{n}\rceil} - \delta)^2$.

To find the optimum solution for an attack scenario, we calculate the minimum of the previous equation by varying δ. The defender uses the same matrix A from Matrix (6) but changes the maximum values of α to agree with the section. Note that $0 \leq \frac{m}{n\lceil\frac{m}{n}\rceil} + \delta \leq 1$ since the probability cannot be negative or exceed 1. δ in this case is constrained to $-\frac{m}{n\lceil\frac{m}{n}\rceil} \leq \delta \leq 1 - \frac{m}{n\lceil\frac{m}{n}\rceil}$. Solving the previous problem gives $\delta = 1 - \frac{m}{n\lceil\frac{m}{n}\rceil} - \frac{1}{2c_m}$. Substituting δ in Eq. (7) gives the optimized cost for the defender as in Eq. (8).

$$\mathbb{C}(k) = \frac{m}{n} + (m \bmod n)\lceil\frac{m}{n}\rceil(1 - \frac{m}{n\lceil\frac{m}{n}\rceil} - \frac{1}{4c_m}) \tag{8}$$

No Attack Scenario. If $c_a \geq \frac{m}{n}$, the defender can distribute the resources in a way that prevents the attack. In this scenario, the defender can minimize the defense cost by maximizing $\alpha(i, Position(i))$ while averting the attack (*i.e.*, $T_c(k) = c_a$). Based on this, the defender cost is shown in Eq. (9).

$$\mathbb{C}(k) = c_m \sum_{k=1}^{m}(1 - \alpha(Position(k), k))^2, \sum_{i=1}^{m}\alpha(i,k) = c_a \tag{9}$$

The defender's objective is to efficiently distribute R across the nodes, by maximizing the value of $\alpha(i, Position(i))$. It should be noted that when c_a equals $\lceil\frac{m}{n}\rceil$ (where $\lceil\frac{m}{n}\rceil$ represents the roundup value of $\frac{m}{n}$), the defender can safely allocate resources statically ($\alpha = 1$) to the nodes, effectively preventing adversary attacks by ensuring that the maximum value of $T_c(k)$ remains below c_a. Beyond the $\lceil\frac{m}{n}\rceil$ threshold, the defender model does not show any change.

It is sufficient to solve on the range where $\frac{m}{n} \leq c_a \leq \lceil\frac{m}{n}\rceil$ to minimize costs and meet the given constraints. To achieve this, while optimizing expenses, the defender's optimal strategy is defined in the following matrix in Matrix (10). The upper left and lower right cells in Matrix (10) are repeated $\lceil c_a\rceil$ times.

$$A = \left.\left[\overbrace{\begin{array}{cc} \frac{c_a}{\lceil c_a\rceil}\cdot\boldsymbol{I}_{N_m}^{\lceil c_a\rceil} & \boldsymbol{0}_{\lfloor c_a\rfloor(n-N_m)\times N_m} \\ \frac{\lceil c_a\rceil - c_a}{\lceil c_a\rceil(n-N_m)}\cdot\boldsymbol{1}_{(\lfloor c_a\rfloor N_m)\times(n-N_m)} & \boldsymbol{I}_{n-N_m}^{\lfloor c_a\rfloor} \end{array}}^{m}\right]\right\}n \tag{10}$$

$\lfloor c_a \rfloor$ is the round down value of c_a and $N_m = m - n\lfloor c_a \rfloor$ is the number of nodes with only moving resources. The adversary does not plan to attack, so the impact of the attack is zero. $N_m \lceil c_a \rceil$ resources have $\frac{c_a}{\lceil c_a \rceil}$ probability of not moving. Note that N_m is strictly positive and when c_a exceeds $\lceil \frac{m}{n} \rceil$ it follows that the defender does not need to move resources and N_m is set to zero. The no attack $\mathbb{C}(k)$ is shown in Eq. (11).

$$\mathbb{C}(k) = c_m \cdot N_m \lceil c_a \rceil (1 - \frac{c_a}{\lceil c_a \rceil})^2 \tag{11}$$

This scenario is used by the defender given it is better than the previous models (*i.e.*, it minimizes $\mathbb{C}(k)$), as discussed next.

4.3 Discussion

Equation (11) presents a situation where the defender faces a dilemma due to the acquisition of two conflicting strategies. On the one hand, optimizing the placement of r_i to minimize migration reduces associated costs. However, decreasing migration increases the attractiveness of attacking the system to the adversary. This increased allure is directly related to the cost of attack c_a and the number of nodes involved. Specifically, when c_a exceeds $\frac{m}{n}$, the adversary no longer perceives attacking the system as opportune.

In summary, the defender is caught between two conflicting strategies: optimizing the placement of r_i and reducing migration costs versus the increased attractiveness of attack and its correlation with the cost of attack and the number of nodes. Once the cost of attack exceeds the threshold of $\frac{m}{n}$, the defender can migrate r_i as denoted by Matrix 10, and attacking will no longer be advantageous to the adversary.

In Eq. (7), the defender assumes that the adversary intends to attack the system, where the benefit of launching an attack outweighs the associated costs. However, the defender encounters another predicament: They have two options: either reposition r_i to confuse the adversary, incurring migration costs, or divide r_i evenly between multiple nodes, thereby preventing the adversary from executing a highly impactful attack.

In Fig. 2, the cost variations of the three approaches for the defender are depicted. We set m to 4 and n to 3. The figure illustrates that the optimal cost of the attack is nearly as efficient as the mathematical optimum. The curve also shows when the no attack strategy is desirable or not depending on the value of c_m.

5 Numerical Simulation

In this section, we validate the new results presented in this paper, using [8] as a reference. We employ numeric simulations for the computation of various values, visualizing data, and generating graphs.

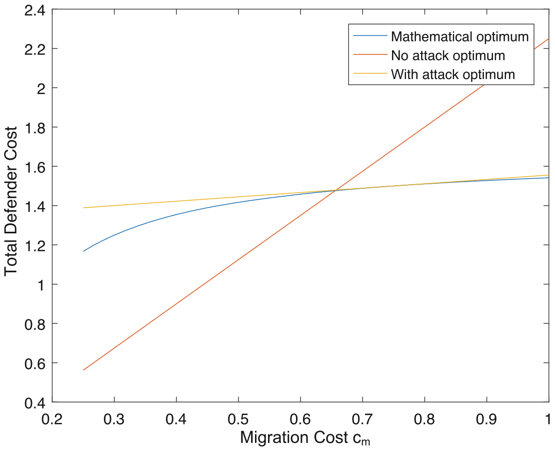


Fig. 2. Comparing $\mathbb{C}$ obtained by using the three models of this paper as c_m varies. The model is setup with $m = 4$ and $n = 3$.

5.1 Simulation Model

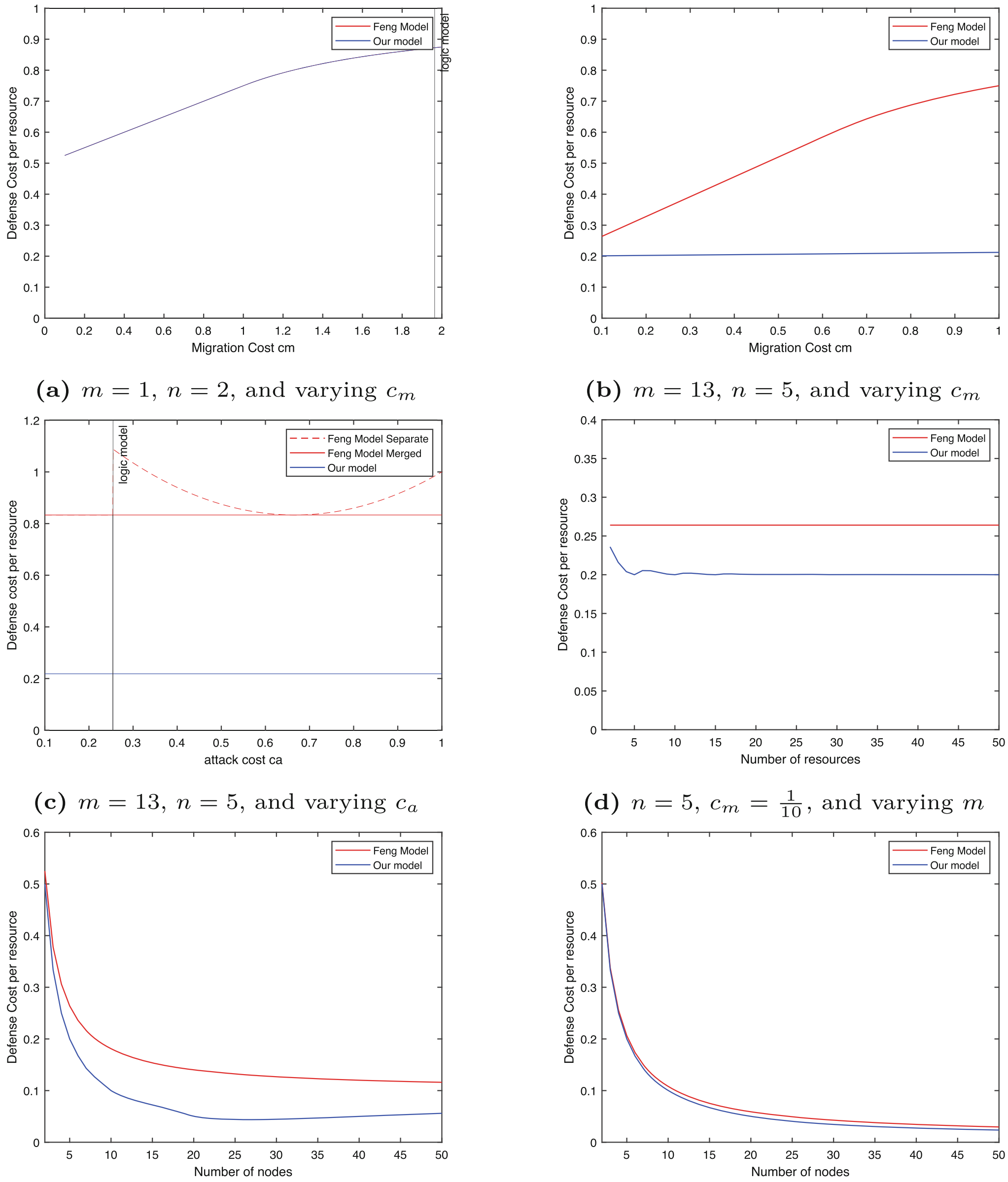
The system is configured as previously described in Sect. 3.1. $\mathbb{C}(k)$ is calculated using what was defined in this paper and in [8]. $\mathbb{C}(k)$ is then divided by m to find the cost per resource. As previously established, all values are normalized to the cost of the resource. We investigate six different scenarios that examine the effect of varying c_m, c_a, m, and n as follows:

1. $m = 1$, $n = 2$, and $c_a = \frac{1}{3}$ while varying c_m from 0.1 → 2 Fig. 3a.
2. $m = 13$, $n = 5$, and $c_a = \frac{1}{3}$ while varying c_m from 0.1 → 1 Fig. 3b.
3. $m = 13$, $n = 5$, and $c_m = \frac{3}{2}$ while varying c_a from 0.1 → 1 Fig. 3c.
4. $m = 20$, $c_a = \frac{1}{3}$, and $c_m = \frac{1}{5}$ while varying n from 2 → 50 Fig. 3e.
5. $m = 20$, $c_a = \frac{1}{3}$, and $c_m = \frac{1}{50}$ while varying n from 2 → 50 Fig. 3f.
6. $n = 5$, $c_m = \frac{1}{5}$, and $c_a = \frac{1}{3}$ while varying m from 2 → 50 Fig. 3d.

5.2 Discussion

The overlaid curves in Fig. 3a show that our new strategy yields the same $\mathbb{C}(k)$ when implemented in the same scenario as the original model ($m = 1$). The subsequent figures illustrate how the new strategy exceeds the previous one. Specifically, Fig. 3b shows how the Feng model exhibits an initial rapid increase in the defense cost as c_m increases. The increase becomes less rapid when the defender changes strategy when $c_m = \frac{n}{2(n-1)}$. The defender in our model uses other resources to maintain the same risk level while decreasing the cost of movement. On the other hand, in the Feng model, the defender is treating resources independently and spending a higher cost on defense.

In Fig. 3(b) we investigate how implementing the strategy in the Feng model [8] can impact the cost of the defender, we define two applications for the Feng model:



(a) $m = 1$, $n = 2$, and varying c_m

(b) $m = 13$, $n = 5$, and varying c_m

(c) $m = 13$, $n = 5$, and varying c_a

(d) $n = 5$, $c_m = \frac{1}{10}$, and varying m

(e) $c_m = \frac{1}{10}$, $m = 20$, and varying n

(f) $c_m = \frac{1}{100}$, $m = 20$, and varying n

Fig. 3. $\mathbb{C}(k)$ per resource for the defined models. The scenario switch signifies the border over which the defender switches from the attack scenario to the non-attack scenario or vice versa

- Feng model Separate: Each resource is treated independently, leading to potentially inefficient defense allocation and inaccurate strategy by the defender.
- Feng model merged: The model considers all resources together, enabling for a more strategic defense.

Separating resources might lead the defender to consider one strategy while the adversary selects another. This difference in strategy results in the defender wrongly predicting the strategy of the adversary. This can be observed in the increase in the cost in Fig. 3(d) to Fig. 3(f). We use these examples to illustrate how the related work could be implemented ineffectively.

The advantage of our strategy becomes more pronounced with an increase of m and n (to a threshold), as shown in Fig. 3(d) to Fig. 3(f). This is because our approach allows for more flexible resource allocation compared to simply moving resources all the time.

When m and n have the same value, the curves in Fig. 3(d) to Fig. 3(f) start to show a marginal change. At this threshold and due to the usage of $\lceil \frac{m}{n} \rceil$ and $m \mod n$, the model reaches a higher stability of the cost per resource as the logic starts to repeat when the number of resources increases. In this case, the defender prioritizes increasing m and n as these values offer the lowest cost per resource.

Finally, the parameter c_m plays a crucial role in influencing the margin between our proposed model and previous work (as shown in Fig. 3(c) and Fig. 3(f)). As expected, increasing the value of c_m leads to a wider gap between the performance of our model and the existing approaches. In a perfect scenario where c_m is very low, the defender can essentially move the resources infinitely without incurring any cost. This makes the cost of the defender solely dependent on the number of resources and nodes, regardless of the chosen strategy or MTD approach, leading to the loss of the advantage of using our strategy.

From the previous results, we form the impact of different variables as:

- Higher c_m incentives using our strategy.
- Increasing m and n is desirable.
- Although not directly affecting cost, knowledge of c_a is crucial to building an optimal defense strategy.

Our proposed strategy offers evident cost savings compared to existing strategies, especially with a larger number of resources and nodes. By understanding the impact of different variables, defenders can take advantage of this strategy to create more efficient defense systems. Since c_m cannot be controlled, they use this value to determine whether MTD is a cost-effective defense strategy. Conversely, the defender can control m and n by varying the system design and in that case can build a more favorable network. Finally, c_a helps the defender establish a limit of the optimal defense cost.

6 Conclusion

In the dynamic cybersecurity landscape, traditional static defense strategies have proven to be inadequate to counter emerging, unrecognized, and advanced threats. This has led researchers to explore innovative approaches that can secure networks without prior knowledge of the adversary or the specific attack that is underway. Among these approaches, MTD offers a promising avenue. Rather than abruptly halting attacks, it aims to hinder attacks by distributing the network's adversary targets without introducing additional entities. By expanding the potential points of attack, the adversary's confidence in executing the attack falters, often causing delays in their actions. Periodic implementation of MTD within specific intervals can force adversaries into a state of continuous delay waiting for an opportune time, effectively deterring attacks. Furthermore, if an attack is initiated, the defender can minimize losses by diverting the impact away from more critical parts of the system.

We have presented a novel MTD strategy for securing segmented nodes, where the main target is the resources distributed across these nodes. Utilizing Bayesian Stackelberg game theory, we have established optimal scenarios for both the defender and the adversary, analyzing how the defender can reduce costs by efficiently moving resources between nodes while reducing the likelihood of attacks. Our simulation results show that the new strategy achieves a lower cost for the defender when multiple resources are present. The results also show that the efficiency of the new strategy is further enhanced as the number of nodes and resources increases. From the numerical results, we find that the new strategy holds significant promise in enhancing network security when compared to previous contributions. Although MTD is a promising cyber defense, it still suffers from limitations born from the current network infrastructure such as the high cost of continued network change. This issue requires a new innovative network management infrastructure alongside models, similar to the one we presented in this paper, that optimize implementation and decrease defense cost.

We have successfully introduced a new mathematical model that demonstrates improved performance when managing multiple correlated resources. By accounting for resource correlations, the model reduces the defender's total cost compared to previous approaches. In future work, our aim is to extend this model to include multiple adversaries and the correlations between these intelligent entities. In a multi-attack scenario, the defender's focus shifts from merely minimizing the attack's impact to managing the system's post-attack state. Additionally, the model could benefit from a more detailed definition of resource criticality and constraints related to node sizes, where resources differ in value to the defender. Lastly, a more comprehensive approach to long-term cost analysis throughout the system's lifecycle should be considered.

Acknowledgment. This work is linked to the SECURING project PID2021-125962OB-C31, funded by the Ministry of Science and Innovation, as well as the ARTEMISA International Chair of Cybersecurity and the DANGER Strategic Project of Cybersecurity, both funded by the Spanish National Institute of Cybersecurity (INCIBE) through the European Union - NextGenerationEU and the Recovery, Transformation, and Resilience Plan.

References

1. Petrosyan, L.A.: Recent Advances in Game Theory and Applications. Springer, Heidelberg (2016)
2. Kassem, J.A., Rifá-Pous, H., Garcia-Alfaro, J.: Diseño de una estrategia probabilística de defensa de objetivo móvil para manejar ataques contra nodos de red con múltiples recursos. XVIII Reunión Española de Criptología y Seguridad de la Información (RECSI) Servicio de Publicaciones de la Universidad de León, 2024 (2024)
3. Borders, K., Falk, L., Prakash, A.: Openfire: using deception to reduce network attacks. In: 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007, pp. 224–233. IEEE, Piscataway (2007)
4. Charpentier, A., Neal, C., Boulahia-Cuppens, N., Cuppens, F., Yaich, R.: Real-time defensive strategy selection via deep reinforcement learning. In: Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES 2023. Association for Computing Machinery, New York (2023)
5. Cho, J.-H., et al.: Toward proactive, adaptive defense: a survey on moving target defense. IEEE Commun. Surv. Tutor. **22**(1), 709–745 (2020)
6. Colbaugh, R., Glass, K.: Predictability-oriented defense against adaptive adversaries. In: 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2721–2727. IEEE, Piscataway (2012)
7. Douligeris, C., Mitrokotsa, A.: DDoS attacks and defense mechanisms: a classification. In: Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795), pp. 190–193. IEEE, Piscataway (2003)
8. Feng, X., Zheng, Z., Cansever, D., Swami, A., Mohapatra, P.: A signaling game model for moving target defense. In: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, pp. 1–9. IEEE, Piscataway (2017)
9. Ghosh, A.K., Pendarakis, D., Sanders, W.H.: Moving target defense co-chair's report-national cyber leap year summit 2009. Technical report, Federal NITRD Program, Washington, DC, USA (2009)
10. Herrera, J.G., Botero, J.F.: Resource allocation in NFV: a comprehensive survey. IEEE Trans. Netw. Serv. Manage. **13**(3), 518–532 (2016)
11. Gonzalez-Granadillo, G., et al.: Dynamic risk management response system to handle cyber threats. Futur. Gener. Comput. Syst. **83**, 535–552 (2018)
12. Han, X., Kheir, N., Balzarotti, D.: Deception techniques in computer security: a research perspective. ACM Comput. Surv. **51**(4), 1–36 (2018)
13. Jeffrey, M.: Return on investment analysis for e-business projects. Internet Encyclopedia **3**, 211–236 (2004)
14. Jia, Q., Sun, K., Stavrou, A.: MOTAG: moving target defense against internet denial of service attacks. In: 2013 22nd International Conference on Computer Communication and Networks (ICCCN), pp. 1–9. IEEE, Piscataway (2013). ISSN: 1095-2055
15. von Neumann, H.J., Morgenstern, O.: The Theory of Games and Economic Behaviour. Princeton University Press (1944)
16. Keromytis, A.D., et al.: The meerkats cloud security architecture. In: 2012 32nd International Conference on Distributed Computing Systems Workshops, pp. 446–450. IEEE, Piscataway (2012)

17. Kiennert, C., Ismail, Z., Debar, H., Leneutre, J.: A survey on game-theoretic approaches for intrusion detection and response optimization. ACM Comput. Surv. (CSUR) **51**(5), 1–31 (2018)
18. Kleinberg, J., Tardos, E.: Algorithm design (2003)
19. Lazarov, M., Onaolapo, J., Stringhini, G.: Honey sheets: what happens to leaked google spreadsheets? In: 9th USENIX Workshop on Cyber Security Experimentation and Test, Berlin, Chausseestraße 20, Germany. ResearchGate (2016)
20. Mizrak, F.: Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Pressacademia (2023)
21. Onaolapo, J., Mariconti, E., Stringhini, G.: What happens after you are pwnd: understanding the use of leaked webmail credentials in the wild. In: Proceedings of the 2016 Internet Measurement Conference, IMC 2016, pp. 65–79, 1601 Broadway, Times Square, New York City. Association for Computing Machinery (2016)
22. Paruchuri, P., Pearce, J.P., Marecki, J., Tambe, M., Ordonez, F., Kraus, S.: Efficient algorithms to solve bayesian stackelberg games for security applications. In: AAAI, pp. 1559–1562, Washington, DC, U.S. (2008)
23. Rowe, J., Levitt, K.N., Demir, T., Erbacher, R.: Artificial diversity as maneuvers in a control theoretic moving target defense. In: National Symposium on Moving Target Research, USA. Artificial diversity as maneuvers in a control theoretic moving target defense (2012)
24. Rrushi, J.L.: NIC displays to thwart malware attacks mounted from within the OS. Comput. Secur. **61**, 59–71 (2016)
25. Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A.R., Garcia-Alfaro, J.: Cyber-resilience approaches for cyber-physical systems (2023)
26. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S.: A survey of moving target defenses for network security. IEEE Commun. Surv. Tutor. **22**(3), 1909–1941 (2020)
27. Wright, M., Venkatesan, S., Albanese, M., Wellman, M.P.: Moving target defense against DDoS attacks: an empirical game-theoretic analysis. In: 3rd ACM Workshop on Moving Target Defense, pp. 93–104, Berlin, Chausseestraße 20, Germany. ResearchGate (2016)
28. Yoon, S., Cho, J.H., Kim, D.S., Moore, T.J., Free-Nelson, F., Lim, H.: Attack graph-based moving target defense in software-defined networks. IEEE Trans. Network Serv. Manag. **17**(3), 1653–1668 (2020)
29. Zhang, H., Zheng, K., Wang, X., Luo, S., Bin, W.: Efficient strategy selection for moving target defense under multiple attacks. IEEE Access **7**, 65982–65995 (2019)
30. Zhu, Q., Başar, T.: Game-theoretic approach to feedback-driven multi-stage moving target defense. In: Das, S.K., Nita-Rotaru, C., Kantarcioglu, M. (eds.) GameSec 2013. LNCS, vol. 8252, pp. 246–263. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-02786-9_15
31. Zhuang, R., Zhang, S., Bardas, A., DeLoach, S.A., Ou, X., Singhal, A.: Investigating the application of moving target defenses to network security. In: 2013 6th International Symposium on Resilient Control Systems (ISRCS), pp. 162–169. IEEE, Piscataway (2013)
32. Zhuang, R., Zhang, S., DeLoach, S.A., Ou, X., Singhal, A., et al.: Simulation-based approaches to studying effectiveness of moving-target network defense. In: National Symposium on Moving Target Research, vol. 246, pp. 1–12, Pennsylvania USA. Citeseer (2012)
33. Zscaler. What is Deception Technology? Importance & Benefits| Zscaler (2023)