IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 12, 2021, accepted January 22, 2021, date of publication January 29, 2021, date of current version February 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3055577

Securing Control and Data Planes From Reconnaissance Attacks Using Distributed Shadow Controllers, Reactive and Proactive Approaches

MUHAMMAD FARAZ HYDER[1] AND MUHAMMAD ALI ISMAIL[2], (Member, IEEE)
[1]Department of Software Engineering, NED University of Engineering and Technology, Karachi 75270, Pakistan
[2]Department of Computer and Information Systems Engineering, NED University of Engineering and Technology, Karachi 75270, Pakistan

Corresponding author: Muhammad Faraz Hyder (farazh@neduet.edu.pk)

This work was supported by the National Centre of Big Data and Cloud Computing, NED University of Engineering and Technology, Karachi, Pakistan, Ministry of Science and Technology (MoST) Endowment, NED University research grants.

ABSTRACT Moving Target Defense (MTD) is an emerging proactive Cyber Security approach. MTD constantly changes the attack surface for making cyber-attacks difficult for the invaders. Software Defined Networking(SDN) provides dynamic network design capabilities with its centralized control plane. In this paper, SMCDS (SDN based Moving Target Defense for control and data planes Security) has been proposed. The SMCDS framework safeguards against the reconnaissance attacks targeted at both data and control planes. The concept of distributed shadow controllers is introduced for securing the control plane. The MTD effect is created through the use of shadow controllers that respond to the malicious probing traffic in place of the actual controller. The availability of the distributed control plane is enhanced through the used of these shadow controllers as well. The proposed framework adopts the reactive and proactive approaches for securing the servers connected at the data plane. The reactive approach capitalizes the technique of shadow servers for providing defense against reconnaissance attacks. The proactive approach provides security enhancement through the technique of IP and port shuffling. The novelty of SMCDS framework is its capability to provide protection of both data and control planes by exploiting SDN based MTD approach. The SMCDS framework was evaluated in terms of the attacker effort, defender cost. From the results, it can be observed that the proposed framework provides security against reconnaissance attacks at a low computational cost. The prototype of the proposed SMCDS was implemented using Mininet emulator and ONOS controller.

INDEX TERMS Cyber kill chain, moving target defense, software defined networking, SDN security, reconnaissance.

I. INTRODUCTION

Cyber security is of pivotal importance in present connected era. Modern Computational technologies like Cloud Computing, 5G (Fifth generation) wireless, Internet of Things (IoT) require special care against cyber-attacks. The high computational capabilities, cheap bandwidth and ominous connectivity make these technologies highly lucrative ground for adversaries to exploit vulnerabilities. Cyber Security is an ever going game between defender and attacker, where attacker always has a competitive advantage. The attacker's edge is due to static nature of systems and networks. This provides static attack surface which can be easily exploited by the attackers.

Moving Target defense (MTD) is an active approach of cyber security. The objective of MTD is minimization of attacker's edge over the defender by continuously changing the attack surface [1]. The attack surface is fundamentally a collection of numerous resources present in the system which can be attacker's target. The constantly moving attack surface makes it difficult for the attacker to learn, predict and attack systems and networks. The term MTD was announced for the first time in 2009 [2]. Fundamentally MTD makes cyber security a level playing field for attacker and defender by eliminating the asymmetric advantages of attackers.

The associate editor coordinating the review of this manuscript and approving it for publication was Ismail Butun.

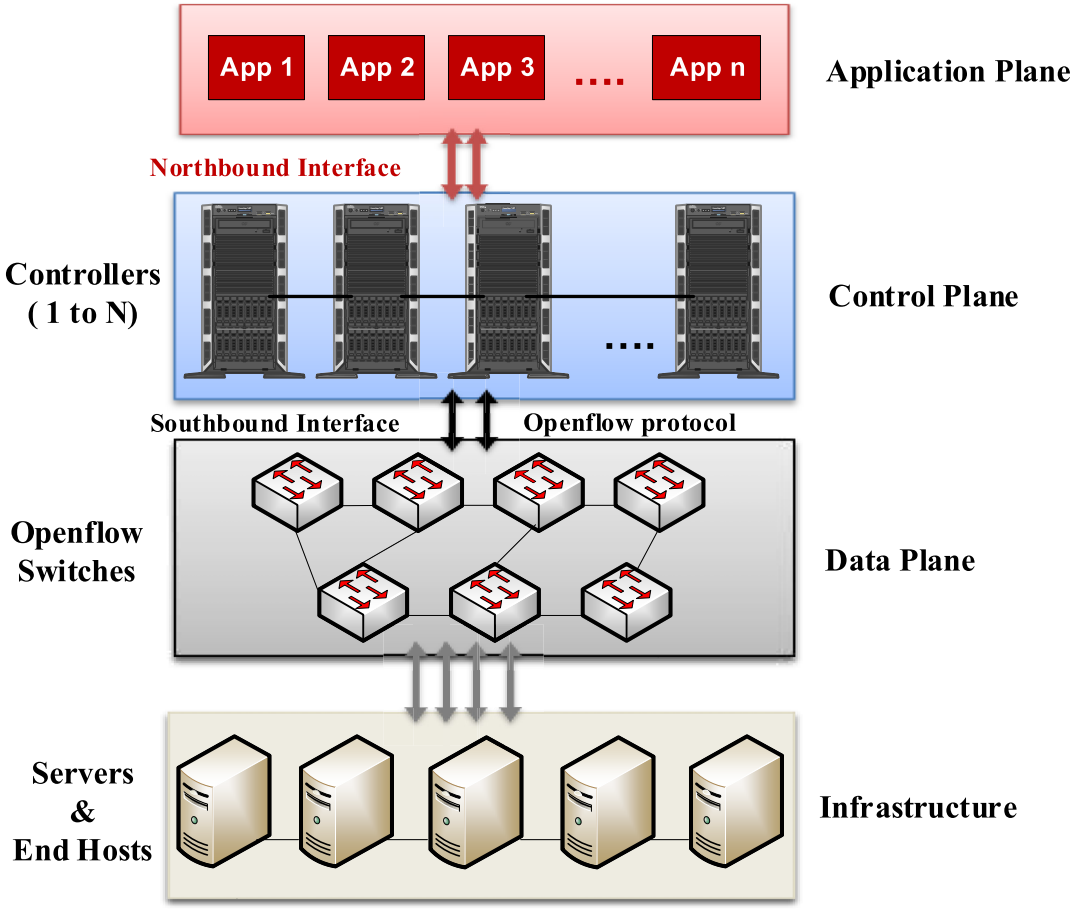

FIGURE 1. Software defined networking layers.

Software Defined Networking (SDN) has gain substantial popularity in the recent past as networking paradigm. It primarily segregates the control and data planes [3]. Its architecture comprises of three fundamental layers namely data, application and control planes as depicted in Fig.1. Control plane comprises of SDN controllers which is the controlling point of entire network. The data planes comprises of the infrastructure containing different switches. This infrastructure is controlled by SDN controller using OpenFlow protocol [4]. The southbound interface connects the control and data planes while northbound interface connects the control and application planes. SDN based security solutions are gaining popularity in the research community in the recent past [5].

Control plane security is of pivotal importance [6]as is the controlling point of entire SDN architecture. On the other hand, SDN data plane security is also critically important [7], [8], [9]. Due to its centralized management, monitoring and programmability SDN has been a popular choice for the design of MTD solutions [1], [10], [11] for data plane security only.

However, as per the best of our knowledge, there is no previous work that proposed MTD based solution for protection of both control and data planes of SDN. This work proposed SMCDS which protects the control plane using distributed controllers for creating manipulated response to reconnaissance traffic targeted towards the controller. To protect the data plane resources like web server, IP and Port shuffling approach has been proposed. The overall notion is protection against the first stage of cyber kill chain i.e. reconnaissance. The proposed SMCDS provides efficient control and data planes security at low computational cost. It also provides high reliability and availability due to distributed control plane. The distributed control plane is synchronized via RAFT consensus algorithm [37].

In our previous work [12], we proposed a model for protecting control plane of SDN using shadow controllers approach against the probing attacks. This work is an extension of our previous work with following contributions.

1) Protection of control plane by exploiting shadow controllers through different selection algorithms.
2) Reactive approach based mechanism for the protection of servers at the data plane through the use of shadow servers.
3) Proactive approach based mechanism for the protection of servers at the data plane through the use of IP and port shuffling.
4) Digital Forensics capabilities incorporation for proposed framework.
5) SMCDS system architecture development through different algorithms along with optimal MTD movement policies.
6) SDN based MTD design with multiple controllers.

Remainder of the paper is arranged as follows, preliminaries are covered in section 2, section 3 describes the related work.

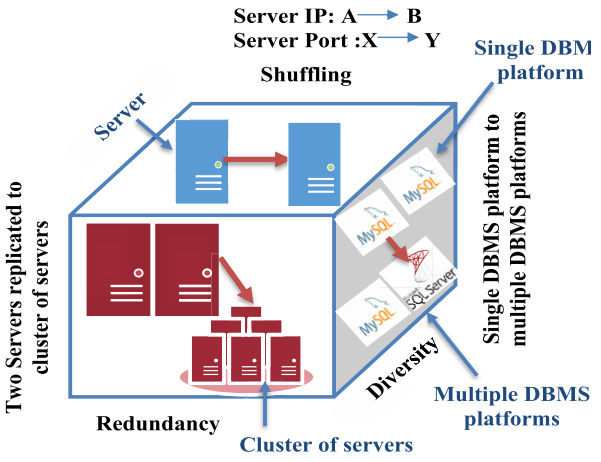

FIGURE 2. Three major classes of MTD: Redundancy, Diversity and Shuffling.

Section 4 presents the proposed SMCDS model. Detailed experimental results, reliability and performance analysis of SMCDS are covered in sections 5, 6 and 7 respectively. Conclusion and future work are discussed in section 8.

II. PRELIMINARIES

A. MOVING TARGET DEFENSE

Moving Target Defense (MTD) can be achieved through three broader classes i.e. Shuffling, Redundancy and Diversity. The core objective of all these three techniques is the change in attributes of the system either periodically or on the basis of certain events. Shuffling's aim is to change the characteristics of a system like IP address, port address etc. The redundancy technique targets the increase of resources having similar capabilities to deceive the attackers. The diversity approach objective is to deploy different platforms to achieve desire functionalities. Examples include changing the DBMS platform or webserver software etc. Modern MTD techniques also exploit the combination of these approaches. Fig. 2 depicts the three main categories of MTD techniques.

B. CYBER KILL CHAIN

A cyber kill chain is defined by Lockheed Martin as a seven step process [38]. It is used to describe attacks like Advanced Persistent Threats (APTs)

1) **Reconnaissance:** attackers collect key information like IP Addresses/subnet, hostnames, active ports, MAC addresses, vulnerabilities etc.
2) **Weaponization:** it is the preparation of different attack tools based upon the vulnerabilities discovered in the previous step.
3) **Delivery:** It is the delivery of malicious software to the victim using some appropriate communication techniques.
4) **Exploitation:** In this phase, actual exploitation occurred like attacking an email or web server or a phishing attack. Exploitation is the key point as the kill chain will proceed from left to right side.
5) **Installation:** In this phase, the backdoor or malware software is installed in the already compromised victim.
6) **Command and Control:** In this stage, command and control channels are created. The goal is to use the infected nodes to damage the assets of targeted victims.
7) **Action on Objectives:** This is the final stage of the cyber kill chain. The motivation is to unsettle the core operations of the defender and collect critical information from the victim.

C. SDN FOR DESIGNING MTD SOLUTIONS

Although MTD solutions have been implemented using different techniques, the programmability, dynamism and centralized capabilities have made SDN a popular choice for designing MTD solutions.

Openflow [4] is the main protocol behind SDN. It is the communication protocol between the SDN controller and Openflow compliant devices. It provides the controller with the capability to program and control the data planes devices. It enables the controller to dynamically modify the packet behavior. This dynamic modification is highly useful for designing MTD solutions.

III. RELATED WORK

A. SDN BASED MTD

A foundation work in the area of MTD based on SDN was proposed in [10]. The author suggested the idea of assigning virtual IP addresses to numerous nodes in the network through predefined frequencies by exploiting Openflow protocol. A framework was devised to provide a transparent real and virtual IP mapping mechanism in order to provide MTD. SDN based MTD for the protection of Internet service providers(ISP) was proposed in [1]. The frame exploits Network function virtualization (NFV) with SDN in order to provide virtual topologies to combat the attacks. The framework also provides the capabilities of Digital forensics. The proposed framework was evaluated against crossfire DDoS attacks. SDN based MTD targeting the security of data plane was proposed in [11]. The main contribution of their work is the implementation of MTD logic at the data plane switches in order to reduce the load on the controller. The framework was validated using Open vSwitch and Cloudlab testbed. The proposed framework achieved low computational cost but it is subjected to some security attacks due to decreased controller involvement. SDN based MTD with capabilities to cater the dynamic strategies of attacker was proposed in Collaborative Mutation framework [13]. The authors exploit self-learning in order to counter the adaptive attackers. The proposed MTD model uses the satisfiability modulo theories for validating different possible network state changes. The suggested MTD model was evaluated for different reconnaissance attacks generated at different frequencies. MTD framework CHAOS based on CTS(Chaos Tower Structure) was proposed in [14]. To increase the attacker's difficulty, it provides obfuscation at different levels of network. It incorporates an Intrusion

detection system (IDS) module for the detecting malicious traffic. A fingerprinting attack protection model using SDN was proposed in [15]. The framework protects against active and passive fingerprinting attacks targeted towards hosts. The proposed framework models the attack and defense mechanism as sequence of one-shot games. Authors in [16] proposed FRVM which is based IP multiplexing approach via random selection to provide SDN based MTD. FRVM provides host with random IP based upon time duration. FRVM was analyzed in terms of attacker's success probabilities. A method for the throttling the reconnaissance attacks using virtual topologies using SDN was devised in [17]. The virtual topology framework focused on the insider attackers. A prototype of RDS (Reconnaissance Deception system) was implemented which comprises of the Deception server, SDN controller, Honey pot server, scanning detection module, SDN controller etc. The proposed framework was evaluated for performance overhead and security. Authors in [18] developed a model MASON for the protection of Cloud Computing resources connected via SDN. The work focused on the effectiveness of SDN based MTD against Cloud intrusion attacks and network vulnerabilities. The authors exploited port hopping techniques. In order to model the threat score, it utilized PageRank algorithm.

B. SDN CONTROL PLANE SECURITY

SDN control plane security is crucial for the successful operation of SDN networks since it is the brain of SDN. It has been an active area of research [19]. Moreover large SDN solutions requires distributed control plane. These distributed control plane has advantage of high availability and reliability but also have different security challenges. The most exploited attack against controllers is DDoS [6], [20]. In order to defend the DDoS attacks on control plane a framework FloodGuard was introduced in [21]. It fundamentally consists of two core components, one is packet migration module the other is proactive flow analyzer. Packet migration essentially buffers the flooding traffic before sending to controller via using packet round robin and rate limit scheduling techniques. The role of flow analyzer is proactively produce flow rules based upon the numerous applications running on controller. The goal is to mitigate the saturation flood attacks against control plane. The prototype was implemented using the POX controller. A DDoS protection mechanism ArOMA for SDN control plane security for an ISP network was proposed in [22]. The proposed model focused on collaborative effort of service provider and its customers for the protection of DDoS attack against the control plane of SDN. The DDoS protection policies are devised based upon the customer side recommendations. The proposed framework was implemented using Ryu controller and Mininet [23]. Distributed SDN control plane based framework was introduced in [24] in order to provide high availability. The proposed framework used the idea of making 3-nodes clusters of controllers. One of controller inside the cluster act as master node while rest as client nodes. The framework was analyzed on Amazon Web Service (AWS) cloud, ONOS and HP VAN SDN controllers. The results confirm higher availability of control plane in the events on unexpected high loads. A framework for the protection of control, Data and Application planes of SDN in smart city applications against DDoS was introduced in [7]. To protect the control plane, authors proposed the use of backup controllers and switch migration strategies. Initially, backup controllers will be used for the purpose of load balancing and once the affective switch is identified, it will use switch migration techniques to mitigate the attack. The proposed SEAL framework was implemented using ONOS controller, Mininet [23]. Authors in [25] proposed framework SGS for the protection of control plane. The model comprised of two core components namely controller defense and anomaly traffic detection. The controller defense uses cluster of controllers to dynamically mapping the affected controller. It also issue different access control messages to switches in order to block the attackers. Role of anomaly detection was to segregate legitimate and malicious flows using feature vector comprises of four tuples. Ryu SDN controller and Mininet were used for the implementation of proposed framework. A method for the finger-printing of the SDN with higher granularity capabilities along with the protection against such attacks was proposed in [26]. The work highlights the security threats pertaining to the disclosure of sensitive information due to controller switch interactions. The author proposed time base analysis approach to capture sensitive SDN information. The proposed solution is independent of controller platform with low computational overhead. Lee *et al.* [27] proposed a framework DELTA for the assessment of security of SDN with capability to run with different controllers platforms. The tool is capable of generating known security vulnerabilities as well as to some extends unknown security attacks in SDN environment. In [28] the authors focused on specific attack table-miss striking and its severity over the traditional saturation attack. The work also proposed SDNGuardian countermeasure technique against this type of attack. The proposed solution protects the switch flow table, device CPU utilization and bandwidth of control channel.

C. SDN DATA PLANE SECURITY

SDN data planes composed of different network infrastructure and hosts. SDN data plane security is of pivotal importance. The centralized control plane of SDN provides opportunities for dynamic security solution and network monitoring. SEAL is a framework proposed in [7] for the protection of all three frames of SDN. To secure data plane against DDoS, it uses three strategies namely Traffic blocking, Traffic redirection and Traffic drop. The main goal of their approach is to protect data plane and avoid DDoS attack at the control and application planes. A device compromised at the forwarding plane can have devastating impact on the operations of SDN. The work presented in [8] highlights the threats that are associated with compromised data plane devices on SDN based Cloud computing environment. The authors demonstrated the new threat model related to SDN based Cloud environment.

The work proposed a worm that affected a substantially large number of virtual machines. The proposed model was analyzed using Open Vswitch [29] and Openstack Cloud environment. A mechanism for the verification of IP forwarding mechanism was proposed in SDN environment was proposed in [30]. The proposed DYNAPFV exploits the SDN environment's central controlling mechanism to detect any statistical violation in flows and packet behavior. The model dynamically alters the sampling rates of packets and flows in order to minimize the load incurred due to verification mechanism. The prototype of the solution was implemented using Mininet and Floodlight. A security model FloodDefender for the protection of both control and data planes was proposed in [31]. The suggested model comprised of three different techniques for the protection of control and data planes. The first one is flow rule management for the elimination of flows that are not required in order to reduce flow table size of openflow switches. The second technique is Packet filtering to reduce attack traffic directed towards the control plane. The last method was reduction in traffic directed towards controller in case when attacker generated excessive amount of table-miss packets. Ryu SDN controller and Mininet were used to implement the FloodDefender. The authors in [9] suggested a model for the protection SDN from malicious end hosts. The notion is the protection of both control and data planes. The solution comprised of SMA i.e. Security Management Application which runs in control Plane while SSC i.e. Switch Security Components running on the switches in the Data plane. To implement the solution Xen Hypervisor, OpenFlow switches, ONOS SDN controller etc., have been incorporated. A network security model PivotWall was proposed in [32] to protect against the stealthy and advanced persistent attacks. The authors proposed a language for specifying the information flow control. The prototype was implemented using POX controller and Open Vswitch. The solution extend the host based tracking to centralized SDN controller. The proposed solution comprises of central SDN application with host based agent.

IV. PROPOSED SMCDS ARCHITECTURE

Both control and data planes security mechanisms of the proposed SMCDS framework highly integrated to ensure efficient performance and security enhancement for overall operations of SDN. The core components of the proposed SMCDS model are depicted in Fig. 3. It comprises of the following components.

A. RECONNAISSANCE DETECTION MODULE (RDM)

RDM has two distinct components in order to detect the malicious traffic directed towards controller and data planes. An Intrusion Detection System (IDS) SNORT [36] is a core component of RDM. Rules customization have been performed and then applied for probing traffic recognition. SNORT is one of the most widely used open source IDS that provides efficient results. In this paper, the detection technique is designed to avoid false positives and false negatives by taking into consideration the appropriate parameters for the detection of reconnaissance traffic. According to the threat model, attackers can initiate probing traffic against the data plane's resources and the controller. RDM's responsibility is the detection of scanning traffic. There are two components of RDM. One is the control plane RDM and the other is data plane RDM. The goal of the control plane RDM is to detect the reconnaissance traffic directed towards the controllers. Data plane RDM can detect the probing traffic targeting the servers and end hosts in the data plane. However, to simplify the experimental analysis, attacks are considered only against the servers.

B. MOVEMENT DECISION MODULE (MDM)

MDM decides the policy for the movement. In order to defend the control plane, MDM will select one of the deception controllers from the pool of ''k'' available deception controllers. This selected deception controller will respond to the reconnaissance traffic. Two techniques namely Random and Round Robin are used for shadow controller selection. Two approaches namely reactive and proactive are incorporated for the data plane security. In the proactive method, port and IP addresses of the server are shuffled on periodic basis. Whereas, in the reactive approach, shadow webservers and load balancers will respond to the reconnaissance traffic similar to the approach adopted at the control plane.

C. MTD MONITORING MODULE (MMM)

The function of MMM is to monitor state of the overall MTD framework. MDM movement decision is based upon the feedback provided by this module. It also determines the effects of MTD in the system and how to alter the frequency of movement to produce optimal performance.

D. DIGITAL FORENSIC MODULE

The importance of digital forensics cannot be ignored for any network. MTD also imposes greater challenges for digital forensics due to constant changes in different system attributes. Therefore, a digital forensics module has been developed for the proposed SMCDS framework. This module consists of two sub components namely data collection and data analysis. In order to perform the forensics at both planes, the module stores important logs from the system. Adding the digital forensics module increases the defender cost. However, as elaborated in the Results section, this cost is minimal.

E. SHADOW CONTROLLERS

In order to throttle the reconnaissance traffic targeting the controllers, the proposed SMCDS architecture exploited the concept of shadow controllers. SMCDS framework is built using distributed control plane comprising of ''N'' controllers along with ''k'' additional shadow controllers. The main role of these shadow controllers is to respond to the probing traffic directed towards the SDN controllers. These shadow controllers also increase the availability of the control plane in case one of the main controllers goes down.

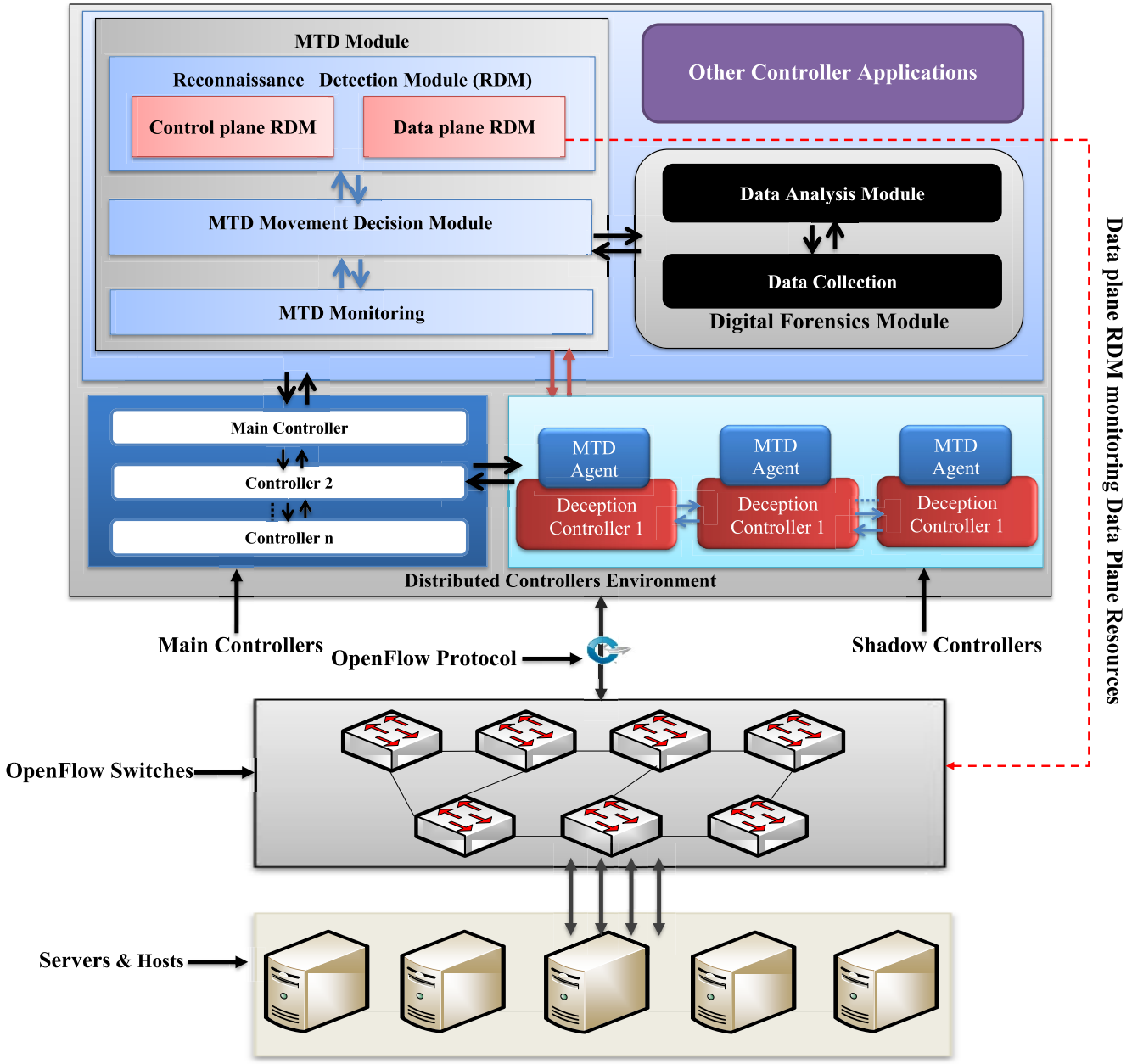

FIGURE 3. The proposed SMCDS Architecture.

F. SHADOW WEB SERVERS AND LOAD BALANCERS

The presented SMCDS framework utilized the concept of shadow web servers and load balancers for the data plane servers protection under reactive approach.

There are four algorithms proposed in this work. These algorithms are implemented at the control plane of SDN. These algorithms are described in detail in the following section.

Algorithm 1 performs the detection and redirection of reconnaissance traffic at the control plane. The algorithm depicts the utilization of shadow controllers. SDN network composed of "k" shadow and "N" distributed controllers. The algorithm detects packets based upon different TCP/IP information like source and destination IP and port addresses. Upon the detection of interesting traffic, it will select one out of "k" shadow controllers in order to produce a manipulated attack response. The selection of shadow controllers is based upon Round Robin and Random techniques. Although, algorithm 1 indicates only Round Robin technique; however, Random selection technique was also used. Table 1 lists the different abbreviations used in algorithms 1 to 4.

Algorithm 2 indicates the protection at the data plane under a reactive approach via probing traffic detection and redirection. The algorithm provides a multilevel defense approach

Algorithm 1 Reconnaissance Traffic Detection at Control Plane and Response Generation

```
SDN Network initialization with different servers and Distributed and Shadow controllers
function PacketArrival (dstIP, dstPort,srcIP, srcPort )
if dstPort!=LLDP AND dstIP==controllerIP AND srcIP!=switchIP then
    SC = = RoundRobinSelection (list of K controllers)
    Set IP_SC==IP_Probed_controller
    Set Port_SC==Port_Probed_controller
    Attacker ←Probing_traffic_Response_Send
else
    Normal_SDN_Forwarding()
end if
```

TABLE 1. List of abbreviations used in algorithms.

Symbol	Abbreviation
SC	Shadow controller
LLDP	Link Layer Discovery Protocol
SL	Shadow Load Balancer
SW	Shadow Web Server
dstIP	Destination IP Address
srcIP	Source IP Address

for different servers connected in the data plane. There are frontend load balancers connecting multiple webservers behind them. The attacker's generated probing traffic will first reach the load balancers. Therefore, in order to counter such attacks, a shadow load balancer will be used to respond to the reconnaissance traffic. The selection of shadow controllers is based upon Round Robin and Random techniques similar. The selected shadow load balancer will respond to the reconnaissance traffic. The IP and port address of the shadow load balancer will be modified to match that of the targeted load balancer. If the attacker successfully identifies the load balancer, their next target will the webservers running behind the load balancers. The attacker will then run the reconnaissance traffic against these webservers. Therefore, this algorithm provides a second level of defense by using the concept of shadow webservers. To respond to the probing traffic, these shadow webservers will be selected based upon Random and Round Robin techniques similar to the shadow load balancers approach.

A proactive approach for protection of data plane servers is presented in algorithm 3. In this technique the IP address of load balancer is shuffled with a frequency of 120 seconds. Moreover, the port address of web servers is shuffled with a frequency of 60 seconds as presented in algorithm 4. The rationale behind this delay is the fact that the IP Address of the load balancer change will require a DNS update as well. The ports are shuffled every 60 seconds that is twice quickly compared to the IP Addresses. The reason is to increase the frequency of movement in order to keep negating the time required by the attackers to get useful information about servers.

Algorithm 2 Reactive Approach: Detection of Reconnaissance Traffic and Response Generation at the Data Plane

```
SDN Network initialization with different servers and Distributed and Shadow controllers
if Data_Plane_Security==REACTIVE then
    function PacketArrival (srcIP, srcPort, dstIP, dstPort)
    if dstIP==LoadBalancerIP AND Port=LoadBalancer_port AND prob_freq> threshold OR SenderIP is listed in Malicious attackers list then
        SL==ShadowLoadBalancerSelection-RoundRobin(List of k shadow load balancers)
        Set IP_SL=IP_Probed_LoadBalancer
        Set Port_SL =IP_Probed_LoadBalancer
        Attacker ←Probing_traffic_Response_Send
    end if
    if dstIP==WebServer_IP AND Port=WebServer_port AND prob_freq> threshold OR SenderIP is listed in Malicious attackers list then
        SW==ShadowWebServerSelection_RoundRobin (List of k shadow web servers)
        Set IP_SW =IP_Probed_Webserver
        Set Port_SW=Port_Probed_Webserver
        Attacker ←Probing_traffic_Response_Send
    end if
else
    Normal_SDN_Forwarding()
end if
```

Algorithm 3 Proactive Approach Through IP Shuffling for Data Plane Security

```
SDN Network initialization with different servers and Distributed and Shadow controllers
if Data_Plane_Security==PROACTIVE then
    IP Shuffling Starting
    Delay(120)
    IP_Load_Balancer==select_ip(pool_range)
else
    Normal_SDN_Forwarding()
end if
```

The traffic flow sequence of SMCDS for the control plane security is shown in Fig. 4. "k" shadow controllers are present with "N" distributed controllers. The objective of control plane RDM is the detection of any reconnaissance traffic targeting the control plane. Various users through end hosts and switches are connected to the SDN network. A normal traffic forwarding approach has been followed for the benign user. In the normal traffic forwarding approach, the controller is contacted against each forwarding request. In response, the controller will insert the required flows. In the case of malicious reconnaissance traffic, one of the "k" shadow controllers will respond to the probing traffic. Random and Round Robin techniques are employed to pick out the shadow controller. The IP address of the chosen shadow

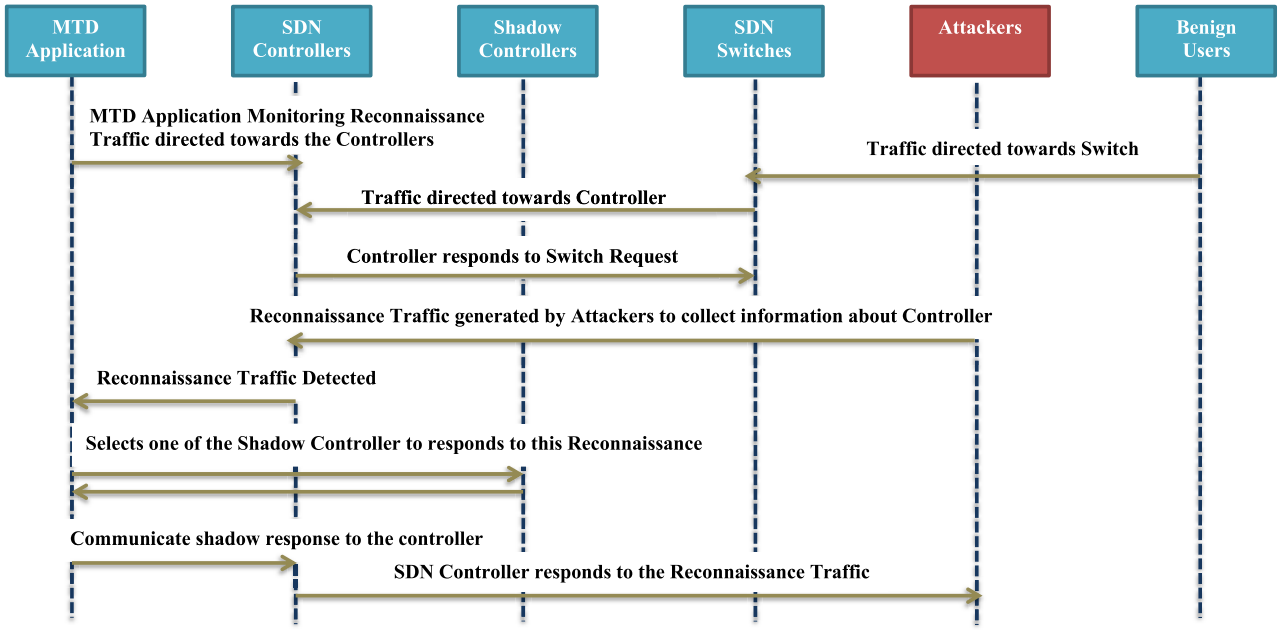

FIGURE 4. The sequence of SMCDS for Control plane protection.

Algorithm 4 Proactive Approach Through Port Shuffling for Data Plane Security

```
SDN Network initialization with different servers and Distributed and Shadow controllers
if Data_Plane_Security==PROACTIVE then
    Port Shuffling Starting
    Delay(60)
    Port_Load-Balancer==select_ip(pool_range)
    Port-Web-servers= Port_Load_Balancer
else
    Normal_SDN_Forwarding()
end if
```

controller will be updated so that the attacker considered it as the targeted controller. Through the IP modification strategy, the technique guarantees that the attacker will target the decoy server in subsequent stages of attack instead of the actual controllers.

The sequence of events that occurred while securing the data plane through a reactive approach is represented by the sequence diagram in Fig. 5. The controller will inject the required flows into the switches as usual SDN forwarding, in case of benign users attempting to connect to the web servers. The RDM module in the data plane of SMCDS is responsible for detecting probing traffic targeting the web-server. Whenever the probing traffic is detected, the response will be generated from one of the "K" shadow web servers. The selection is based on any one of the mechanisms from the Random and the Round Robin techniques. The IP address of the selected shadow webserver will be updated as per the targeted webserver and then the shadow webserver will respond to the reconnaissance traffic. For future analysis and data forensics, the IP address of the attacker will also be added to the database. The stored IP address will also be blocked at the firewall.

Fig. 6 depicts the security of the data plane through a proactive approach. Port and IP shuffling has been performed in a proactive approach. The shuffling frequency of 120 seconds is set for the IP address of frontend load balancers while for web servers, the port address shuffling frequency is 60 seconds.

V. RESULTS AND DISCUSSION

A. THREAT MODEL

In our threat model, the attacker can run reconnaissance attacks against both control and data planes. Further, in our target SDN network, attackers can be connected directly or indirectly. Both controllers and data plane servers are attacker targets. Attackers will run varying scanning attacks for deducing information regarding the controller. Also, they will run scanning attacks against the multiple servers in the data planes. In comparison to previous works, our work considers reconnaissance attacks both at SDN data and control planes.

B. SCANNING TECHNIQUES

Several number of scans ranging from 1 to 3200 were performed through nmap [34] for analyzing the security of control and data planes. The scanning techniques are IP and port scanning.

C. EXPERIMENTAL SETUP

The SMCDS framework was realized using Mininet [23] and Distributed ONOS controller [33]. Both were implemented as virtual machines on the DELL Server having Intel Xenon Processor E5-2620. There are 32 CPUs with 2.1 GHz speed and 32GB RAM. The scanning traffic was produced using Nmap [34]. The experimental setup for the proposed framework is shown in Fig. 7.

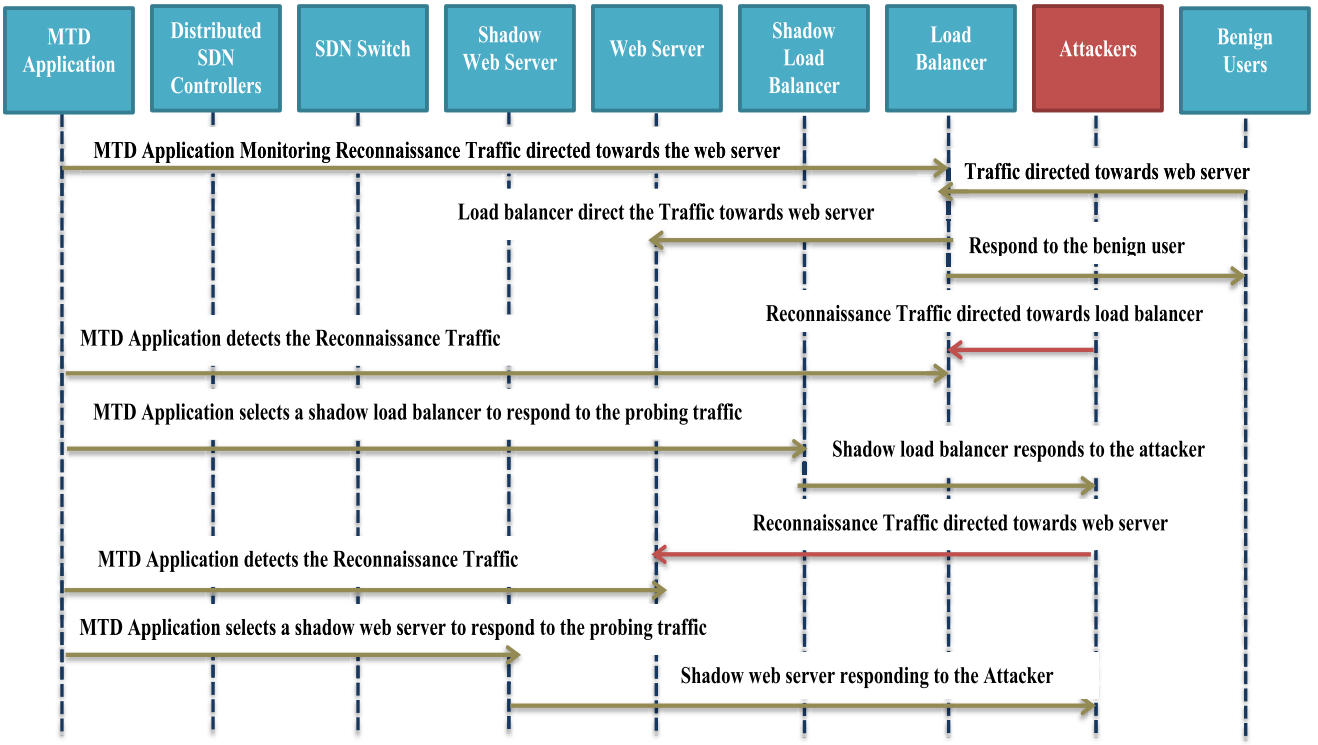

FIGURE 5. The sequence of SMCDS for data plane protection in the case of Reactive Approach.

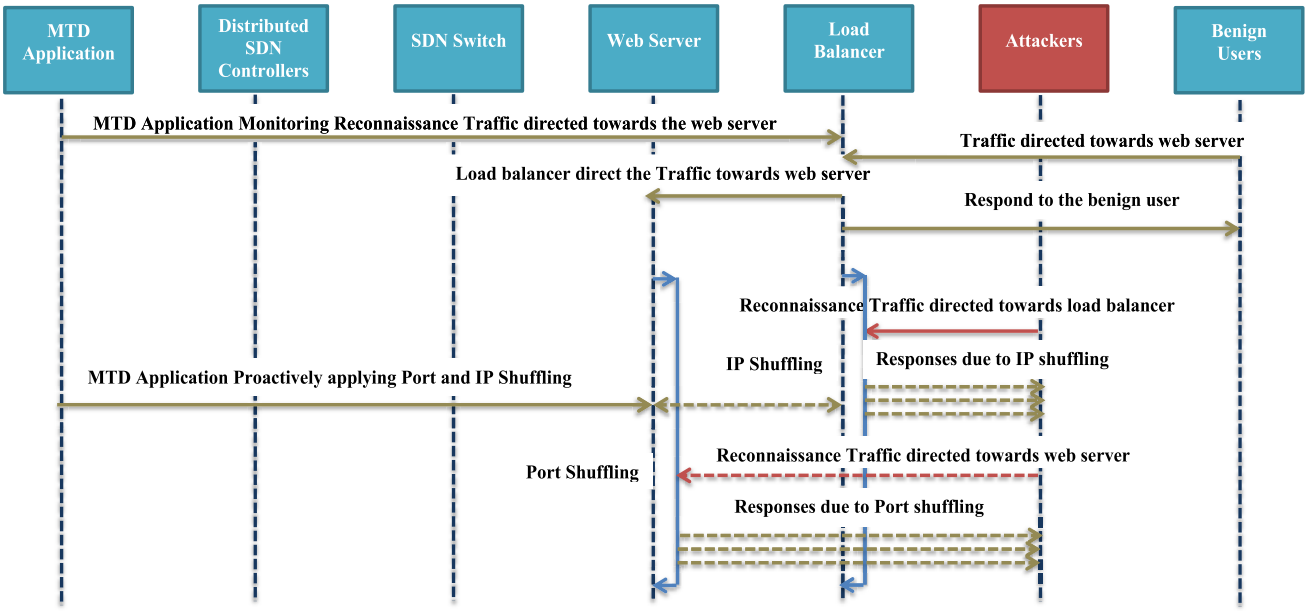

FIGURE 6. The sequence of SMCDS for data plane protection in the case of Proactive Approach.

D. CONTROL PLANE PROTECTION

According to algorithm 1, the shadow controllers are selected based upon Random and Round Robin schemes. Defender success is the ability to respond to the probing traffic from one of the shadow controllers instead of letting the attacker to prob the actual controller. The defender's success for Round Robin selection of shadow controllers is depicted in Fig. 8. Defender's success is minimum for the case of the highest number of scans and the smallest number of shadow controllers. In other words, the attacker's success probability

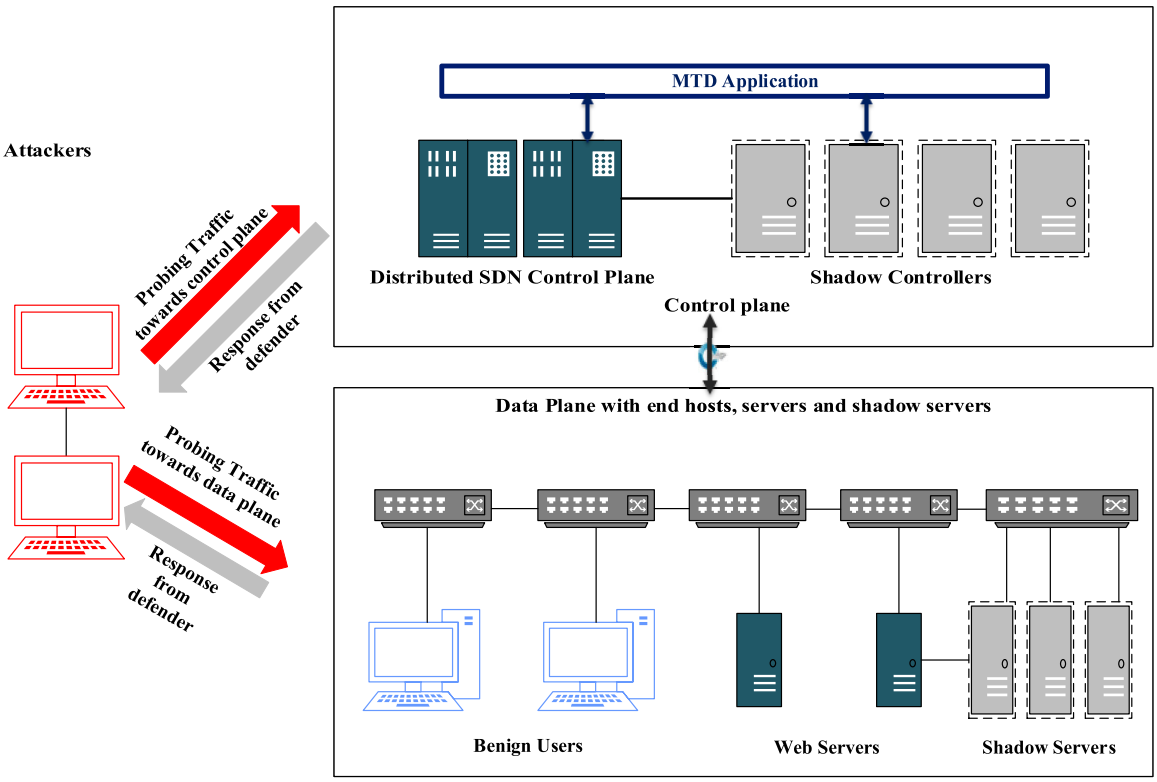

FIGURE 7. SMCDS simulation setup.

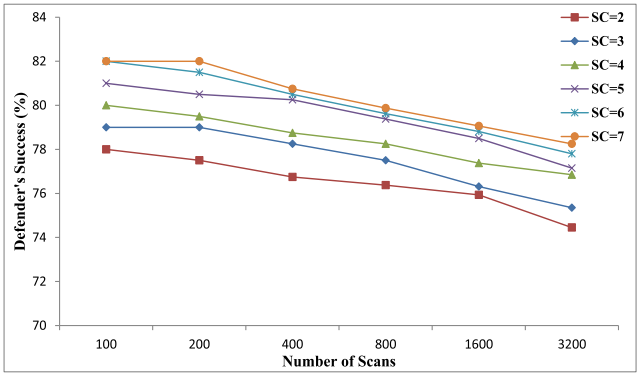

FIGURE 8. Defender success at the control plane in the case of selection of shadow controllers via Round Robin technique.

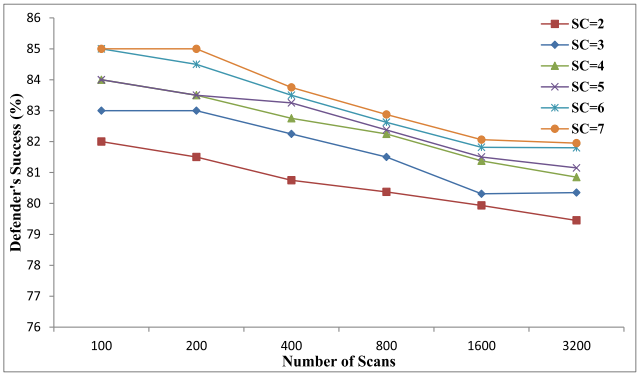

FIGURE 9. Defender success at the control plane in the case of selection of shadow controllers via Random technique.

rises as the number of scans increases. The defender's success varies from 74.45% (for 2 shadow controllers and 3200 scans) to 82% (for 7 shadow controllers and 100 scans). Different parameters impact the defender's success including the number of shadow controllers, number of scans, selection mechanism of shadow controllers. Defender's success for the case of Random selection is presented in Fig. 9. In this case, the defender's success varies from 79.5% (2 shadow controllers, 3200 scans) to 85% (7 shadow controllers, 100 scans). The experimental analysis considered maximum 3200 scans. This number is a pragmatic limit for reconnaissance traffic because a higher number of scans increases the probability of detection of an attacker by the IDS or firewall system of the defender. The results indicate that the Random selection scheme performed marginally better compared to the Round Robin. Moreover, the defender's success did not increase substantially beyond 7 shadow controllers.

E. DATA PLANE SERVERS PROTECTION USING SMCDS

Reactive and proactive approaches are applied for the protection of data plane servers against probing traffic.

1) REACTIVE APPROACH

The shadow servers are used for countering the reconnaissance traffic in reactive approach. We have considered the

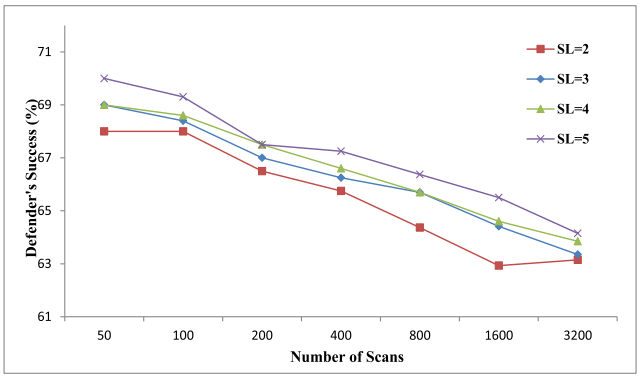

FIGURE 10. Defender success at the data plane in the case of selection of shadow load balancers via Round Robin technique.

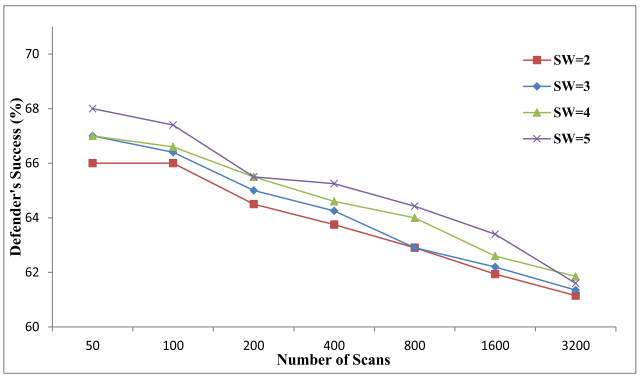

FIGURE 12. Defender success at the data plane in the case of selection of shadow web servers via Round Robin technique.

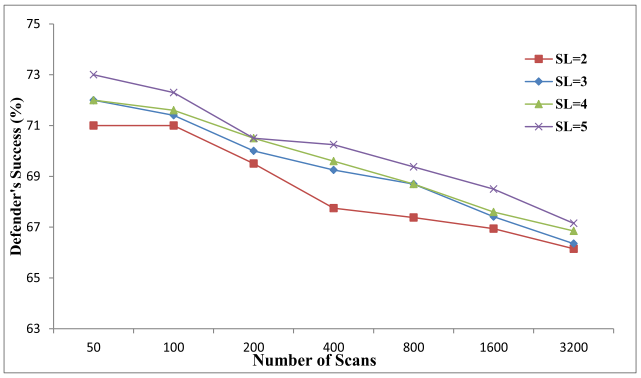

FIGURE 11. Defender success at the data plane in the case of selection of shadow load balancers via Random technique.

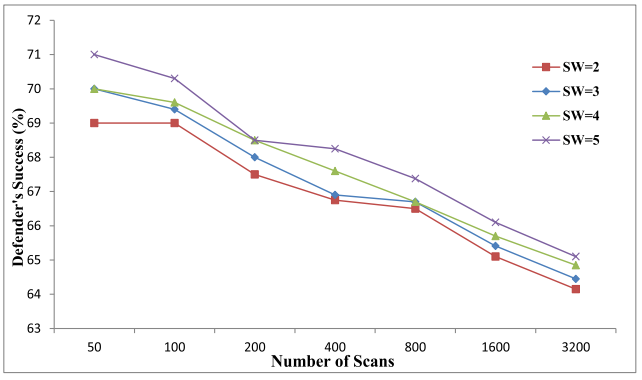

FIGURE 13. Defender success at the data plane in the case of selection of shadow web servers via Random technique.

case of web servers running behind load balancer for experimental analysis. The load balancers are implemented using Nginx [35]as reverse proxy. The attacker generated the probing traffic against the load balancer. In order to respond to this traffic, a shadow load balancer will be selected using Round Robin and Random selection based upon algorithm 2. The pictorial representation of the same is depicted in Fig. 10 and Fig. 11. In case of Round Robin, defender's success varies from 63.1% (2 load balancers, 3200 scans) to 70% (5 load balancers, 50 scans). The defender's success ranges from 66.15% (2 load balancers, 3200 scans) to 73.2% (5 load balancers, 50 scans) in the Random selection scheme. Once the load balancer is successfully discovered, attacker will then proceed towards web servers. The defender's success against the web server probing attack is presented in Fig. 12 and Fig. 13. In case of Round Robin technique, defender's success increases from 61.1% (2 web servers, 3200 scans) to 68% (5 web servers, 50 scans). Moreover, 64.1% (2 web servers, 3200 scans) to 71% (5 web servers, 50 scans) defender's success attained by using Random selection technique.

2) PROACTIVE APPROACH

Through periodic modification in IP and port addresses, a multilevel proactive MTD approach has been adopted.

The **IP shuffling technique**is used for modifying the load balancer's IP address. DNS modification technique is also implemented so that the IP modification is transparent from the end user. Binomial Probability distribution function is applied for calculating the Attacker success probability (ASP) as:

$$P(X = x) = \binom{k}{x} * p^x * (1-p)^(k-x) \quad (1)$$

As the load balancer's public IP can not be modified very frequently, therefore, we have used a small address space of N=256 for public IP modification. Moreover, we have to limit the address space as there is cost associated with public IPs. Attacker success probability (ASP) is calculated after simplifying equation 1 as equation 2. From equation 2, it is observed that a host can be discovered by the attacker in k scans for an address space N.

$$ASP = P(0 < X \leq N) = 1 - (1 - v/N)^k \quad (2)$$

Here, "N" represents the address space, "k" indicates the number of scans, "v" shows the number of vulnerabilities. In this case, N=256, v=1 and k=500. The Defender success probability (DSP) can be computed as

$$DSP = 1 - ASP \quad (3)$$

Fig. 14 indicates that the DSP value reduces from 1 to 0.02 as the number of scans increases from 1 to 1000 for address space having value 256. This indicates that the attacker can effectively discover IP address of frontend load balancer with a probability value of 0.98 for 1000 scans.

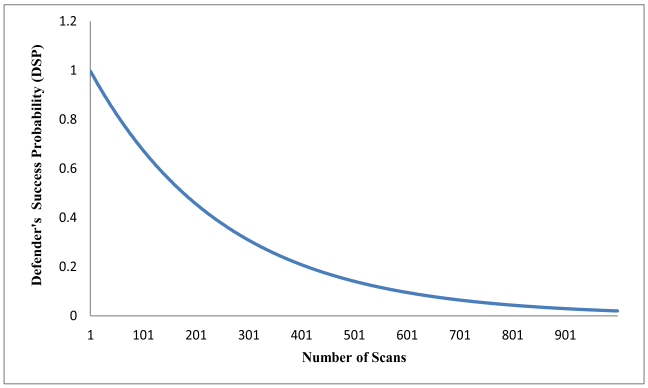

FIGURE 14. DSP in the case of IP shuffling technique at the load balancer.

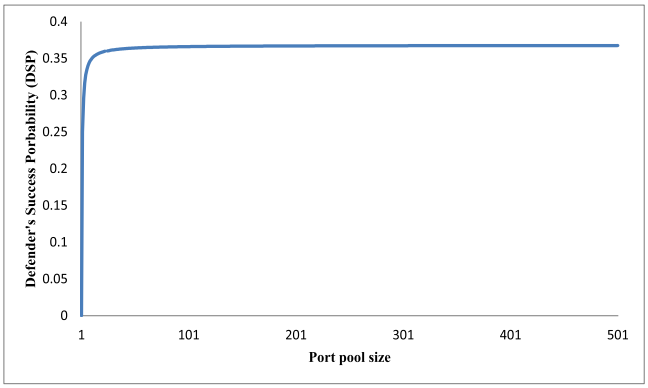

FIGURE 15. DSP in the case of port shuffling technique at the web server.

Port Shuffling Port shuffling technique is adopted at the web server level running behind a load balancer. The ports ranging 1024-65535 are used in order to perform the port shuffling excluding the well known ports 1-1024. Fig. 15 presents the DSP value which reaches a contact value of 37% as the number of ports rises. It indicates the attacker's success can reach a maximum value of 67%. The maximum available value of 64511 ports for shuffling makes it substantially difficult for the attacker to determine the same port across different scans.

F. DIGITAL FORENSICS

Digital forensic is a critically challenging task in the domain of MTD because of attack surface continuous variation. This makes forensics analysis more challenging compare to non-MTD based systems. Digital forensics functionalities provided at the data and control planes are an important attribute of the proposed SMCDS framework. Interesting traffic at the control plane level is the reconnaissance traffic directed at the controller. In order to store this information, an entry of 17 bytes is required. This includes 4 bytes each for the controller and source IP address of the attacker, 2 bytes for ID and 7 bytes for entry time and date fields. Whereas, at the data plane level in order to store forensics information 21 bytes are needed for an entry. This includes 2 bytes for ID field, 7 bytes for time and date field and 4 bytes each for storing IP addresses of the attacker, load balancer and web servers. The logs stored in the digital forensics module will help in identifying the attacker's footprints. Moreover, it will also provide substantial help in blocking the attacker's IP addresses. The cost related to storage is computed as:

$$C_{ST} = NumberofScans * StorageRequiredforonescan \quad (4)$$

VI. RELIABILITY OF THE PROPOSED SMCDS MODEL

MTD approaches based upon the Redundancy technique enhance the reliability of overall system [39]. The proposed SMCDS model is reliable because it consists of multi-controllers. This approach increases availability and reliability of control plane. The shadow controllers also add to the reliability of SMCDS. The cluster formation in ONOS is achieved via the RAFT consensus algorithm [37] which is an efficient and reliable technique.

Similarly, at the data plane, the SMCDS exploits shadow web servers and load balancers not only to throttle the attacker but also provides a substantial increase in reliability.

VII. PERFORMANCE EVALUATION OF SMCDS

This constantly changing attack surface of MTD reduces attacker advantage but it also impacts the system performance. The proposed SMCDS is evaluated in terms of attacker and defender cost. The ideal design goal of MTD is to increase the attacker cost. The defender and attacker cost is estimated for control and data planes for different strategies.

A. ATTACKER COST

Attacker cost is dependent on accuracy of probing traffic detection, number of scans performed by the attacker, MTD technique adapted by the defender, and number of shadow servers/controllers. MTD method can be reactive or proactive as elaborated in the previous section. Attacker cost can be calculated as:

$$C_{ATT} = A_{detection} + N_{scan} + N_{shadowserver} + MTD_{approach} \quad (5)$$

where, C_{ATT} represents the attacker cost, $A_{detection}$ represents scanning traffic detection accuracy, N_{scan} indicates the number of scans performed by attacker, $N_{shadowserver}$ is the count of shadow servers and $MTD_{approach}$ is the MTD strategy adapted by the defender like reactive or proactive.

B. DEFENDER COST

1) CONTROL PLANE

Incorporation of MTD in the system will add to the cost. Therefore, we have formulated the defender's cost by considering the factors added due to the introduction of MTD as shown in equation 6.

$$C_{DEF\_CP} = K * C_{PR\_SC} + C_{ST} + C_{REC\_CP} \quad (6)$$

where, K represents shadow controllers' count,C_{DEF_CP} is the defender cost at the control plane. C_{PR_SC} is the shadow controller's computational power, C_{ST} is the storage cost associated with digital forensics at the control plane and C_{REC_CP} is the reconnaissance detection cost at the control plane.

The defender cost at the control plane depends on the count of shadow controllers along with the computational cost associated with each of them, reconnaissance detection cost, storage cost related to log maintenance for digital forensics purpose. There is no IP or port shuffling technique at the controller level. Moreover, the container technology is used to implement the shadow controllers that require low computational power. The storage cost C_{ST} is 17 bytes for an entry at the control plane level as discussed in the section of digital forensics.

2) DATA PLANE

In the case of **Reactive approach**, the data plane's defender cost will be as follows.

$$C_{DEF\_DP\_R} = m * C_{PR\_SL} + n * C_{PR\_SW} + C_{ST} + C_{REC\_DP} \tag{7}$$

where, n represents decoy web servers' count, m indicates the shadow load balancers' count, C_{PR_SL} and C_{PR_SW} represents the computational cost of shadow load balancer and shadow web servers respectively, C_{REC_DP} is the cost of detection of probing traffic at the data plane, C_{ST} is the storage cost.

In **proactive approach** at the data plane, IP and port addresses shuffling at load balancer and webserver are the main contributors of the added cost. IP shuffling also requires DNS update. However, for limiting the cost overhead, IP shuffling address space is restricted to 246 only as mentioned in the previous section. Equation 8 represents the defender's cost at the data plane under proactive approach.

$$C_{DEF\_DP\_P} = IPS_{LW} + PortS_{WS} + DNS_{LBIPupdate} + C_{ST} + C_{REC\_DP} \tag{8}$$

where $C_{DEF\_DP\_P}$ is the defender cost at the data plane under proactive approach.

IPS_{LW} indicates the IP shuffling cost associated at load balancer. $PortS_{WS}$ presents the port shuffling cost of webservers. $DNS_{LBIPupdate}$indicates DNS update cost due to IP shuffling at load balancer C_{ST} presents logs storage cost and C_{REC_DP} indicates cost of Reconnaissance Detection module at the data plane.

VIII. CONCLUSION

This paper proposed SDN based MTD solution SMCDS, for protecting data and control planes of SDN. SMCDS enhances the control plane security by exploiting the distributed shadow controllers for countering the probing attacks along with providing the high availability and resilience of the control plane. The data plane security is improved by proposing proactive and reactive techniques. The proactive method utilized Port shuffling at the Web Servers and IP Shuffling at load balancer for creating the MTD effect. At the data plane, the reactive approach utilized the decoy servers for responding to the probing traffic which is directed towards original servers. Another significant aspect of SMCDS is digital forensic capabilities which analyze the attacker's footprints. For performing the analysis, SMCDS was assessed by means of success and cost pertaining to attacker and defender along with complexities that are introduced in the system. Additionally, SMCDS showed low computational overhead.

In the future, the effectiveness of SMCDS will be investigated against the crossfire DDoS attacks. Furthermore, this work will be extended by incorporating other IP packet attributes for designing an efficient crossfire DDoS protection technique. Also, SMCDS will be enhanced to cater to moving attackers.

REFERENCES

[1] A. Aydeger, N. Saputro, and K. Akkaya, "A moving target defense and network forensics framework for ISP networks using SDN and NFV," *Future Gener. Comput. Syst.*, vol. 94, pp. 496–509, May 2019.

[2] F. Chong, R. Lee, A. Acquisti, W. Horne, C. Palmer, A. Ghosh, D. Pendarakis, W. Sanders, E. Fleischman, H. Teufel, and G. Tsudik, "National cyber leap year summit 2009: Co-chairs' report," NITRD Program, Arlington, VA, USA, Tech. Rep., 2009. [Online]. Available: https://www.nitrd.gov/nitrdgroups/images/b/b8/Moving_Target_Summit_Ideas_Draft_090824_v3.pdf

[3] B. G. Assefa and Ö. Özkasap, "A survey of energy efficiency in SDN: Software-based methods and optimization models," *J. Netw. Comput. Appl.*, vol. 137, pp. 127–143, Jul. 2019.

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.

[5] R. Sahay, W. Meng, and C. D. Jensen, "The application of software defined networking on securing computer networks: A survey," *J. Netw. Comput. Appl.*, vol. 131, pp. 89–108, Apr. 2019.

[6] A. Abdou, P. C. van Oorschot, and T. Wan, "Comparative analysis of control plane security of SDN and conventional networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3542–3559, 4th Quart., 2018.

[7] N. Z. Bawany and J. A. Shamsi, "SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks," *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, Art. no. 102381.

[8] K. Thimmaraju, B. Shastry, T. Fiebig, F. Hetzelt, J.-P. Seifert, A. Feldmann, and S. Schmid, "Taking control of SDN-based cloud systems via the data plane," in *Proc. Symp. SDN Res.*, Mar. 2018, p. 1.

[9] V. Varadharajan and U. Tupakula, "Counteracting attacks from malicious end hosts in software defined networks," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 160–174, Mar. 2020.

[10] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 127–132.

[11] S.-Y. Chang, Y. Park, and B. B. Ashok Babu, "Fast IP hopping randomization to secure hop-by-hop access in SDN," *IEEE Trans. Netw. Service Manage.*, vol. 16, no. 1, pp. 308–320, Mar. 2019.

[12] M. F. Hyder and M. Ali, "Distributed shadow controllers based moving target defense framework for control plane security," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, p. 79, 2019.

[13] H.-Q. Zhang, C. Lei, D.-X. Chang, and Y.-J. Yang, "Network moving target defense technique based on collaborative mutation," *Comput. Secur.*, vol. 70, pp. 51–71, Sep. 2017.

[14] Y. Shi, H. Zhang, J. Wang, F. Xiao, J. Huang, D. Zha, H. Hu, F. Yan, and B. Zhao, "CHAOS: An SDN-based moving target defense system," *Secur. Commun. Netw.*, vol. 2017, pp. 1–11, Oct. 2017.

[15] Z. Zhao, F. Liu, and D. Gong, "An SDN-based fingerprint hopping method to prevent fingerprinting attacks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–12, Feb. 2017.

[16] D. P. Sharma, D. S. Kim, S. Yoon, H. Lim, J.-H. Cho, and T. J. Moore, "FRVM: Flexible random virtual IP multiplexing in software-defined networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 579–587.

[17] S. Achleitner, T. F. L. Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, "Deceiving network reconnaissance using SDN-based virtual topologies," *IEEE Trans. Netw. Service Manage.*, vol. 14, no. 4, pp. 1098–1112, Dec. 2017.

[18] A. Chowdhary, A. Alshamrani, D. Huang, and H. Liang, "MTD analysis and evaluation framework in software defined network (MASON)," in *Proc. ACM Int. Workshop Secur. Softw. Defined Netw. Netw. Function Virtualization*, Mar. 2018, pp. 43–48.

[19] S. Saraswat, V. Agarwal, H. P. Gupta, R. Mishra, A. Gupta, and T. Dutta, "Challenges and solutions in software defined networking: A survey," *J. Netw. Comput. Appl.*, vol. 141, pp. 23–58, Sep. 2019.
[20] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN control: Survey, taxonomy, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 333–354, 1st Quart., 2018.
[21] H. Wang, L. Xu, and G. Gu, "FloodGuard: A DoS attack prevention extension in software-defined networks," in *Proc. 45th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, Jun. 2015, pp. 239–250.
[22] R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "ArOMA: An SDN based autonomic DDoS mitigation framework," *Comput. Secur.*, vol. 70, pp. 482–499, Sep. 2017.
[23] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: Rapid prototyping for software-defined networks," in *Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw. (Hotnets)*, 2010, p. 19.
[24] A. Akhunzada, A. Gani, N. B. Anuar, A. Abdelaziz, M. K. Khan, A. Hayat, and S. U. Khan, "Secure and dependable software defined networks," *J. Netw. Comput. Appl.*, vol. 61, pp. 199–221, Feb. 2016.
[25] Y. Wang, T. Hu, G. Tang, J. Xie, and J. Lu, "SGS: Safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking," *IEEE Access*, vol. 7, pp. 34699–34710, 2019.
[26] J. Hou, M. Zhang, Z. Zhang, W. Shi, B. Qin, and B. Liang, "On the fine-grained fingerprinting threat to software-defined networks," *Future Gener. Comput. Syst.*, vol. 107, pp. 485–497, Jun. 2020.
[27] S. Lee, J. Kim, S. Woo, C. Yoon, S. Scott-Hayward, V. Yegneswaran, P. Porras, and S. Shin, "A comprehensive security assessment framework for software-defined networks," *Comput. Secur.*, vol. 91, Apr. 2020, Art. no. 101720.
[28] J. Xu, L. Wang, and Z. Xu, "An enhanced saturation attack and its mitigation mechanism in software-defined networking," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107092.
[29] B. Pfaff, J. Pettit, T. Koponen, E. Jackson, A. Zhou, J. Rajahalme, J. Gross, A. Wang, J. Stringer, P. Shelar, and K. Amidon, "The design and implementation of open vswitch," in *Proc. 12th USENIX Symp. Netw. Syst. Design Implement.*, 2015, pp. 117–130.
[30] Q. Li, X. Zou, Q. Huang, J. Zheng, and P. P. C. Lee, "Dynamic packet forwarding verification in SDN," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 6, pp. 915–929, Nov. 2019.
[31] G. Shang, P. Zhe, X. Bin, H. Aiqun, and R. Kui, "FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun.*, May 2017, pp. 1–9.
[32] T. OConnor, W. Enck, W. M. Petullo, and A. Verma, "PivotWall: SDN-based information flow control," in *Proc. Symp. SDN Res.*, Mar. 2018, p. 3.
[33] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, and G. Parulkar, "ONOS: Towards an open, distributed SDN OS," in *Proc. 3rd Workshop Hot Topics Softw. Defined Netw.*, 2014, pp. 1–6.
[34] G. F. Lyon. (Oct. 26, 2020). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. [Online]. Available: https://dl.acm.org/doi/book/10.5555/1538595
[35] W. Reese, "Nginx: The high-performance Web server and reverse proxy," *Linux J.*, vol. 2008, p. 2, Sep. 2008.
[36] M. Roesch, "Snort: Lightweight intrusion detection for networks," in *Proc. Lisa*, 1999, pp. 229–238.
[37] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proc. USENIX Annu. Tech. Conf.*, 2014, pp. 305–319.
[38] L. Martin. (Oct. 26, 2020). *Cyber Kill Chain*. [Online]. Available: http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
[39] 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 Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 709–745, 1st Quart., 2020.

MUHAMMAD FARAZ HYDER received the B.E. degree in computer and information systems from NED, in 2005, the M.Eng. degrees in telecommunications engineering and computer systems engineering from the NED University of Engineering and Technology, in 2010 and 2014, respectively, and the Ph.D. degree in cybersecurity from the Department of Computer and Information Systems Engineering, NED University, in 2020. He has 16 years of experience in industry, academics, and research centers. His areas of research include cyber security, moving target defense systems, cloud security, software defined networking, network function virtualization, network and information security, privacy, and digital forensics.

MUHAMMAD ALI ISMAIL (Member, IEEE) received the Ph.D. degree in high performance computing in 2011. He is currently a Professor and the Chair of the Department of Computer and Information Systems Engineering, NED University of Engineering and Technology, where he is also serving as the Director of the High Performance Computing Center and the Scientific Director of the Exascale Open Data Analytics Laboratory, National Center in Big Data and Cloud Computing. He has more than 16 years' experience of research, teaching, and administration in both national and international universities. Afterwards, he pursued his Ph.D. degree in automatic design space exploration from ULBS Romania and become a HiPEAC member. He has published more than 65 scientific articles in international journals and conferences along with U.S. patent. He has won many of the national and international grants of worth above Rs. 200 Million. His current research interests include computational HPC, big data mining, cluster and cloud computing, multicore processor architecture and programming, machine learning, heuristics, and automatic design space exploration. He is a member of IET. He was a recipient of the Research Productivity Award by Pakistan Council for Science and Technology-Ministry of Science and Technology, Government of Pakistan. He is also serving IET Karachi Network as its Vice Chairman.