A Comprehensive Architectural Framework of Moving Target Defenses Against DDoS Attacks

Belal M. Amro[1], Saeed Salah[2,*] and Mohammed Moreb[3]

[1]*College of Information Technology, Hebron University, Hebron, Palestine, P.O. Box 40*
[2]*Department of Computer Science, Al-Quds University, Jerusalem, Palestine, P.O. Box 20002*
[3]*Smart College for Modern Education (SCME), Hebron, Palestine, P.O. Box 777*
E-mail: bilala@hebron.edu; sasalah@staff.alquds.edu; m.moreb@scme.edu.ps
[*]*Corresponding Author*

Received 10 January 2022; Accepted 21 March 2023;
Publication 21 June 2023

Abstract

Distributed Denial-of-Service (DDoS) attacks are among the top toughest security threats in today's cyberspace. The multitude, diversity, and variety of both the attacks and their countermeasures have the consequence that no optimal solutions exist. However, many mitigation techniques and strategies have been proposed among which is Moving Target Defense (MTD). MTD strategy keeps changing the system states and attack surface dynamically by continually applying various systems reconfigurations aiming at increasing the uncertainty and complexity for attackers. Current proposals of MTD fall into one of three strategies: shuffling, diversity, and redundancy, based on what to move? how to move? and when to move? Despite the existence of such strategies, a comprehensive Framework for MTD techniques against

Journal of Cyber Security and Mobility, Vol. 12_4, 605–628.
doi: 10.13052/jcsm2245-1439.1248

DDoS attacks that can be used for all types of DDoS attacks has not been proposed yet. In this paper, we propose a novel and comprehensive Framework of MTD techniques considering all stages, mechanisms, data sources, and criteria adopted by the research community, the Framework will apply to all DDoS attacks on different systems. To efficiently use our proposed model, a comprehensive taxonomy of MTD mitigation techniques and strategies is also provided and can be used as a reference guide for the best selection of the model's parameters.

Keywords: MTD, DDoS, IoT, SCADA systems, enterprise networks, cloud computing.

1 Introduction

In the modern era of cybersecurity, Distributed Denial-of-Service (DDoS) attacks are among the top toughest security threats facing security defenders worldwide [1]. DDoS attacks aim at making machines, or network resources unavailable to their legitimate users in accessing the necessary services. This leads to massive amounts of temporary or indefinite service disturbance and financial losses. Despite the availability of many DDoS mitigation techniques [2], it is still an active area of research, and extension efforts are still in progress to find the best technique that can efficiently defend against these attacks, there has been a tremendous increase in the diversity, power, scope, frequency, severity, attack inter-launching time, and volume of DDoS attacks. Recently, Amazon Inc., proclaimed that 2.3 Tbps and 1.35 Tbps of DDoS attacks traffic were experienced in February 2020 and 2018 targeting Amazon Web Services (AWS), and GitHub, respectively [3, 4]. In other similar reports, Cisco Inc., and Arbor Networks (NETSCOUT) [5, 6], mentioned that the number of DDoS attacks is growing quickly with an increased rate of 2.6-fold with an annual growth rate of 21%, and the peak DDoS attack size keeps increasing with a rate of 10–25% yearly, and they constitute 10% of total Internet traffic, they also reported that about 87% of the actual threats that face ISPs belongs to the DDoS activities.

To mitigate these attacks, many DDoS mitigation mechanisms exist. Research efforts have been proposed to classify these mechanisms, the literature commonly agrees on four categories: attack prevention, attack detection, attack response, and attack tolerance. Prevention mechanisms are proactive measures that are deployed to prevent a DDoS event, examples of DDoS

attack prevention filtering, load balancing, Intrusion Prevention Systems (IPSs), honeypots, and security overlay [7].

Detection mechanisms aim to detect DDoS attacks and are classified as anomaly-based, signature-based, Intrusion Detection Systems (IDSs), and middleware-based systems [8]. The response techniques are the actions taken once an attack is detected and are classified as during-attack techniques which include rate/resource limiting and capability-based responses and after-attack techniques which include forensics, traffic pattern analysis, and event log analysis [2, 9]. In attack tolerance, the aim is to reduce the effect of DDoS attacks once the previous strategies fail. Tolerance techniques include congestion policy, fault tolerance, and DDoS mitigation as a service/risk transfer for cloud computing technologies [10].

Despite the availability of many mitigation techniques, DDoS attacks can easily bypass traditional defense mechanisms by exploiting systems' vulnerabilities to structure attack packets to mimic legitimate traffic. One of the major reasons is that network configurations nowadays are typically deterministic, static, and homogeneous. However, with the rapid growth of Emerging Networking Technologies (ENTs), such as cloud computing [11], Software-Defined Networking (SDN) [12], Internet of things (IoT) [13], and Supervisory Control and Data Acquisition (SCADA) [14], system and network configurations are now migrating from static hardware-based to dynamically programmed software-based systems. This shift increased the flexibility of the newly emerging network technologies which brought a new set of attacks that targeted these networks and technologies. Because of such new attacks on these systems, new mitigation techniques have been proposed, among these techniques is Moving Target Defense (MTD). MTD is among the rising proactive defense techniques that utilize emerging network technologies, and it can effectively deal with DDoS security issues by dynamically changing the network and systems parameters.

Despite the availability of many MTD concepts and approaches, the literature lacks a generic framework model that defines the structure, components, data sources, behaviour, and more views of existing MTD mechanisms. Even though existing architectures target specific technologies – SDN, IoT, SCADA, and Cloud – they share common characteristics. Thus, in this paper, we collect all the previous efforts and propose a generic MTD framework for any existing or forthcoming proposals. The remainder of the paper is structured as follows. Section 2 summarizes the literature review of MTD techniques. In Section 3, an explanation of our proposed framework is

detailed. Section 4 discusses the suggested MTD classification taxonomy. Section 5 concludes the paper and presents some future research lines.

2 Literature Review

In MTD, the hacker and defender are performing a game race, and the defender eventually aims at changing the attack surface on a dynamic basis and continue to harden the success of the attack and hence leverage the security of the systems and the networks as well. These changes are used to increase the difficulty of the attack and reduce the possibility of attack success by making the attacker's knowledge, gathered during the reconnaissance phase, obsolete while launching her attack. MTD techniques can change one or more system attributes automatically and continually. To ensure that an MTD approach is effective at maximizing security and minimizing the impact on the system's performance, the considerations of an optimal movement strategy (How to move), a set of moving attributes (what to move), and spatiotemporal moving mechanisms (when to move) must be chosen carefully.

MTD was defined as "the ability of creating, analyzing, evaluating, and deploying mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities to attack, and increase system resiliency" [15]. In the past few years, MTD developed rapidly, and many concepts and approaches have been proposed. Among the frequently cited MTD techniques is a selection strategy for moving target defense based on the Markov game [16] that changes the attributes of network elements in a controlled manner for defenders, making the targeted network random, dynamic, and heterogeneous. IP address randomization [9, 12, 17], where the IP address is repeatedly altered. Virtual machine (VM) migration [1, 18], is a technique that has been proposed in different forms and suggests a repeated relocation of VMs across hypervisors to move them out of the attacker's reach. While these techniques often come with convincing examples that demonstrate the ability to leverage the security, verification of such demonstration is not provided yet [13].

Existing MTD techniques focused on special systems such as SCADA, IoT, and SDN. Many efforts have been done to determine the moving strategy such as shuffling, diversity, and redundancy. Existing proposals adopted many strategies to choose the moving attributes. To help in better selecting the moving strategy, some researchers suggested the use of datasets such as

KDD [19], and knowledgebase (Deep Learning and Artificial Intelligence (AI)) [20].

In this regard, several data sources can be used to help in choosing the appropriate moving strategy. These strategies can be used individually or for more advanced mechanisms, and a hybrid approach can be adopted. Some proposals suggested using human intervention as a useful data source (system expert) to analyse vulnerabilities discovered by various security modules. Others used attack analysis modules utilizing well-known vulnerability datasets such as NVD, OVSDB [21], and CVSS [22], these sources of data and many others were fed as inputs to the proposed techniques. Such datasets are important in this field because they contain valuable information about attacks, network traffic, system states, and service or topology infrastructure. Other research work used some knowledge-based, machine learning, and decision-support systems to determine which optimal moving strategy to choose. In addition to empirical studies on datasets and real testbeds, some researchers developed their proposals using simulation environments based on some simulation software such as NS2, MATLAB, or Python modules.

Besides the selection of the moving strategy, many works have been done to select the attributes to be moved when applying the moving strategy. These attributes are categorized as follows:

Machine level techniques: in the machine level, the concentration is on attributes that are related to the underlying machine such as instruction set and address space. In the instruction set, the idea is to change the machine instructions in a way such that it generates the desired output. It was introduced by [23] to safeguard against injection attacks, similar works have been proposed later that are based on changing the instruction set [19]. In Address space, the basic idea is to change the addresses of certain system components dynamically and randomly [24]. Similar work was proposed to prevent reverse engineering attacks based on deep neural network architecture and provided a taxonomy of Address Space Layout Randomization with an advanced statistical tool to evaluate the effectiveness of the implementation [25].

Network level techniques: these techniques concentrate on network level attributes such as IP address and port numbers, In the IP addresses technique, the IP addresses of hosts are changed dynamically, and the hacker will find a different system that was detected during the reconnaissance phase. In [19], the authors proposed a technique called Random Host Mutation (RHM), where hosts are assigned virtual IP addresses that are changed randomly and

synchronously over time. Similar approaches were proposed for different areas such as cloud computing platforms [26], IoT [27], Mobile Ad Hoc Networks (MANETs) [28], and network-level applications. Port numbers are logical addresses that are used to deliver packets to the corresponding protocol. During the reconnaissance phase, the attacker lists out the set of running services on a particular host by finding out open ports. In MTD, similar to IP address shuffling, port numbers might also be changed so that attacker will not be able to use his gathered information to continue with her attack since the port numbers will be dynamically changed [29]. Some implementations were designed specifically for some application protocols such as Domain Name System (DNS) [30] others were designed as a combination of IP and port changes to leverage security [29].

System-level techniques: Proxies are dedicated devices that hide internal IP addresses from the outside and send requests on behalf of the internal hosts. MOTAG is one of the implementations that secure service access for authenticated users by deploying a group of dynamic packet indirection proxies [31]. Using proxies as MTD attributes are mostly related to the redundancy strategy as proposed in [32].

Virtual machines: The techniques imply changing the software stack of a system using virtualization which will lead to changing system characteristics and leverage the ability to defend against attacks [33]. Most VM migrations were deployed for cloud services and enhancement has been done such as using a continuous Markov chain to precisely select the destination server of the virtual machine [34]. In [35], the authors proposed an empirical study of using virtual machines as an MTD and showed that VM migration can significantly mitigate the memory DoS attack. Genetic algorithms were used to develop an MTD technique for virtual machine migration in the cloud computing environment. Many researchers have studied virtual machine migration and its effect in leveraging the security of the services against attacks [36].

Operating systems: MTD techniques might be extended to include operating systems through rotation among different operating systems [37], in cloud environments, a scientific workflow execution system was proposed that relies on changing operating systems based on mimic defense [38].

Application level techniques: The idea behind application program diversity is to design a compiler that can generate multiple functionally equivalent variants of programs that are internally different [39], this method can be

used in many application programs such as WebAssembly [40], a run time portable diversification system was proposed by [41] that exploit multiple heterogeneous programming system to ensure diversity. Analysis of the correctness and equivalence of the diverse code was also studied by researchers who developed methods to find the correctness of the generated variants of the code [42].

Despite the availability of many MTD concepts and approaches, the literature lacks a generic Framework model that defines the structure, components, data sources, behaviour, and more views of existing MTD mechanisms. Even though existing architectures target specific technologies – SDN, IoT, SCADA, and Cloud – they share some common characteristics. However, the proposed MTD techniques designed for a specific technology might not fit other technologies.

3 Proposed Framework of Moving Target Defense

In this section, we detail our proposed MTD framework that will be used as a reference model for adopting any MTD mechanism against DDoS attacks. First, we provide our motivation and the attacker threat model, then we explain the proposed model in detail.

3.1 Motivation

Many research efforts have been devoted to developing efficient MTD mechanisms, architectures, and strategies. Existing efforts target specific technologies such as Cloud [43], Software Defined Networks (SDN) [42, 44–46], SCADA systems, and IoT [47]. Despite this diversity, most developed technologies share common procedural guidelines and stages. In this paper, we unify all these efforts into one comprehensive generic MTD Framework to be used as a reference guide for developing current and forthcoming MTD proposals. The model can be used with all DDoS MTD techniques in different disciplines and is not dedicated for to a specific system or application. Moreover, an updated taxonomy of MTD techniques is proposed and can be used as a heuristic to use the best MTD-applicable strategy.

3.2 Attacker Threat Model

Before proceeding with our proposed model, we have first to introduce attacker threat models related to DDoS attacks on systems and networks [48], proposed a detailed description of the attackers' model. In

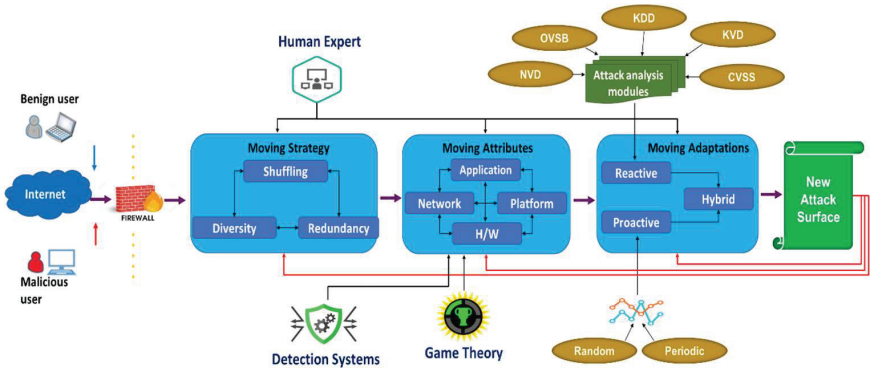

Figure 1 The proposed moving target defense framework.

today's cyberspace, new types of smarter attackers exist including (*i*) persistent attackers whose attacks take several iterations and have not been executed in a one-time attack [49], (*ii*) adaptive attacker who always adapts to change dynamically the system cases, (*iii*) motivated attackers who are smart enough to efficiently carry out attacks, so the attacks have a little damage but maximum results and (*iv*) stealthy attackers who do not exhibit recognizable attacking attitude every time. They conduct the attacks in a so secretive manner. The proposed MTD model is a generic model that can be adapted to defend against any type of the beforementioned attacker models.

Based on a deep analysis of the literature belonging to the above-mentioned technologies, it is observed that any MTD technique must go through three main stages: Choosing the moving strategy (how to move); choosing one/multiple moving attributes (what to move) and adjusting the time of movement (when to move).

3.3 MTD Generic Framework

As shown in Figure 1, the proposed MTD framework is composed mainly of three stages namely: moving strategy, moving attributes, and moving adaptations. In each stage, one or more operation is performed according to the inputs of that stage and the desired outputs as well. The input to the first stage is the network traces and system logs. The desired output of the last stage is a new and more complex attack surface. Human intervention might be required at some stages to gain better strategy selection, and hence optimal attack surface. In the following subsections, a detailed description of each stage is provided.

3.3.1 Moving strategy

Based on the dynamic diversity of the platform, system, or application, the moving strategy is further classified into three categories: shuffling, diversity, and redundancy. Platform diversification involves any change in platform properties to stop or obstruct the attack process. The shuffle technique targets a variety of system settings located at different layers (e.g., randomizing port or IP address, migration among different platforms, rearranging topology, etc.) The diversity technique presents similar functions with various implementations at the operating system level or system inputs. The redundancy technique implement mechanism that facilitates the process of replicating different systems, network, or platform components (e.g., servers) to make multiple replicas with the same functions.

Referring to Figure 1, the output of the first stage is fed as an input to the moving attributes stage. It contains a set of methods to choose the appropriate system/platform or application attributes to move. In this regard, choosing the number and type of attributes play a key role in the performance and the induced overhead. However, despite the availability of several promising methods, choosing the optimal set of attributes is still an open research question. Many contributions suggested the use of several mechanisms for optimizing the attributes' selection process.

3.3.2 Moving attributes

When talking about moving attributes, it means the dynamically configured items in the system that are used to change the attack surface [50]. These items represent the set of attributes that provide an answer to the question "What to move?" in Moving Target Defense (MTD). Moving attributes might be done on the machine level, network level, application level, and system level. The selection of the level to be chosen to move attributes depends on the environment we are trying to guard. In case we are trying to mitigate DDoS attacks against a web server, then we may choose the network level as well as the system level. That is, we may choose to change the IP address and port numbers as well as to change the operating system or virtual machine.

3.3.3 Moving adaptations

By moving adaptation, we seek to find the optimal time to perform the change so that the data gained by the hacker is invalid to carry out her attack. Moving adaptation can be done as reactive, proactive, or hybrid. In the reactive approach, the method is carried out based on an alert or event occurrence. This method is required to work with security tools and systems such as

firewalls and Intrusion Detection Systems (IDSs), this method completely depends on security tools and hence will not succeed if the security tool or system fails to detect an event [44].

In proactive defense, the move is carried out based on periodic time intervals or random selection of the time interval that might be done using either periodic or random time series [45], this method depends on the time interval and might degrade the performance if the time interval is short [46]. In the hybrid approach, both reactive and proactive approaches might be used together, this will allow the change upon some time interval and will also carry out the change based on an alert from the IDS or firewall that might enhance the security [51].

The reactive approach works in tandem with attack analysis modules and detection systems, once an event is detected, the system decides to perform the change. The attack analysis modules use different techniques to detect attacks and require some datasets that include NVD, OSVB, KDD, KVB, and CVSS [52], Figure 2 shows how a hybrid strategy works.

4 Taxonomy of MTD Techniques

Figure 2 summarizes the main classifications of existing MTD techniques. We divided MTD techniques into six categories: technology, architecture, performance metric/s, testbed, mitigation method, and evaluation method. In what follows, we describe each category.

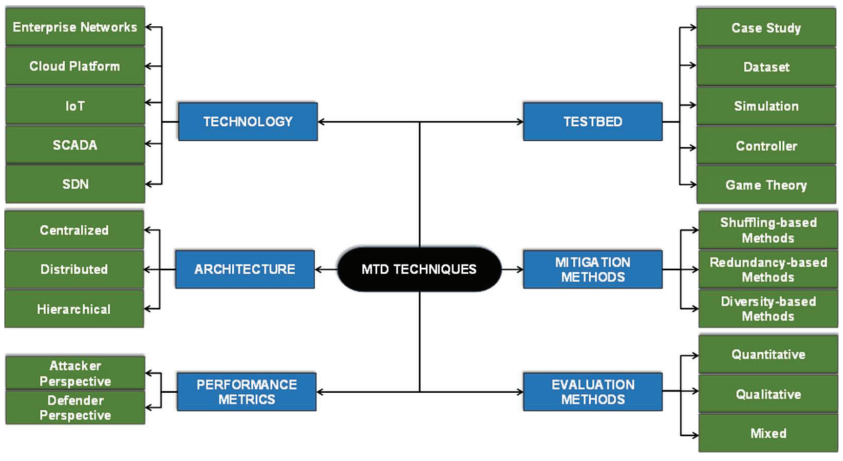

Figure 2 The proposed classification of existing MTD techniques.

4.1 Technology (Application)

MTD techniques can be classified based on the target application or technology of any DDoS attack. Some techniques were specifically developed to manage common DDoS attacks for the following applications.

- Enterprise networks: An enterprise network facilitates the communication between machines throughout departments, shares files between employees, eases access to systems, and analyses the performance of IT environments.
- Cloud platforms: Due to their characteristics, many companies and organizations rely on cloud computing to run their applications. It is a computing paradigm that facilitates access to a configurable set of IT resources, e.g., storage, network, services, and computing. It allows a gradual decrease or increase of information resources' allocation, and the adaptation of any available proceeding power to the current needs. Securing cloud services becomes an essential part of any cloud-based service to protect the information and all the applications associated with it against network attacks [53].
- Internet of Things (IoT): It is a type of network technology consisting of a set of protocols to facilitate the connectivity of anything to the Internet infrastructure. It consists of data sensing, data management and exchange, and data communication to achieve smart positioning, tracking, monitoring, and administration of IoT-based applications.
- SCADA systems: Supervisory Control and Data Acquisition (SCADA) are frameworks with sensors, implemented monitoring and tracking stages, and advanced communications that provide prompt notifications to the central stations in process control. SCADA systems are designed to work in a standalone way and relied on proprietary protocols for securing the system.
- Software Defined Networking (SDN): It is a network management approach that enables dynamic and programmatically network configurations to improve network performance, stability, and monitoring [54].

4.2 Architecture

MTD architecture can be centralized, distributed, or hierarchical.

- Centralized based: In this mitigation system, all components and modules are deployed at the same place, in which no communication or cooperation framework is needed [55].

- Distributed based: In a distributed architecture, all system's modules and components are deployed at multiple places in the environment. This way, some form of cooperation and communication between modules is required [55].
- Hierarchical system/application or hardware architectures can be used to develop the MTD technique. Here, a mix of approaches from both centralized and distributed systems can be used to improve detection accuracy [16].

4.3 Performance Metrics

To evaluate the accuracy of MTD techniques, several evaluation measures were suggested by the literature. They can be broadly classified based on attack perspective from both attackers' and defenders' points of view.

- Attacker perspective: Some existing mitigation systems use some developed attackers' metrics to estimate the attack performance. These metrics are mainly used to capture how much penalty is introduced for an attacker to achieve its attack success when a developed MTD is deployed such as attack cost, and penalty in attack payoff [56].
- Defender perspective: Some mitigation techniques use defenders' metrics to measure the performance in achieving the security goals of a given system such as Quality of Service (QoS), system performance, and defense cost [57].

4.4 Testbed

It is a composite abstraction of systems that are built by combining prototypes and elements of actual systems and is used to study system components and their interactions into the essence of the real system [58]. The following are some methods used in this category.

- Case study: The aim here is to implement an MTD technique on a system and gather information about this implementation to find out its effectiveness and feasibility. A well-known case study was proposed by [22], and a comprehensive survey including case studies regarding MTD techniques was provided by [59].
- Dataset: Many testbed techniques relied on data from different data sources called datasets, these datasets were specifically generated to help

researchers assess their techniques using such data. Different datasets are available for MTD techniques such as NVD, OSVB, KDD, KVB, and CVSS [52].
- Simulation: instead of working on a real system that might not be available for a researcher, some researchers used simulation software such as NS2, MATLAB, or Python modules to build their systems and gather information based on some configuration of the simulated environment. An example of a simulation base model is shown in [60].
- Game theory: Game theory has been used thoroughly in designing an MTD technique. Many researchers propose the use of game theory to effectively set the MTD parameters and trigger the change. A Bayesian Stackelberg game was used to define the optimal moving target defense strategy [52]. A different usage of game theory was to build some models for cyber deception [61].

4.5 Mitigation Methods

These are the methods that are designed and implemented to mitigate the effect of DDOS attacks on systems, below is a list of them.

- Shuffling-based: As described before, shuffling techniques target different system settings at different layers such as randomizing port numbers or IP addresses, migration among different platforms, and rearranging topology. The aim is to harden the attack on the system by changing the information the attacker gained during the reconnaissance phase. Diversity has been studied in the literature for example IP shuffling was recently studied by [28], where port number shuffling was studied by [29], platform migration was studied by [31, 32], and rearranging topology has been studied by [23].
- Redundancy-based: It aims at leveraging system's immunity against DDOS attacks by replicating systems, networks, or platform components as servers to gain multiple replicas of different systems. An example of redundancy using proxy servers is provided by [62].
- Diversity-based: The idea of diversity is to automatically generate variants of a system or program by changing some of the properties at the system or input level while ensuring that the final output will not change by these different variants [63] an example of application program diversity is provided by [39].

4.6 Evaluation Methods

These methods are used to evaluate MTD mitigation methods based on some predefined criteria, these methods are listed below:

- Quantitative methods: these are used to evaluate the effectiveness and feasibility of the MTD systems and use some well-defined metrics such as confidentiality, integrity, availability, attack representation, and quality of service impact. Different approaches might be used in quantitative testing such as pure analytical approaches based on mathematical analysis, coarse-grained simulation, data gained from test beds, and experimentation [50] a quantitative approach for instruction set randomization was proposed by [64].
- Qualitative methods: are methods that are based on observational findings to identify design features, different metrics are used in qualitative analysis such as risk analysis and performance costs. A comparison between qualitative and quantitative MTD techniques is provided by [59].
- Mixed methods: Both quantitative and qualitative methods are used to evaluate the MTD techniques. Mixed methods will give a more complete picture of the feasibility and effectiveness of the system as they engage different metrics for better evaluation.

5 Conclusion and Future Work

Distributed Denial-of-Service (DDoS) attacks are among the most frequent attacks in today's cyber world; these attacks are of different multitude types with huge diversity and different countermeasures that led to the absence of an optimal solution. One of these effective countermeasures is called Moving Target Defense (MTD). In MTD, the nature of the system is changed dynamically and continuously based on different attributes. This dynamic change makes it hard for an attacker to pursue the attack because he will face different parameters than those gained during the reconnaissance phase. The literature provided some MTD models designed specifically for a particular application domain and there is no generalized model that fits most domains. A comprehensive architectural framework for moving target defense techniques against DDoS attacks was proposed in this paper, the framework was adapted to fit the most five widely used technology application domains, namely: enterprise network, cloud computing, IoT, SCADA systems, and SDN. Besides, an extensive survey of MTD mitigation techniques was also conducted and

a taxonomy of these techniques has been provided, this taxonomy can be used as a heuristic for our proposed framework to better choose the moving strategy or attribute. In future work, we will assess the proposed framework against a category of DDoS attacks based on some attack models and report the best mitigation technique for each attack type.

References

[1] S. Salah, B. Amro, "Big Picture: Analysis of DDoS Attacks Map – Systems and Network, Cloud Computing, SCADA Systems, and IoT, *Int. J. of Internet Technology and Secured Transactions*, InderScience, vol. 12, no. 6, 2022.

[2] S. Bhatia, S. Behal, and I. Ahmed, "Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions," *Advances in Information Security*, vol. 72, pp. 55–97, 2018, doi: 10.1007/978-3-319-97643-3_3/FIGURES/7.

[3] K. Kalkan, G. Gür, and F. Alagöz, "SDNScore: A Statistical Defense Mechanism Against DDoS Attacks in SDN Environment".

[4] J. E. Varghese and B. Muniyal, "An Efficient IDS Framework for DDoS Attacks in SDN Environment," *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.

[5] T. B. Jr, A. Sumits, S. Jain, U. Andra, T. K.- Cisco, and undefined 2016, "FCisco Visual Networking Index (VNI) and VNI Service Adoption," *audentia-gestion.fr*, Accessed: Jul. 03, 2022. [Online]. Available: http://audentia-gestion.fr/cisco/pdf/2016-VNI-Complete-Forecast-PT.pdf.

[6] N. Arbor, "Worldwide Infrastructure Security Report." Accessed: Jul. 03, 2022. [Online]. Available: rbornetworks.com/rs/arbor/images/WISR2014.pdf.

[7] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques:," https://doi.org/10.1177/1550147717741463, vol. 13, no. 12, Dec. 2017, doi: 10.1177/1550147717741463.

[8] S. Badotra and S. N. Panda, "SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking," *Cluster Comput*, vol. 24, no. 1, pp. 501–513, Mar. 2020, doi: 10.1007/S10586-020-03133-Y.

[9] A. Y. Nur, "Combating DDoS Attacks with Fair Rate Throttling," *15th Annual IEEE International Systems Conference, SysCon 2021 – Proceedings*, Apr. 2021, doi: 10.1109/SYSCON48628.2021.9447054.

[10] R. K. Deka, D. K. Bhattacharyya, and J. K. Kalita, "DDoS Attacks: Tools, Mitigation Approaches, and Probable Impact on Private Cloud Environment," Oct. 2017, doi: 10.48550/arxiv.1710.08628.

[11] P. K. Senyo, E. Addae, and R. Boateng, "Cloud computing research: A review of research themes, frameworks, methods and future research directions," *Int J Inf Manage*, vol. 38, no. 1, pp. 128–139, Feb. 2018, doi: 10.1016/J.IJINFOMGT.2017.07.007.

[12] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A Survey on Software-Defined Networking," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 1, pp. 27–51, Jan. 2015, doi: 10.1109/COMST.2014.2330903.

[13] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications*, vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/JCC.2015.35021.

[14] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1942–1976, Jul. 2020, doi: 10.1109/COMST.2020.2987688.

[15] "Trustworthy Cyberspace: Strategic plan for the Federal cybersecurity research and development program |Global System for Sustainable Development." https://gssd.mit.edu/search-gssd/site/trustworthy-cyberspace-strategic-plan-59912-mon-02-11-2013-1132 (accessed Jul. 16, 2022).

[16] S. Huang, H. Zhang, J. Wang, and J. Huang, "Markov Differential Game for Network Defense Decision-Making Method," *IEEE Access*, vol. 6, pp. 39621–39634, Jun. 2018, doi: 10.1109/ACCESS.2018.2848242.

[17] X. L. Xiong, L. Yang, and G. S. Zhao, "Effectiveness Evaluation Model of Moving Target Defense Based on System Attack Surface," *IEEE Access*, vol. 7, pp. 9998–10014, 2019, doi: 10.1109/ACCESS.2019.2891613.

[18] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019, doi: 10.1186/S42400-019-0038-7/FIGURES/8.

[19] E. Al-Shaer, Q. Duan, and J. H. Jafarian, "Random host mutation for moving target defense," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, vol. 106 LNICS, pp. 310–327, 2013, doi: 10.1007/978-3-642-36883-7_19/COVER.

[20] D. Ding, M. Savi, and D. Siracusa, "Tracking Normalized Network Traffic Entropy to Detect DDoS Attacks in P4," *IEEE Trans Dependable Secure Comput*, 2021, doi: 10.1109/TDSC.2021.3116345.

[21] S. Musman and A. Turner, "A game theoretic approach to cyber security risk management," *Journal of Defense Modeling and Simulation*, vol. 15, no. 2, pp. 127–146, Apr. 2018, doi: 10.1177/1548512917699724.

[22] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "FlipIt: The game of 'stealthy takeover,"' *Journal of Cryptology*, vol. 26, no. 4, pp. 655–713, Oct. 2013, doi: 10.1007/S00145-012-9134-5/TABLES/2.

[23] G. lin Cai, B. sheng Wang, W. Hu, and T. zuo Wang, "Moving target defense: state of the art and characteristics," *Frontiers of Information Technology and Electronic Engineering*, vol. 17, no. 11, pp. 1122–1153, Nov. 2016, doi: 10.1631/FITEE.1601321/TABLES/7.

[24] H. Shacham, M. Page, B. Pfaff, E. J. Goh, N. Modadugu, and D. Boneh, "On the effectiveness of address-space randomization," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 298–307, 2004, doi: 10.1145/1030083.1030124.

[25] H. Marco-Gisbert and I. R. Ripoll, "Address Space Layout Randomization Next Generation," *Applied Sciences 2019, Vol. 9, Page 2928*, vol. 9, no. 14, p. 2928, Jul. 2019, doi: 10.3390/APP9142928.

[26] V. Getov, "Security as a service in smart clouds – Opportunities and concerns," *Proceedings – International Computer Software and Applications Conference*, pp. 373–379, 2012, doi: 10.1109/COMPSAC.2012.112.

[27] N. Bandi, H. Tajbakhsh, and M. Analoui, "FastMove: Fast IP switching Moving Target Defense to mitigate DDOS Attacks," *2021 IEEE Conference on Dependable and Secure Computing, DSC 2021*, Jan. 2021, doi: 10.1109/DSC49826.2021.9346278.

[28] P. Wang, M. Zhou, and Z. Ding, "A Two-Layer IP Hopping-Based Moving Target Defense Approach to Enhancing the Security of Mobile Ad-Hoc Networks," *Sensors 2021, Vol. 21, Page 2355*, vol. 21, no. 7, p. 2355, Mar. 2021, doi: 10.3390/S21072355.

[29] Di. P. Sharma, J. H. Cho, T. J. Moore, F. F. Nelson, H. Lim, and D. S. Kim, "Random Host and Service Multiplexing for Moving Target Defense in Software-Defined Networks," *IEEE International Conference on Communications*, vol. 2019-May, May 2019, doi: 10.1109/ICC.2019.8761496.

[30] M. F. Hyder and M. A. Ismail, "Toward Domain Name System privacy enhancement using intent-based Moving Target Defense framework over software defined networks," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, p. e4318, Oct. 2021, doi: 10.1002/ETT.4318.

[31] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving target defense against internet denial of service attacks," *Proceedings – International Conference on Computer Communications and Networks, ICCCN*, 2013, doi: 10.1109/ICCCN.2013.6614155.

[32] D. Fleck, A. Stavrou, G. Kesidis, N. Nasiriani, Y. Shan, and T. Konstantopoulos, "Moving-target Defense against Botnet Reconnaissance and an Adversarial Coupon-Collection Model," *DSC 2018 – 2018 IEEE Conference on Dependable and Secure Computing*, Dec. 2017, doi: 10.48550/arxiv.1712.01102.

[33] N. Ben-Asher, J. Morris-King, B. Thompson, and W. Glodek, "Attacker Skill, Defender Strategies and the Effectiveness of Migration-Based Moving Target Defense in Cyber Systems".

[34] E. M. Kandoussi, I. el Mir, M. Hanini, and A. Haqiq, "Modeling Virtual Machine Migration as a Security Mechanism by using Continuous-Time Markov Chain Model," *Proceedings of 2019 IEEE World Conference on Complex Systems, WCCS 2019*, Apr. 2019, doi: 10.1109/ICOCS.2019.8930781.

[35] M. Torquato and M. Vieira, "VM Migration Scheduling as Moving Target Defense against Memory DoS Attacks: An Empirical Study", Accessed: Jul. 24, 2022. [Online]. Available: https://www.linux-kvm.org/.

[36] R. Dhaya et al., "Energy-Efficient Resource Allocation and Migration in Private Cloud Data Centre," *Wirel Commun Mob Comput*, vol. 2022, 2022, doi: 10.1155/2022/3174716.

[37] M. Thompson, N. Evans, and V. Kisekka, "Multiple OS rotational environment an implemented Moving Target Defense," *7th International Symposium on Resilient Control Systems, ISRCS 2014*, Sep. 2014, doi: 10.1109/ISRCS.2014.6900086.

[38] Y. wen Wang, J. xing Wu, Y. fei Guo, H. chao Hu, W. yan Liu, and G. zhen Cheng, "Scientific workflow execution system based on mimic defense in the cloud environment," *Frontiers of Information Technology and Electronic Engineering*, vol. 19, no. 12, pp. 1522–1536, Dec. 2018, doi: 10.1631/FITEE.1800621.

[39] T. Jackson et al., "Compiler-Generated Software Diversity," pp. 77–98, 2011, doi: 10.1007/978-1-4614-0977-9_4.

[40] J. Cabrera Arteaga, O. Floros, O. Vera Perez, B. Baudry, and M. Monperrus, "CROW: Code Diversification for WebAssembly", doi: 10.14722/madweb.2021.23004.

[41] J. Kim, S. Lee, B. Johnston, and J. S. Vetter, "IRIS: A Portable Runtime System Exploiting Multiple Heterogeneous Programming Systems", Accessed: Jul. 24, 2022. [Online]. Available: http://energy.gov/downloads/doe-public-access-plan.

[42] J. W. Jang, F. Verbeek, and B. Ravindran, "Verification of Functional Correctness of Code Diversification Techniques," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12673 LNCS, pp. 160–179, 2021, doi: 10.1007/978-3-030-76384-8_11.

[43] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Resource-Aware Detection and Defense System against Multi-Type Attacks in the Cloud: Repeated Bayesian Stackelberg Game," *IEEE Trans Dependable Secure Comput*, vol. 18, no. 2, pp. 605–622, Mar. 2021, doi: 10.1109/TDSC.2019.2907946.

[44] B. Liu and H. Wu, "Systematic planning of moving target defence for maximising detection effectiveness against false data injection attacks in smart grid," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 151–163, Sep. 2021, doi: 10.1049/CPS2.12012.

[45] M. Ge, J.-H. Cho, D. S. Kim, G. Dixit, and I.-R. Chen, "Proactive Defense for Internet-of-Things: Integrating Moving Target Defense with Cyberdeception," *ArXiv*, pp. 1–19, May 2020, doi: 10.48550/arxiv.2005.04220.

[46] N. Saputro, S. Tonyali, A. Aydeger, K. Akkaya, M. A. Rahman, and S. Uluagac, "A Review of Moving Target Defense Mechanisms for Internet of Things Applications," *Modeling and Design of Secure Internet of Things*, pp. 563–614, Jul. 2020, doi: 10.1002/9781119593386.CH24.

[47] A. A. Mercado-Velazquez, P. J. Escamilla-Ambrosio, and F. Ortiz-Rodriguez, "A Moving Target Defense Strategy for Internet of Things Cybersecurity," *IEEE Access*, vol. 9, pp. 118406–118418, 2021, doi: 10.1109/ACCESS.2021.3107403.

[48] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Communications Surveys and Tutorials*,

vol. 21, no. 2, pp. 1851–1877, Apr. 2019, doi: 10.1109/COMST.2019.2891891.

[49] L. Miao and S. Li, "Cyber security based on mean field game model of the defender: Attacker strategies," *Int J Distrib Sens Netw*, vol. 13, no. 10, pp. 1–8, Oct. 2017, doi: 10.1177/1550147717737908.

[50] P. M. Figliola, "CRS Report for Congress the Federal Networking and Information Technology Research and Development Program: Funding Issues and Activities," 2010, Accessed: Jul. 24, 2022. [Online]. Available: www.crs.govRL33586.c11173008.

[51] J. H. Cho *et al.*, "Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 709–745, Jan. 2020, doi: 10.1109/COMST.2019.2963791.

[52] E. v. Doynikova, A. v. Fedorchenko, and R. O. Kryukov, "Determination of features of cyber-attack goals based on analysis of data in open security data sources," *IOP Conf Ser Mater Sci Eng*, vol. 734, no. 1, Jan. 2020, doi: 10.1088/1757-899X/734/1/012160.

[53] M. Nguyen and S. Debroy, "Moving Target Defense-Based Denial-of-Service Mitigation in Cloud Environments: A Survey," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/2223050.

[54] M. Azab, M. Samir, and E. Samir, "'MystifY': A proactive Moving-Target Defense for a resilient SDN controller in Software Defined CPS," *Comput Commun*, vol. 189, pp. 205–220, May 2022, doi: 10.1016/J.COMCOM.2022.03.019.

[55] D. Krohmer and H. D. Schotten, "Decentralized Identifier Distribution for Moving Target Defense and beyond," *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*, Jun. 2020, doi: 10.1109/CYBERSA49311.2020.9139717.

[56] H. Alavizadeh, J. Jang-Jaccard, and D. S. Kim, "Evaluation for Combination of Shuffle and Diversity on Moving Target Defense Strategy for Cloud Computing," *Proceedings – 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 573–578, Sep. 2018, doi: 10.1109/TRUSTCOM/BIGDATASE.2018.00087.

[57] M. Wright, S. Venkatesan, M. Albanese, and M. P. Wellman, "Moving Target Defense against DDoS Attacks: An Empirical Game-Theoretic Analysis," *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, doi: 10.1145/2995272.

[58] P. J. Fortier and H. Edgar. Michel, "Computer systems performance evaluation and prediction," p. 525, 2003.

[59] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A Survey of Moving Target Defenses for Network Security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1909–1941, May 2019, doi: 10.48550/arxiv.1905.00964.

[60] M. Ayrault, E. Borde, U. Kuhne, and J. Leneutre, "Moving Target Defense Strategy in Critical Embedded Systems: A Game-theoretic Approach," *2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC)*, vol. 2021-December, pp. 27–36, Dec. 2021, doi: 10.1109/PRDC53464.2021.00014.

[61] A. Eldosouky and S. Sengupta, "Moving Target Defense Games for Cyber Security: Theory and Applications," *Game Theory and Machine Learning for Cyber Security*, pp. 160–179, Sep. 2021, doi: 10.1002/9781119723950.CH10.

[62] G. Kaur and R. Sachdeva, "Virtual machine migration approach in cloud computing using genetic algorithm," *Lecture Notes in Networks and Systems*, vol. 135, pp. 195–204, 2021, doi: 10.1007/978-981-15-5421-6_20/COVER.

[63] D. Evans, A. Nguyen-Tuong, and J. Knight, "Effectiveness of Moving Target Defenses," pp. 29–48, 2011, doi: 10.1007/978-1-4614-0977-9_2.

[64] B. Potteiger, Z. Zhang, and X. Koutsoukos, "Integrated data space randomization and control reconfiguration for securing cyber-physical systems," *ACM International Conference Proceeding Series*, Apr. 2019, doi: 10.1145/3314058.3314064.

Biographies

Belal M. Amro is an assistant professor at college of IT at Hebron University – Palestine. Dr Belal has received his PhD in Computer Science and

Engineering from Sabanci University – Istanbul, Turkey in 2012. In 2004 he received his MSc in complexity and its interdisciplinary applications from IUSS, Pavia, Italy. His BSc degree was awarded from Palestine polytechnic university in computer systems engineering in 2003. Dr. Amro has served as technical program committee member for different international conferences and journals and reviewed more than 50 papers in the field of information technology including privacy and security. Currently, Mr. Amro is conducting research in network security, wireless security, privacy preserving data mining techniques and has published more than 18 papers in international journals and conferences in the field of computer security and privacy.

Saeed Salah is an Assistant Professor and researcher at the Department of Computer Science at Al-Quds University in Jerusalem. He received his BSc. in Electrical/Computer Engineering from Al-Najah National University in 2003, his MSc. degree in Computer Science from Al-Quds University in 2009, and his Ph.D. from the Department of Signal Theory, Telematics and Communications of the University of Granada in 2015. His research interests are focused on network management, information and network security machine learning, data mining, MANETs, routing protocols, and blockchain. Dr. Salah published many peer-reviewed research papers in recognized international journals and conferences. Moreover, he acts as a reviewer for a number of journals in his field.

Mohammed Moreb is an Vice President of Academic Affairs at SCME. He obtained his Ph.D. in Electrical and Computer Engineering. Dr. Moreb Expertise in Cybercrimes & Digital Evidence Analysis, specifically focusing on Information and Network Security, with a strong publication track record, work for both conceptual and practical which built during works as a system developer and administrator for the data centre for more than 10 years, config, install, and admin enterprise system related to all security configuration, he improved his academic path with the international certificate such as CCNA, MCAD, MCSE; Academically he teaches the graduate-level courses such as Information and Network Security course, Mobile Forensics course, Advanced Research Methods, Computer Network Analysis and Design, and Artificial Intelligence Strategy for Business Leaders.