Cyber Deception against DDoS attack using Moving Target Defence Framework in SDN IOT-EDGE Networks

Haula Galadima
School of Digital Technologies
Middlesex University
Flic en Flac, Mauritius
hg429@live.mdx.ac.uk

Amar Seeam
School of Digital Technologies
Middlesex University
Flic en Flac, Mauritius
a.seeam@mdx.ac.mu

Visham Ramsurrun
School of Digital Technologies
Middlesex University
Flic en Flac, Mauritius
v.ramsurrun@mdx.ac.mu

***Abstract*—Software Defined Networking (SDN) networking paradigm advancements are advantageous, but they have also brought new security concerns. The Internet of Things (IoT) Edge Computing servers provide closer access to cloud services and is also a point of target for availability attacks. The Distributed Denial of Service (DDoS) attacks on SDN IoT-Edge Computing caused by botnet of IoT hosts has compromised major services and is still an impending concern due to the Work From Home virtual office shift attributed by Covid19 pandemic. The effectiveness of a Moving Target Defense (MTD) technique based on SDN for combating DDoS attacks in IoT-Edge networks was investigated in this study with a test scenario based on a smart building. An MTD Reactive and Proactive Network Address Shuffling Mechanism was developed, tested, and evaluated with results showing successful defence against UDP, TCP SYN, and LAND DDoS attacks; preventing IoT devices from being botnet compromised due to the short-lived network address; and ensuring reliable system performance.**

***Keywords*—IoT, Moving Target Defense, SDN, IDS, DDoS, Deception**

I. Introduction

Software Defined Networks (SDN) have evolved to revolutionize pre-existing standards of networking by totally segregating the conventional control and data planes, therefore enabling programmable, portable, and autonomous networks [1]. These changes, although effective, has also brought about novel security concerns. The ability of SDN to launch sophisticated DDoS comes from a variety of angles owing to its architectural nature. An instance of this is the controller providing the SDN with a centralized network topology perspective [2]

The Internet of Things (IoT) network is rapidly expanding and is anticipated to have a significant influence on society via smart cities, smart grids and among other applications [3] . Edge Computing brings service, data, or applications nearer to the point in which its needed. Fog Computing, in essence, relies on these Edge devices to do the majority of processing, storing, or transmission onsite [4]. IoT is limited in every way, including memory, CPU etc., and so as growing numbers of IoT become integrated, efficient security becomes significantly difficult, especially with low power devices. These limitation and its static nature makes the IoT platform most vulnerable to reconnaissance, exploit execution, and availability attacks such as DDOS [5]. Amongst the most common remedies is moving target defence, it is an approach that involves the notion of dynamic change of the attack surface so as to enhance ambiguity and deceive adversaries [5]. Simultaneously, this mechanism can be leveraged in the emerging SDN framework [6].

The implementation of a unique MTD approach that consist of a constant change of the attack surface by employing a Reactive and Proactive MTD Shuffling mechanism that shuffles the network addresses of the IoT devices and Edge Computing servers proactively to complement current Moving target defence strategy in SDN IoT-Edge Computing Network research via examination of secondary research for the problem background, feasibility study on the derived theory, and critical analysis of current state of the art. Thenceforth, it will be tested and evaluated via a network emulator.

The body of the paper is structured as follows. In Section II, the paper initially covers the background information on SDN, DDoS and MTD while Section III addresses existing research. In Section IV, the methodology for implementing and assessing the MTD framework is derived and then, Section V describes the proposed MTD mechanism's system design and architecture. Section VI presents resources and processes in the implementation of the mechanism. In Section VII, evaluation of the MTD mechanism is carried out via emulation and graphical representation. In Section VIII, the results of the evaluation are analyzed. The paper is concluded in Section IX, which also presents details on future work.

II. Background

A. Software Defined Networking

SDN is an approach to network that specifies techniques that allows programmable establishment, configuration, monitoring, modification, and regulation of network activity by the network administrators via interfaces that are open like the OpenFlow protocol. The architecture of the OpenFlow

protocol consist of three components: Switches, Controllers, and Flow Entries. [7].

1) Comparison: Traditional Networking VS SDN: In traditional networking, no single or centralized device has the control or oversight of the whole network even though there is interaction between these devices [8]. In SDN, the control plane adopts a centralized model. The SDN controller is located control plane whilst the data plane contains the switches [7].

B. Denial of Service Attack

A denial-of-service attack is an act by adversaries to prevent rightful accessibility of systems/services [9] . The objectives of this attack are Network resources depletion, exhaustion, or consumption; Configuration/State data and Network component Disruption;and System Collapse or Malfunction [10]

1) Distributed Denial of Service (DDos): [11] described DDoS as an assault in which a system is attacked by a group of infected machines known as zombies or bots in order to deplete the target network/system.

2) DDos in SDN: A survey by [12] examines the state-of-the-art methods addressing DoS/DDoS attack in SDN through perspectives of intrinsic (emphasis is on SDN component and functional features.) and extrinsic (emphasis on flow of the network as well as their properties.) techniques in this work [13], expounding the research area of DoS/DDoS in SDN. The outcome of the research showed need for more studies in the prevention area of DDoS in SDN more than the importance of detection/mitigation, of which we propose Moving Target Defence.

C. Moving Target Defence (MTD)

NITRD [14] defined MTD as a changing paradigm to the asymmetric state that exists amongst defences and attacks, thus providing a dynamic change in the safeguarded system's attack surface.

1) Overview of MTD: [15] described MTD's purpose as a boost to security by combining two forms of action, one of which is to "transform", and the other to "move" the structure/configurations of the system in a set time frame. MTD mechanisms are carried out in instances in basis of either proactive or reactive viewpoints. In proactive defence, detection of the DDoS attack and the defence action is done prior to major damage while the reactive defence involves defensive response following an attack [6].

2) MTD Techniques: According to [16], MTD approaches are divided in three categories that modifies network settings in a distinctive manner: shuffle, diversity, and redundancy.

- Shuffle: MTD techniques that are based on shuffling reorganize the setup of the current network.
- Diversity: MTD approaches based on diversity have multiple network and system element setups although retaining the same functions and processes.
- Redundancy: MTD approaches based on redundancy replicate current network elements to provide availability. They mostly focus on DoS attacks.

3) MTD Strategy Classification: Studies by [17] has classified MTD into a Timeliness and Operation based types. In Timeliness-based, the techniques based on criteria to determine 'when to move.', it consists of a time, event, and a hybrid (combination of both) category of approach. The operation-based MTD categorizes the techniques based on criteria to determine 'How to move'.

III. Related Works

The existing research literatures are reviewed are for the purpose of identifying gaps in current knowledge and noting the already established research components in MTD mechanisms in SDN against DDOS from year 2015 to 2021. Table 1 gives an overview of top research reviewed based on [18] survey methodology to dissect papers to be analysed for this study.

A. Critical Analysis

A major consideration to reviewed work such as author [19], [20], [21], [22], and [23] whom some have not considered evaluation of system performance and QoS; and that of some whose proposed technique impacted performance and degraded QoS. The proposed MTD mechanism will cover this research gap and covered ranges of performance metrics to prove the theory.

The theory for the proposed mechanism was mostly propounded based on author [24] whom had no major weakness and considered a cost effective shuffling that accommodates overhead, but it did not consider SDN IoT-Edge Architectures or DDoS focuses on exploitation of IoT devices whom which this study expanded a light on. Author [25] research also focused on defence for IoT and considers Edge Computing level servers but the moving rate for the changing configurations is not specified and the computation of shuffling unpredictability for the system is not carried out which the proposed system has made a clear configurable function for event generation.

IV. Methodology

This project's research is conducted using a hybrid research methodology of both qualitative and quantitative research methods with more emphasis on the latter. In the field of experimental implementation research for SDN-based MTD, this is a standard methodology.

1) Research design: The study began with an inductive research approach based on existing literature, which commences with a series of empirical findings pertaining SDN based MTD against DDoS, examining commonalities in the observational data, and finally establishing a theory based on research gaps or loopholes.

With these established grounding, the study then used a deductive method to data analysis based on the facts and the hypothesis established. This starts with the established theories and research questions, then the development of hypotheses, implementation and finally collection and analysis of primary data via testing via an emulation model to acquire experimental evidence through alteration and monitoring scenarios for test variables.

TABLE I
CURRENT STATE OF THE ART

[HTML]C0C0C0 Author(s)	Focus of the Paper
(1) Ma, Xu and Lin (2015)	MTD defence against blind DDoS
(2) Aydegar et al, (2016)	MTD in SDN to defend against DDoS
(3) Nguyen, Pal, and Debroy (2018)	A network obfuscation strategy in SDN enabled MTD operating at two levels.
(4) Liu et al, 2018	MTD in SDN/NFV to mitigate and fuzzy logic detect DDoS.
(5) Steinberger et al, (2018)	MTD-based DDoS protection for high-speed SDN
(6) Aydegar et al, (2018)	Configurations of moving network path using an MTD and NFV-based technique against link flooding.
(7) Aydegar et al, (2019)	MTD architecture that deceives attackers by using Shadow Networks via NFV on SDN ISP networks.
(8) Luo et al, (2019).	SDN use for MTD and honeypots for DDoS in IoT
(9) Liu et al, (2019)	Adaptive MTD framework for SDN
(10) Zhou et al, (2019)	A shuffling MTD strategy that is cost effective whilst accounting the attack/shuffling cost and the attack/defender performance
(11) Narantuya et al. (2019)	MTD approach for assigning hosts virtual IP addresses across large networks using multiple controllers.
(12) Debroy et al, (2020).	A combination of both a proactive and reactive VM migration technique based on MTD to safeguard cloud applications from attacks on availability
(13) Zhou et al, (2020)	Improved cost effective shuffling which incorporates regular users as trilateral games to generate strategies.
(14) Wang (2021)	To safeguard virtual networks, a network-level MTD system and collection of strategies are utilized.

2) Phases of the Methodology: The phases carried out are divided into five steps, as follows:

- System Model: This is an SDN-based network with an RYU SDN-controller, Open vSwitch SDN switches, and end user hosts. The suggested MTD defensive mechanism is implemented by the SDN controller, which centrally supervises transmission of data and network nodes routing functions via the OpenFlow protocol.
- Attacker Model: Assumptions about the attacker's objectives and abilities, as well as their familiarity with target systems and attack tools. The potential attack is regarded to be internal with capacity to interrupt availability.
- Defense Model: The Defense system incorporates a hybrid MTD strategy of both reactive and proactive defensive measures to provide network security using SDN.
- Measurement and Metrics: To assess the efficiency of MTD techniques used in SDN-based network settings, a set of dynamic security metrics has been established.
- Evaluation: To examine the capability and performance of the developed system, an analysis via Attack based experiments using emulation methods is implemented.

3) Data Collection and Analysis Method: The assessment methodology is depicted in Fig. 1 where the experimental metrics, factors, and parameters are presented. The data used is produced by the Evaluation and Measurement Metric to assess the effectiveness of the developed system. This will cover the Attackers strategy, Attack Surface, Defence Solution and Quality of Service (QoS).

V. SYSTEM ANALYSIS, ARCHITECTURE, AND DESIGN

The proposed approach establishes obfuscation of the network via hybrid strategy of both time and event based movements. The proposed methods include two mechanisms, the first being the proactive stage that involves obfuscating the IP during map generation, and the second being the reactive stage that mitigates the attack. As the network address shuffling is based on multiplexing, a host can have several randomized virtualized addresses. The virtual IP is periodically remapped when multiplexing/demultiplexing occurs. This provides end-hosts with relatively short-lived virtual addresses continuously and arbitrarily modified in order to mask their actual addresses.

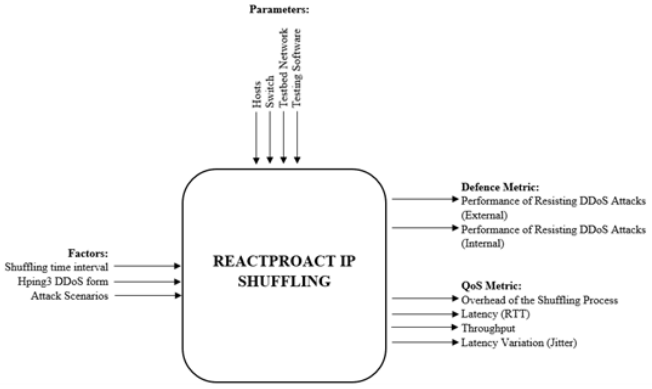

Fig. 1. Methodology

A. Scenario

1) Attack focus: A smart building's local network, which includes IoT devices, the edge server, and SDN-enabled networking components. In a case where the IoT device is hindered by resource exhaustion and cannot operate due to a DDoS attack that prevents the edge server from providing cloud services to the IoT nodes whilst simultaneously overloading the network. The attacker device could be a hijacked gateway / IoT that generates hostile traffic. The traffic is to a specific IP address (Edge server Node) connected to the core switch. The IoT Edge Servers is the computing infrastructure that supports IoT data administration services to and from cloud.

B. Network Architecture

The network design depicted in Fig. 2 comprises of a single subnet with a topology of a single remote SDN controller, four switches (1 core switch and 3 Edge switches), an edge server, and the end devices (6 IoT devices and 3 Attacker Machines). The architecture includes SDN-enabled Open Flow switches serving as a gateway between the local and access network connection for the internet. The host devices utilize the networking forwarding/routing services to transmit packets amongst each other. The edge node has the ability of continually processing feeds of data from IoT end devices and storage provision.

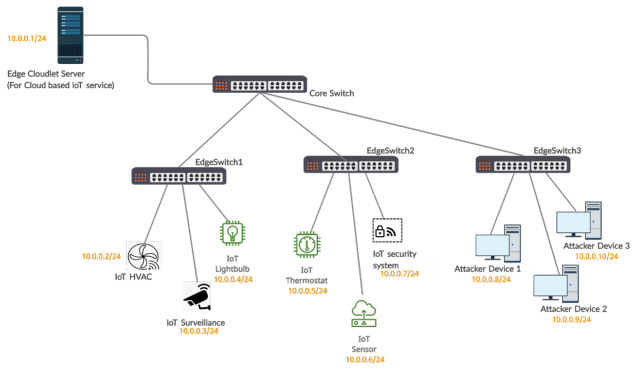

Fig. 2. Network Architecture

C. Development Environment

The project was established on a PC with a core i5 processor and a base OS of Windows. The minimal prerequisites for project execution are core i3 processor and 4 gigabytes of RAM. The aim notably incorporates a cost-effective approach, therefore open-source platforms and tools are utilized.

1) Virtualization Software: VMware was selected for its easier Networking setup, reliability, snapshot, and Management tools. VMware Workstation 16 was installed.

2) Network Emulator: In order to create and evaluate software-defined networking topologies and settings, Mininet was used network emulator.

3) Switches: Open Virtual Switch (OVS) was used to connect hosts. To communicate with the SDN controller, the OVS implements the OF protocol.

4) Controller: The controller is connected to nodes (Switches, hosts) on the network. Developed entirely in Python, Ryu, a free and open source, licensed under Apache 2.0. NETCONF, OF-config and OF was used.

5) DDoS Generation Tool: Hping3 is a tool that enables transmission of tampered packets across network. It is utilized for mimicking the effects of a UDP, TCP SYN flood, and LAND DDoS attack on the network.

VI. Implementation and Testing

A. Code-based Implementation

The Mininet topology, MTD Ryu Controller and Attack script were all written in python.The core dependencies include: Python, Xterm, Iperf, Hping3, Wireshark, Mininet, Ryu, sFlow

1) Experimental Setup:

- Terminal 1: This terminal will run the sFlow-rt client with syntax "./start.sh"
- Terminal 2: This terminal will start the Ryu controller with syntax "ryu-manager MTDSwitchController.py"
- Terminal 3: This terminal will load the Mininet topology with syntax "sudo mn –custom ./Topology.py –topo=mytopo –controller remote"
- Firefox Web browser: This is where the sFlow analytics web interface is loaded for the Mininet topology.
- Terminal 4: This terminal will load Wireshark "sudo wireshark"
- Terminal 5: Checking flows "sudo ovs-ofctl dump-flows s1"

2) Testing: The testing phase verified the features and functionalities of the program with a set of criteria tested based on the test plan.

VII. Evaluation

A. MTD Mechanism Requirement Evaluation

1) Factors: Several elements can be changed in these studies in an emulation setting to quantify the variations they generate. As factors, just a small set of variables are employed.

- Shuffling time interval: This signifies the time length that there is a shuffling of virtual IP address. Each host will be assigned a different VIP at expiration of the configured timeframe. This number will be changed for to evaluate different metrics, it is classified as a factor having 45 seconds as time parameter.
- Hping3 DDoS form: The DDOS attack forms that will be used to evaluate the performance of the MTD mechanisms consist of a UDP Flood DDoS attack, TCP SYN Flood DDoS attack and a LAND DDoS Attack via Hping3 tool all automated in the Attack script.
- Attack Scenarios: There will be two attack scenarios consisting of a point of Internal and External Attack Scenarios.

2) Parameters: They consists of the Switch, Hosts and Emulation Environments.

3) Measurement Metrics of Evaluation: The metrics by [21] are utilized to assess the proposed MTD defensive mechanisms' security, performance, and overhead impact.

VIII. Results and Discussion

1) Defence Metric: The MTD system is evaluated against the Static System to grasp the capability of the MTD mechanism to resistance of DDoS attacks in terms Defense Performance evaluation with the different factors and metrics parameters. Hping3 customized script is used for the attack and sFlow is used to monitor flow and topology traffic and of both the static network and the MTD network.

- Performance of Resisting DDoS Attacks [External]: It is assumed that the attacker knows the address range but does not know about the Virtual IPs, so the contact is to the actual network Addresses. The flow analytics shows the difference of the static and MTD network's traffic to DDoS attack from an external attacker.The attacker had no chance of success trying to attack the network with its actual network address as it drops all packet coming from hosts trying to form contact with their real addresses. The static network was overwhelmed and lead to the hosts being down and unable to carry out ping, and even leading to controller malfunction. The MTD network however did not accept any packets whatsoever and flow rules were empty even with the continuous probes by

the attack machine. The little overhead created was from continuous dropping of packets from the controller. All three attacks(UDP, TCP SYN, LAND) were combatted successfully, and uninformed attacks is proven to be unsuccessful.

- Performance of Resisting DDoS Attacks [Internal]: It is assumed that the attacker knows the address range and knows about the Virtual IPs, so the contact is to the virtual network Addresses. It is seen that the DDoS UDP traffic was dropped as soon as the shuffling event took place, and the attack surface (IP Mapping) has rechanged rendering the attack obsolete with all previous stream of traffic flows dropped. It will be near impossible for the attacker to guess the next VIP and even if it is acquired by the attacker again, it gives the attacker less time and increased cost to perform an attack. The mechanism is more defensive towards TCP SYN and LAND DDoS attack as the flow of traffic is not stable, as the mechanisms has the ability to discover probe ICMP packets. Even with variations as to the defence process to each attack, it is seen that the hostile traffic cannot affect the network for a long time and the only bottle neck will be if the reshuffling brings back a similar address range as the previous one that will continue accepting flows of traffic even while the flow rules are cleared, but this scenario is highly unlikely.

2) QoS Metric: The Overhead of SDN Controller's CPU Load was calculated here. Traffic was generated using the Iperf with various CLI parameters. TCP traffic for network's throughput, whereas UDP traffic for jitter. ICMP/PING packets for determining the network's delay latency (RTT).

- Shuffling Process Overhead: To analyse the computational cost of the shuffling event, the comparison of the impact on CPU from the controller is examined amongst each shuffling interval. The increased CPU burden is around 0.5 to 1.3 percent in comparison to the non-shuffling state. The additional computational cost is minimal and tolerable.
- Latency RTT: This represents the time it takes for a packet to travel to and from source to the destination with an ACK [26]. As presented in Fig. 3, both the static and MTD latency RTT findings are relatively similar, with just a couple spikes adding to the average delay which is attributed to the RIP-VIP translation process and switching overhead.
- Throughput: This represents the quantity of data transferred between nodes in terms of time [26]. As presented in Fig. 4, the throughput of the MTD system spike seems to be at the start of the packet transmission and all through it showed a normal and almost similar good rate of bandwidth transmission rate as the static network and is doubtful to produce a perceptible impact.
- Latency variation (Jitter): The Jitter signifies delay difference in latency between packets [26]. As presented in Fig. 5, the jitter results for the MTD network were higher than the average static network but is not a case for concern as it does not exceed the recommended 20ms rate.

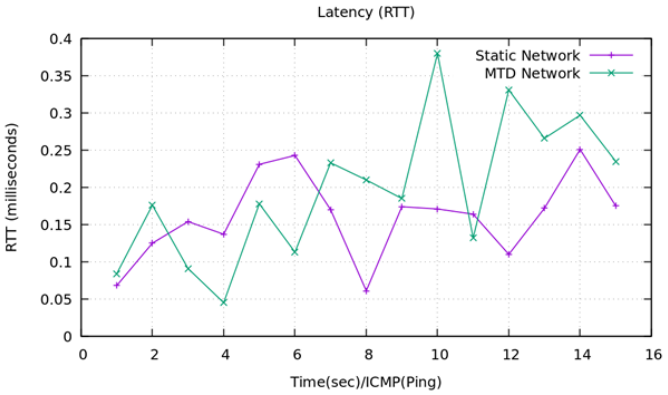

Fig. 3. Latency RTT

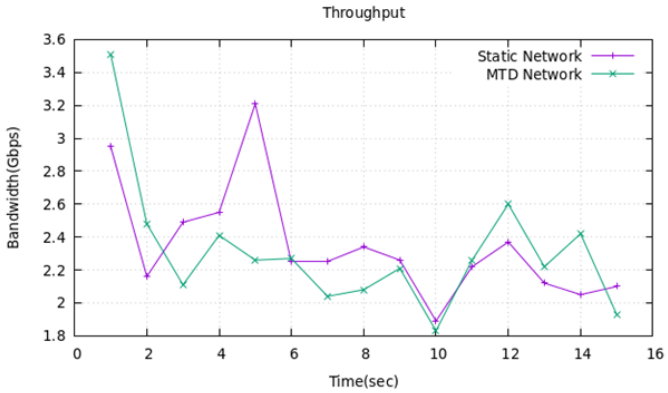

Fig. 4. Throughput

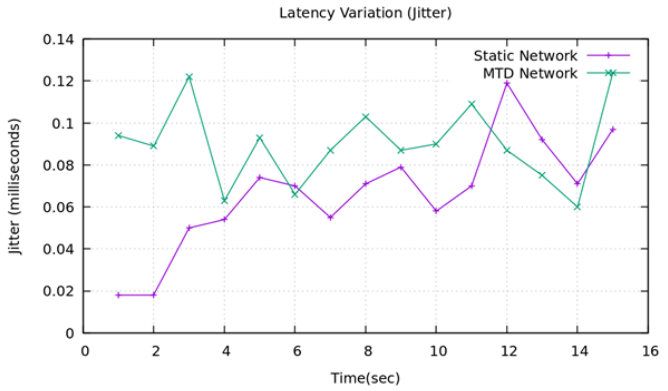

Fig. 5. Latency variation (Jitter)

IX. Conclusion

This research investigated the effectiveness of an MTD strategy based on SDN for defending DDoS attacks in IoT-Edge networks. Secondary research and the current state of the arts on SDN based MTD mechanisms against DDoS were reviewed and critically analysed to formulate the theory for the proposed system. The test scenario was based on smart

building scenario to focus on the forms of attacks attributed by the Covid pandemic targeting remote workers IoT networks and loss of availability in critical IoT system in a building. The MTD Reactive and Proactive Network Address Shuffling Mechanism implementation was thus tested and evaluated.

The mechanism delivered a satisfactory result to both by providing a top notch Defense to UDP, TCP SYN and LAND DDoS attack; preventing IoT devices to be botnet compromised due to the short lived network address while still not generating Overheads and ensuring reliable system performance and proactive security. The strategy formulated is deceptive in a form of giving a wrong perceived view of the actual network address and defensive in a way that it does not allow communication to the perceived hosts while continually dropping unrecognized traffic, clearing flows, and mutating the IP Mappings. The strategy formulated continually reshuffles virtual network address based on the set time intervals and reacts to unidentified/approved communication form. The strategy has proved to work successfully without affecting system performance and guaranteeing smooth network activity and end host communication.

A. Strengths

The strength of the MTD proposed mechanism inherently stems from its ability to combat different forms of attack stemming from reconnaissance, Dos, DDoS, and Zero Day Attacks. Additionally, it is a lightweight solution that does not degrade system performance whilst providing the required proactive moving target defence.

B. Weakness

The drawbacks in this study involves the singularity of evaluation method which could not be tested on a real SDN test bed due to lack of resource access.

C. Future Work

To cover the complete context of Cloud to Fog to Edge Computing in IoT DDoS protection and also to implement the mechanism in an actual SDN Testbed.

REFERENCES

[1] G. Kaur and P. Gupta, "Classifier for ddos attack detection in software defined networks," *Internet of Things in Business Transformation: Developing an Engineering and Business Strategy for Industry 5.0*, pp. 71–90, 2021.

[2] R. Swami, M. Dave, and V. Ranga, "Software-defined networking-based ddos defense mechanisms," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–36, 2019.

[3] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1495–1502, 2019.

[4] J. Gedeon, J. Heuschkel, L. Wang, and M. Mühlhäuser, "Fog computing: Current research and future challenges. 1. GI/ITG KuVS fachgespräche fog computing," pp. 1–4, 2018.

[5] D. P. Sharma, "Software-defined networking based moving target defenses." 2020.

[6] S. Debroy, P. Calyam, M. Nguyen, R. L. Neupane, B. Mukherjee, A. K. Eeralla, and K. Salah, "Frequency-minimal utility-maximal moving target defense against ddos in sdn-based systems," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 890–903, 2020.

[7] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and openflow: From concept to implementation," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014.

[8] A. Prajapati, A. Sakadasariya, and J. Patel, "Software defined network: Future of networking," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. IEEE, 2018, pp. 1351–1354.

[9] L. Jia, "The research on ddos attack based on botnet," in *Advances in Future Computer and Control Systems*. Springer, 2012, pp. 325–330.

[10] P. Bera, A. Saha, and S. K. Setua, "Denial of service attack in software defined network," in *2016 5th International Conference on Computer Science and Network Technology (ICCSNT)*. IEEE, 2016, pp. 497–501.

[11] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (ddos) attacks in sdn and cloud computing environments," *IEEE Access*, vol. 7, pp. 80 813–80 828, 2019.

[12] L. F. Eliyan and R. Di Pietro, "Dos and ddos attacks in software defined networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149–171, 2021.

[13] K. Kalkan, G. Gur, and F. Alagoz, "Defense mechanisms against ddos attacks in sdn environment," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 175–179, 2017.

[14] F. Chong, R. Lee, A. Acquisti, W. Horne, C. Palmer, A. Ghosh, D. Pendarakis, W. Sanders, E. Fleischman, H. Teufel III *et al.*, "National cyber leap year summit 2009: Co-chairs' report," *NITRD Program*, 2009.

[15] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a theory of moving target defense," in *Proceedings of the first ACM workshop on moving target defense*, 2014, pp. 31–40.

[16] J. B. Hong, S. Yoon, H. Lim, and D. S. Kim, "Optimal network reconfiguration for software defined networks using shuffle-based online mtd," in *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*. IEEE, 2017, pp. 234–243.

[17] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 709–745, 2020.

[18] I. A. Valdovinos, J. A. Perez-Diaz, K.-K. R. Choo, and J. F. Botero, "Emerging ddos attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions," *Journal of Network and Computer Applications*, vol. 187, p. 103093, 2021.

[19] D. Ma, Z. Xu, and D. Lin, "Defending blind ddos attack on sdn based on moving target defense," in *International Conference on Security and Privacy in Communication Networks*. Springer, 2014, pp. 463–480.

[20] A. Aydeger, N. Saputro, K. Akkaya, and M. Rahman, "Mitigating crossfire attacks using sdn-based moving target defense," in *2016 IEEE 41st Conference on Local Computer Networks (LCN)*. IEEE, 2016, pp. 627–630.

[21] Y. Zhou, G. Cheng, S. Jiang, Y. Hu, Y. Zhao, and Z. Chen, "A cost-effective shuffling method against ddos attacks using moving target defense," in *Proceedings of the 6th ACM Workshop on Moving Target Defense*, 2019, pp. 57–66.

[22] J. Narantuya, S. Yoon, H. Lim, J.-H. Cho, D. S. Kim, T. Moore, and F. Nelson, "Sdn-based ip shuffling moving target defense with multiple sdn controllers," in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks–Supplemental Volume (DSN-S)*. IEEE, 2019, pp. 15–16.

[23] L. Wang, "Shoal: A network level moving target defense engine with software defined networking," *EAI Endorsed Transactions on Security and Safety*, vol. 7, no. 25, p. e5, 2021.

[24] Y. Zhou, G. Cheng, S. Jiang, Y. Zhao, and Z. Chen, "Cost-effective moving target defense against ddos attacks using trilateral game and multi-objective markov decision processes," *Computers & Security*, vol. 97, p. 101976, 2020.

[25] X. Luo, Q. Yan, M. Wang, and W. Huang, "Using mtd and sdn-based honeypots to defend ddos attacks in iot," in *2019 Computing, Communications and IoT Applications (ComComAp)*. IEEE, 2019, pp. 392–395.

[26] M. H. R. Jany, N. Islam, R. Khondoker, and M. A. Habib, "Performance analysis of openflow based software defined wired and wireless network," in *2017 20th International Conference of Computer and Information Technology (ICCIT)*. IEEE, 2017, pp. 1–6.