Distributed Shadow Controllers based Moving Target Defense Framework for Control Plane Security

Muhammad Faraz Hyder[1]
Department of Software Engineering
NED University of Engineering & Technology
Karachi, Pakistan

Muhammad Ali Ismail[2]
Department of Computer and Information Systems
Engineering, NED University of Engineering & Technology
Karachi, Pakistan

***Abstract*—Moving Target Defense (MTD) has drawn substantial attention of research community in recent past for designing secure networks. MTD significantly reduced the asymmetric advantage of attackers by constantly changing the attack surface. In this paper Software Defined Networking (SDN) based MTD framework SMTSC (SDN based MTD framework using Shadow Controllers) has been proposed. Although the previous work in SDN based MTD targets the Data plane security, we exploit MTD for the protection of Control plane of SDN. The proposed solution uses the concept of Shadow Controllers for producing dynamism in order to provide security at the Control plane of SDN environment. We proposed the concepts of Shadow Controllers for throttling the reconnaissance attacks targeting Controllers. The advantage of our approach is multifold. First it exploits the mechanism of MTD for providing security in the Control plane. The other advantage is that the multi-controller approach provides higher availability in the SDN network. Another critical gain is the lower computational overhead of SMTSC. Mininet and ONOS Controller are used to implement the proposed framework. The effectiveness and overheads of the framework is evaluated in terms of attacker's effort, defender cost and complexity introduced in the network. Results demonstrated promising trends for the protection of Control plan of SDN environment.**

***Keywords*—Control plane security; moving target defense; shadow controllers; software defined networks**

I. Introduction

Cyber Security is a critical challenge of today's connected world. The emergence of technologies like Internet of Things (IoT), Web of Things (WoT), 5G have significantly increased the opportunities of Cyber-attacks. Cyber Security is a never-ending game between attacker and defender in which attackers always have the advantage. In current Cyber Security scenario, attackers have ample amount of time to analyze and launch attacks on the systems. The reason is that targeted systems and networks are static. Therefore, analyzing these systems from the perspective of vulnerabilities is much easier.

Moving Target defense (MTD) is an emerging area in cyber security. The motivation behind MTD is to make Cyber Systems dynamic and thus making them harder to discover, predict and attack. MTD removes the asymmetric advantages of attackers and make the cyber security field an equal playing ground. The term Moving Target Defense (MTD) was introduced for the first time in 2009 [1]. It is one of the game changing themes of cyber security defense. The main objective of MTD is to make the cyber security an equal playing field for both attackers and defenders. MTD eliminate the asymmetric advantage of adversaries by continuously changing the attack surface. Attack surface [2] of a system is basically a set of resources available in the systems that can be exploited by the attacker.

MTD ensures that attackers are not provided with slowly-changing /constant and predictable attack surface. MTD can be broadly classified as Network Based, Host based, Application based and Hybrid Approaches, etc. [3]. There are different parameters at each of these levels which can be changed in order to increase the difficulty level for attackers. Such attributes may include IP Address, Ports, OS versions, MAC Address, Routing paths etc.

SDN is a popularly growing networking paradigm. It fundamentally decouples the network control plane from forwarding data plane [4]. In recent past, there is a trend to design MTD solutions using Software Defined Networking (SDN) [5-8]. SDN substantially enhance the utilization of resources in the network, provides simplified network management, reeducation in operating cost and provides opportunities for network innovation and evaluation. SDN has a 3-layer architecture comprising of Application, Control and Data planes as shown in Fig. 1. Application Plane contains different application for numerous functionalities like network management, security and policy management etc. In the Control Plane SDN has SDN controller which is the brain of SDN network. In the Data Forwarding plane SDN has switches which forwards the packet based upon the directions from the Controller. The fundamental model behind SDN is OpenFlow [4]. It operates between the Control and Data planes. Its main role is defining the communication mechanism between the controller and switches in the data planes. The Controller has a clear unified view of the network. This global visibility of the Control plane enhances the network security. Control plane has the capability of network wide monitoring, vulnerabilities diagnostics and security policy deployment etc.

There has been a lot or research work in the domain of SDN security and MTD based SDN. Moreover, Distributed Controllers and Control planes security are also very active area of research. However, to the best of our knowledge there is no previous work which used the concept of MTD for the security of Control plane of SDN.

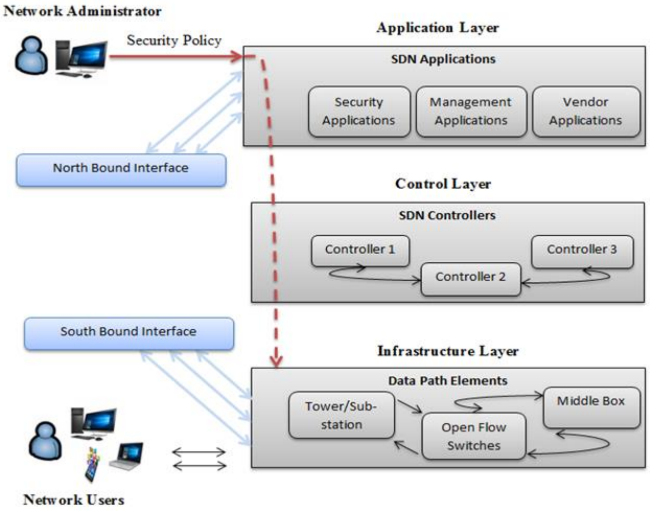

Fig. 1. Software Defined Networking Architecture.

The previous works for the protection mechanisms of control plane of SDN mainly focus on load balancing and mitigation of DDoS attacks [9-11]. Most of these solutions are reactive in nature, lacking a proactive approach like MTD. Moreover, these works do not take into consideration the first stage of Cyber kill chain which is reconnaissance. These solutions do not prevent the critical information collected by malicious attackers in the first stage of cyberattacks. The accurate information collected by the attackers is one of the main reasons of attackers' success. There is a need to design a solution which can prevent such attacks against the control plane of SDN at the first stage of cyber kill chain. This is one of the main motivations of this work. The proposed approach substantially protects against the reconnaissance attacks targeted towards the controller. The proposed approach will substantially enhance the DDoS protection of SDN control plane. The proposed MTD approach will make it difficult for the attackers to detect the actual controllers.

In this paper we proposed the idea of MTD for securing the Brain of SDN network i.e. Controller. The Brain of SDN has been the target of number of attacks. Its security is pivotal for the successful operations of SDN as it is the central controlling part of SDN. We used the concept of shadow Controllers for protecting against reconnaissance attacks which is the first stage of cyber-attack chain. The notion is to detect the reconnaissance traffic targeted against Controllers and provide manipulated response. Our proposed scheme has many advantages like increase difficulty level for the attacker to predict the correct Controller, higher availability and reliability due to the use of distributed Controllers and very low overhead for MTD implementation. Mininet emulator [12] and ONOS Controller [13] are used to implement the prototype of SMTSC.

Rest of the paper is outlined as follows: section 2 highlights the related work in the domain of SDN based MTD. Problem definition and threat model is presented in Section 3. The proposed SMTSC is explained in Section 4. Performance evaluation of SMTSC is presented in Section 5 whereas Section 6 covers the conclusion.

II. Related Work

One of the very first works in the domain of SDN based MTD was done in [5]. It provides the randomization of IP addresses in order to thwart the scanning attacks. It exploits OpenFlow to provide virtual IP address to different nodes in the network using a predefined frequency. Aydeger et al [6] proposed a MTD framework using SDN and Network Function Virtualization (NFV). The main motivation of their work is to exploit the benefits of both SDN and NFV for MTD design along with forensic capabilities. The framework utilizes three different MTD techniques to protect against the reconnaissance phase of cyber kill-chain [8].The framework was implemented in Mininet and considered indirect DDoS attacks as the threat model. An SDN based MTD was proposed in [7] securing the data plane. Their solution comprises of hopping of IP addresses. The solution protects against unauthorized access and reconnaissance attacks. The work substantially reduced the controller overhead by reducing its involvement in the MTD strategies. However, this may lead to some security problems and risks. An MTD using SDN with collaborative network mutation was proposed in [8]. It combines the idea of network and endpoint mutation for enhancing the security benefits. The collaborative model also utilized the hypothesis tests in order to adapt against the reconnaissance tactics of attackers. It also used the satisfiability modulo theories for generating optimal strategies. CHAOS which is an MTD system was proposed in [14]. It utilized the concept of CTS (Chaos Tower Structure). It divides the hosts based upon the security levels and then obfuscates the resources correspondingly. It used IDS to detect abnormal traffic patterns. The key strategy is to keep the legitimate traffic pass through the network normally while mystifying the abnormal traffic. An MTD utilizing SDN for protection against Fingerprinting attacks was proposed in [15]. The author proposed a method based upon hopping of Fingerprinting information (FPH). The main idea is to protect against fingerprinting attacks which are primarily used to gather the Operating System information. To devise an optimal strategy for proposed MTD, the FPH model fingerprinting attack and its defense as game. Authors in [16] developed SDN based MTD based on the concept of multiplexing of virtual IP addresses. The model was named as FRVM which is for multiplexing of virtual IPs in random fashion. There is a de-multiplexing module which provides the mapping of real IP address to virtual IPs. The proposed random mapping may suffer from performance degradation. A model to collect SDN Controller information was presented in [17]. The attack model proposed in this paper assumed that attacker is connected in Data plane of SDN. The model utilized simple TCP based measurement techniques to detect the Controller's platform. The authors in [18] proposed a mechanism to collect critical information of SDN based network without being detected. The attack KYE (Know your enemy) can collect critical information like network virtualization, threshold values against different probing attacks, QoS parameters and different security mechanisms implemented in a given SDN network. The authors also proposed a mechanism to protect against such attacks. SDN based virtual topologies for countering the Reconnaissance attacks was proposed in [19]. The work also proposed mechanism for the identification of malicious nodes generating scanning through statistical information. An MTD analysis framework was proposed in [20]. The work primarily focused on the developing a framework for the evaluation of SDN based MTD. A proactive security using MTD was proposed in [21] to secure the web servers running behind proxy servers in cloud environment. The work fundamentally focused on the botnets attacking the web servers. Proxy servers change at specific rate making a Moving target effect. A framework for the evaluation and optimization of container based cloud was proposed in [22]. The DSEOM framework provides mechanism for the analysis of MTD in dynamic cloud environment. It also provides optimization of different MTD techniques in the Cloud environment. Authors in [23] proposed the idea of MTD based protection for SDN enabled smart grids. These cyber physical have a high security requirements as security breach can cause substantial damage. Therefore, authors provide the idea of securing such systems with MTD based dynamic security techniques. The SFV which is security function virtualization was proposed in this paper. MTD based mechanism for privacy enhancement was proposed in [24]. The work targeted privacy leakage protection using MTD. For the experimental verification of the work, Domain Name system (DNS) was used. A Smart collaborative distribution provides protection against privacy leakage due to DNS queries using Moving Target Defense. A Cyber deception method based on MTD was proposed in [25] to counter the insider threats. Previous MTD work focused on the external attacks, while this is one of its kind works that exploited MTD for countering the insider threats. A Moving target defense approach was presented in [26] to counter adversarial machine learning approach of attackers. Stackelberg game based approach was used model the problem between attacker and defender.

III. Methodology

A. Threat Model

Our threat model assumes that attacker can run scanning to gather the information of Controller. Attackers in our work can be a host which is connected to target SDN network either directly or indirectly. Attackers target is to detect the SDN based System and then run different scanning attacks to gather information regarding Controller which is the brain of SDN network. In different previous work of SDN based MTD the attack model focused predominantly on the Data plane of SDN Network. However, our threat model assumes that attacker fundamentally targets the Controller of SDN. Modern attackers [18] can detect the presence of security mechanisms of SDN by observing the Controller and switch communication.

B. Proposed SMTSC Model

Fig. 2 presents the overall concept of SMTSC. In this framework there are “n” Controllers for building a distributed SDN network. All large SDN system uses the Distributed Controllers in order to run a reliable, highly available network. SMTSC also utilizes shadow Controllers. There are “k” shadow controllers. The reason for incorporating extra “k” controllers is to provide protection against the reconnaissance traffic generated by the attacker against Controllers. These “k” virtual controllers will generate responses against the reconnaissance traffic in order to constantly changing the attack surface and thus providing an MTD effect. There are other advantages of this approach as well. First one is fault tolerance. In case of failure in the “n” clusters, these shadow controllers may also provide backup support.

Fig. 3 represents the SMTSC internal components and the Data plane of SDN. According to our threat model discussed in the previous section, after successfully detecting the presence of an SDN based Network, the attacker will run the reconnaissance traffic against the Controller to capture critical information like Controller’s platform etc. The notion is to exploit vulnerabilities of Controller. The proposed SMTSC framework will come into play now. It will detect the reconnaissance traffic using its Reconnaissance Detection Module (RDM). RDM is implemented primarily using SNORT [27] which is an open source Intrusion Detection System. We have modified its configuration to detect the reconnaissance traffic directed against the Controllers. After the successful detection of Probing traffic, next task is performed by Movement Decision Module (MDM). Its fundamental role is the selection of strategy for movement. It will select one of the “k” shadow controllers to generate a response for the probing traffic. This selection is based upon the Round Robin fashion. There is another critical module which MTD Monitoring engine. Its responsibility is the overall monitoring of the proposed MTD framework. MDM also has capability to store the mapping of probing traffic and responses generated by respective k controller. It will be beneficial for the forensic analysis by tracking the footprints of attackers.

Algorithm 1 represents method of detection of interesting traffic. The required SDN network comprises of N distributed and K shadow Controllers is initialized. PacketArrival received the packets with their respective source and destination TCP/IP information. It checks for the interesting traffic directed towards controller. Once it detects the interesting scanning traffic, it will call the MTD Selection Algorithm. Algorithm 2 represents MTD Strategy and Shadow Controller Selection. This algorithm selects the shadow controllers from the list on Round Robin basis.

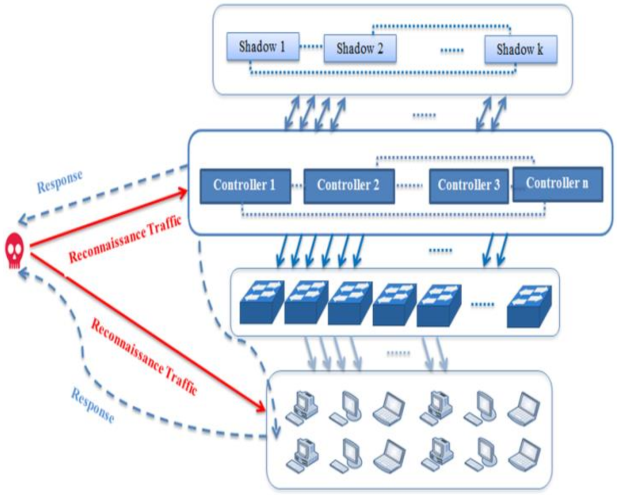

Fig. 2. SMTSC Block Diagram Indicating Distributed and Shadow Controllers.

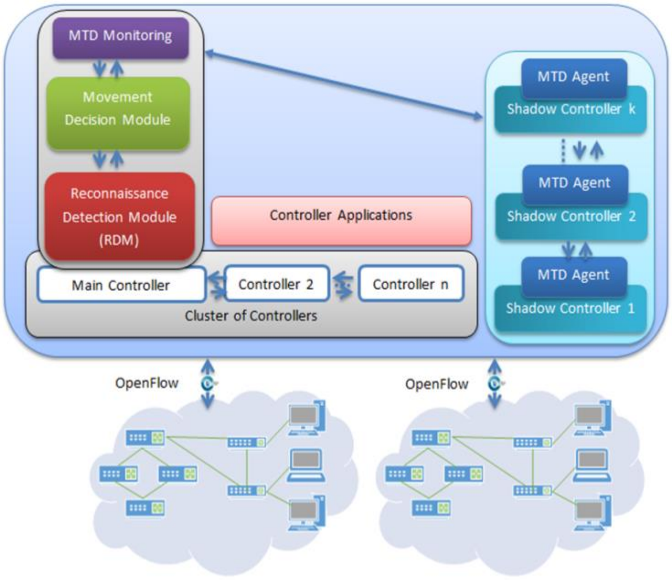

Fig. 3. SMTSC Internal Components.

Algorithm 1 Shadow Controller interesting traffic received

```
[Initialization of SDN based Network with Distributed and Shadow Controllers]
function PacketArrival (srcIP, srcPort, dstIP, Protocol)
    if (dstIP = = ControllerIP) AND (srcIP ! = switch_IP) AND (Protocol ! = LLDP) then
        SC ← ShadowControllerSelection ()
            Prepare_Response_probabing_traffic
                Set IP_SC =IP_Probed_Controller
                Set Ports_SC=Port_Probed_Controller
            Attacker ← SendResponse_to_probing_traffic
    endif
    else
    Normal_SDN_Forwarding ()
end function
```

Algorithm 2 Shadow Controller Selection

```
function ShadowControllerSelection
SelectedShadowcontroller = = RoundRobinSelection (list of K controllers)
Return SelectedShadowcontroller
end function
```

Fig. 4 represents the workflow of SMTSC. The MTD Application is constantly monitoring the reconnaissance traffic. As discussed in the previous sections, the network is running using Distributed SDN controllers. There are k shadow controllers as well in the system. The Data plane comprises of different switches and hosts connected to these switches. Both benign and malicious are present in the system. Traffic generated by legitimate users will pass through different switches and controllers as per the requirements. The Controller will install the required flows. However, the malicious users will generate the probing traffic directed towards the SDN controllers. The MTD application will detect this reconnaissance traffic. It will select one of the shadow controllers to respond to this traffic. The shadow controller will be selected based upon round robin fashion.

C. *Experimental Setup*

The experimental setup for the proposed framework comprises of Dell Server (Intel Xeon CPU E5-2620 2.1GHz) with 32 GB RAM. The platform for the distributed SDN Controller is ONOS [13]. The proposed network topology was implemented in Mininet simulator. The topology comprises of Distributed Controllers. All practical implementation of SDN requires Disturbed Control Plane for redundancy, higher availability and scalability. For the detection of reconnaissance traffic Snort was configured in an IDS (intrusion detection system) mode. We used Nmap [28] for running scanning traffic against the Controllers. Fig. 5 represents the implemented topology.

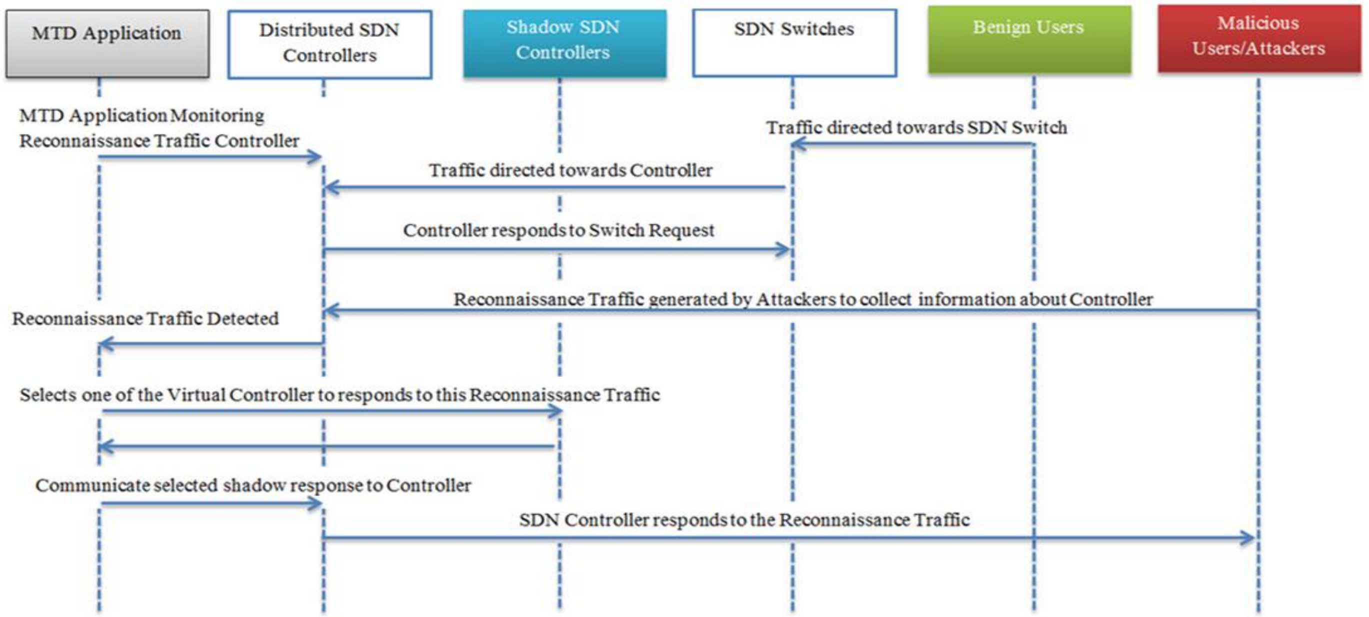
MTD Application
Distributed SDN Controllers
Shadow SDN Controllers
SDN Switches
Benign Users
Malicious Users/Attackers
MTD Application Monitoring Reconnaissance Traffic Controller
Traffic directed towards SDN Switch
Traffic directed towards Controller
Controller responds to Switch Request
Reconnaissance Traffic generated by Attackers to collect information about Controller
Reconnaissance Traffic Detected
Selects one of the Virtual Controller to responds to this Reconnaissance Traffic
Communicate selected shadow response to Controller
SDN Controller responds to the Reconnaissance Traffic

Fig. 4. Workflow of SMTSC.

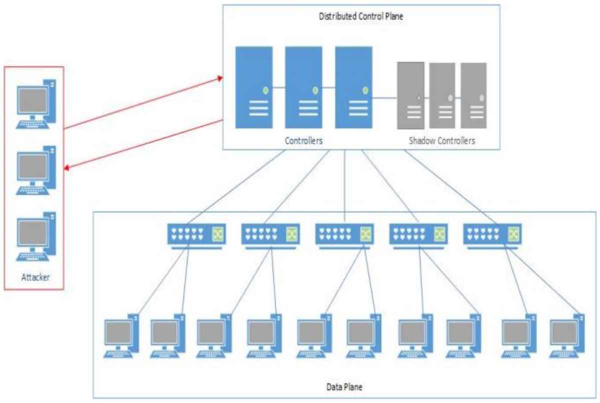

Fig. 5. Simulation Setup of SMTSC.

IV. Results and Discussion

Table I represents the time elapsed while the attacker is running Nmap scan against the Controllers for all possible ports. After several scans the following time ranges has been obtained with respect to number of controllers. As it is evident from the table that as the number of Controllers increased, the time required to scan will increase and hence the attacker's effort. Therefore, it is useful to have a Distributed Control plane for SDN in order to increase its security against reconnaissance attacks. Fig. 6 represents the box plot of Scanning time for different controllers.

A. Attacker Cost

The main objective of MTD is the increase in attacker's effort to attack a system. In this section, attacker's cost is analyzed. After incorporating the SMTSC, the snort configuredin IDS mode intercepts the reconnaissance traffic and redirect it one of the shadow Controllers as per Algorithms 1 and 2. The attacker will get response from one of those shadow controllers. Table II represents the attacker accurate detection with respect to total number of scans for different number of Shadow Controllers (SC). The accurate detection here means that attacker is able to correctly identify the Real Controller rather than getting response from one of the shadow Controllers. As evident from table, the attacker's success rate ranges from 15% to 20.55% after the adaptation of SMTSC.

For the purpose of experimental analysis, a maximum of 2000 scans were performed. Fig. 7 presents the graph of Attacker's success.

Attacker's cost is dependent on various factors like the accuracy of scanning traffic detection by IDS, the number of shadow controllers, and the number of scans by the attacker. Accurate detection by IDS is critical as it is the first step of our framework. The number of shadow Controllers plays important role. The higher number of Shadow Controller will increase the probability of successful response from these controllers and making it difficult for the attacker to identify the manipulated response. The number of scans performed by the attacker increases the probability of attacker's success. The reason is that the attacker scan may be able to get through the scanning detection mechanism without being detected. Hence, the increase in the number of shadow controllers decreases the attacker's success rate. However, increasing the number of shadow controllers beyond 6-7 doesn't substantially increase the attacker effort as evident from Fig. 7.

$$C_{attacker} = N_{scan} + N_{shadowcontroller} + A_{detection} \qquad (1)$$

TABLE. I. NMAP Scan Time with Single and Multiple Controllers

Scan time with 1 Controller (seconds)	Scan time with 2 Controllers (seconds)	Scan time with 3 Controllers (seconds)
1753-1882	2963-3062	3663-3721

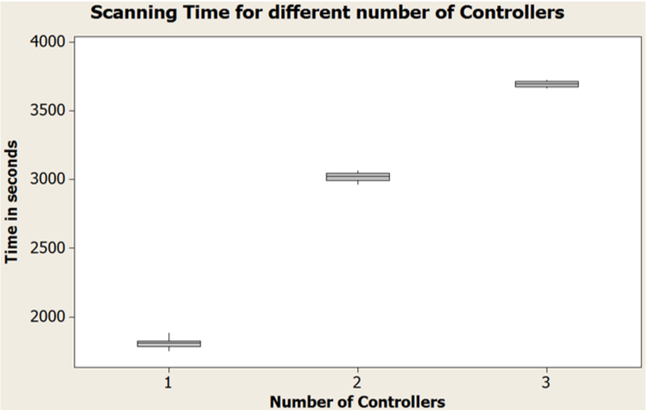

Fig. 6. Scanning Time for different Number of Controllers.

TABLE. II. Accurate Detection by Attacker after SMTSC for different Number of Shadow Controllers

Controllers	Number of Scans		Number of Shadow Controllers (SC)					
			SC=2	SC=3	SC=4	SC=5	SC=6	SC=7
3	100	Attacker Success (%)	18	17	16	16	15	15
3	200		18.5	17	16.5	16.5	15.50	15
3	400		19.25	17.75	17.25	16.75	16.50	16.25
3	800		19.62	18.50	17.75	17.62	17.37	17.12
3	1600		20.06	19.68	18.62	18.50	18.18	17.93
3	2000		20.55	19.65	19.15	18.85	18.2	18.05

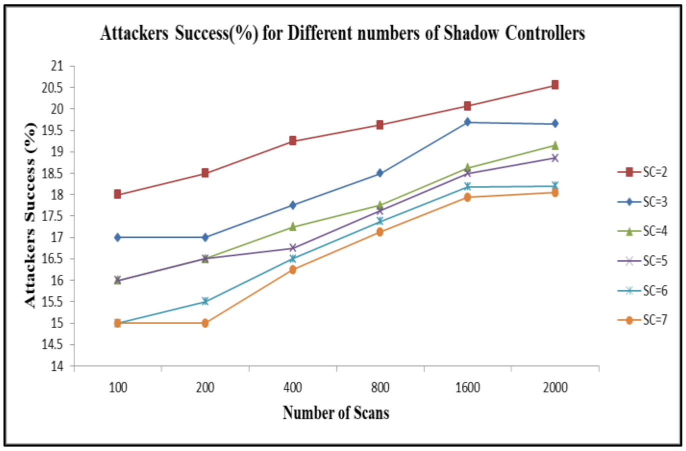

Fig. 7. Accurate Detection by Attacker.

Where $\boldsymbol{C_{attacker}}$ is the attacker cost, $\boldsymbol{N_{scan}}$ is the number of scans attacker perform, $\boldsymbol{N_{shadowcontroller}}$ is the number of shadow controllers and $\boldsymbol{A_{detection}}$ is the accuracy of scanning traffic detection.

B. Defender Cost

One of the main challenges of MTD is the overhead it introduced in the existing system. The proposed SMTSC model takes into consideration this problem. It utilizes the concept of Shadow Controllers which are running as different Virtual Machines. Moreover, it doesn't reset any IP address or Port address of running connections, therefore no such network overhead added in the original system. The SMTSC, stores the footprint of interesting traffic for the purpose of forensic analysis. For this purpose it requires minimal storage which won't incur substantial cost. For analysis purpose, a storage entry will require 17 bytes. It includes 2 bytes for ID field, 4 bytes for source IP address, entry date and time field comprises of 7 bytes and 4 bytes for Controller IP.

$$C_{storage} = Number\ of\ Scans \times Storage\ Required\ for\ one\ scan \tag{2}$$

The overall Defender's cost comprises of Number of Shadow Controllers present in the model and the computation power required by each controller. It also includes the storage cost required for storing the logs for analysis and reconnaissance detection mechanism cost.

$$\boldsymbol{C_{defender}} = \boldsymbol{k} \times \boldsymbol{C_{processing}} + \boldsymbol{C_{storage}} + \boldsymbol{C_{\mathrm{reconnaissancedetection}}} \tag{3}$$

Where, $\boldsymbol{k}$ is the count of shadow controllers, $\boldsymbol{C_{processing}}$ is the processing required by each shadow controller. $\boldsymbol{C_{storage}}$ is the storage cost and $\boldsymbol{C_{reconnaissancedetection}}$ is the cost of reconnaissance detection module.

For each shadow controller, we implemented a Virtual Machine (VM) with 2 CPUs, 2GB RAM, and 20GB hard disk. Therefore, $\boldsymbol{C_{processing}}$ is the computational cost of each VM. For SMTSC, the storage cost is $C_{storage} = 2000 \times 17 = 34Kbytes$. $\boldsymbol{C_{reconnaissancedetection}}$ is cost associated with reconnaissance detection module. Since all modern network protection scheme requires probing detection as the part of their IDS system. Therefore, this cost may be ignored for SMTSC as it will already be covered. Hence the main cost of SMTSC is cost of Shadow Controllers. Fig. 8 depicts the Defenders' success (%) for different number of scans.

The proposed framework was analyzed for maximum of 2000 scans. An attacker cannot perform very large number of scans as it will get permanently detected by the defender system. As evident from Fig. 8 and Table III, our framework can sustain realistic number of scans with a maximum accuracy of 85%.

C. Control Plane Security Analysis after SMTSC

In this section we analyzed the control plane security before and after the SMTSC. Attacker's success increases as the number of scans increased. Table IV presents Reconnaissance of SDN Network with and without SMTSC. Fig. 9 represents the attacker success on SDN Network with and without SMTSC.

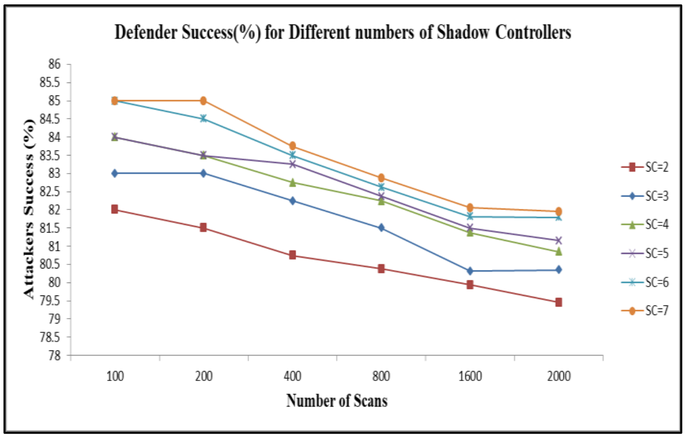

Fig. 8. Successful Response from Shadow Controllers.

TABLE. III. DEFENDER SUCCESS AGAINST NUMBER OF SCANS AND DIFFERENT NUMBER OF SHADOW CONTROLLERS

Controllers	Number of Scans		Number of Shadow Controllers(SC)					
			SC=2	SC=3	SC=4	SC=5	SC=6	SC=7
3	100	Defender Success (%)	82	83	84	84	85	85
3	200		81.5	83	83.50	83.5	84.5	85
3	400		80.75	82.25	82.75	83.25	83.5	83.75
3	800		80.37	81.50	82.25	82.37	82.62	82.87
3	1600		79.93	80.31	81.37	81.50	81.81	82.06
3	2000		79.45	80.35	80.85	81.15	81.8	81.95

TABLE. IV. RECONNAISSANCE OF SDN NETWORK WITH AND WITHOUT SMTSC

Controllers	Number of Scans	Attacker Success against Native SDN	Number of Shadow Controllers(SC)					
			SC=2	SC=3	SC=4	SC=5	SC=6	SC=7
3	100	97	18	17	16	16	15	15
3	200	195	37	34	33	33	31	30
3	400	391	77	71	69	67	66	65
3	800	788	157	148	142	141	139	137
3	1600	1569	321	315	298	296	291	287
3	2000	1962	411	393	383	377	364	361

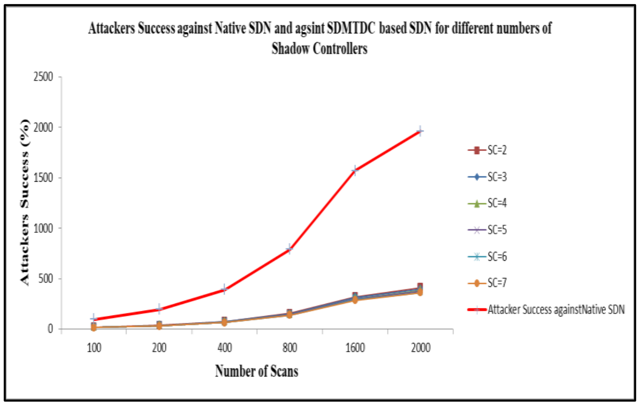

Fig. 9. Reconnaissance of SDN Network with and without SMTSC.

V. Conclusion

In this paper SDN based MTD SMTSC has been proposed. The SMTSC is distributed SDN Controller based system. It uses shadow Controllers to respond to the reconnaissance traffic directed towards the SDN Controllers. The notion is the protection of the brain of SDN. Another benefit of SMTSC is the distributed control plane for providing high availability and resilience for SDN network. The proposed model was analyzed against Reconnaissance attacks as well the overhead it introduces in the network. The results showed significant increase in the attackers' cost at minimum overhead in the system.

In future, we want to investigate in detail the impact of Multi-controller approach on users' privacy and protection against such privacy leakages. Moreover, another area that we will target is the crossfire attacks DDoS protection using this framework.

References

[1] F. Chong, R. Lee, A. Acquisti, W. Horne, C. Palmer, A. Ghosh, et al., "National Cyber Leap Year Summit 2009: Co-chairs' Report," NITRD Program, 2009.

[2] P. K. Manadhata, "Game theoretic approaches to attack surface shifting," in Moving Target Defense II, ed: Springer, 2013, pp. 1-13.

[3] J. Zheng and A. S. Namin, "A Survey on the Moving Target Defense Strategies: An Architectural Perspective," Journal of Computer Science and Technology, vol. 34, pp. 207-233, 2019.

[4] B. G. Assefa and Ö. Özkasap, "A survey of energy efficiency in SDN: Software-based methods and optimization models," Journal of Network and Computer Applications, 2019.

[5] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: transparent moving target defense using software defined networking," in Proceedings of the first workshop on Hot topics in software defined networks, 2012, pp. 127-132.

[6] Aydeger, N. Saputro, and K. Akkaya, "A moving target defense and network forensics framework for ISP networks using SDN and NFV," Future Generation Computer Systems, vol. 94, pp. 496-509, 2019.

[7] S.-Y. Chang, Y. Park, and B. B. A. Babu, "Fast IP Hopping Randomization to Secure Hop-by-Hop Access in SDN," IEEE Transactions on Network and Service Management, vol. 16, pp. 308-320, 2019.

[8] H.-q. Zhang, C. Lei, D.-x. Chang, and Y.-j. Yang, "Network moving target defense technique based on collaborative mutation," computers & security, vol. 70, pp. 51-71, 2017.

[9] A. Abdou, P. C. Van Oorschot, and T. Wan, "Comparative analysis of control plane security of sdn and conventional networks," IEEE Communications Surveys & Tutorials, vol. 20, pp. 3542-3559, 2018.

[10] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN control: Survey, taxonomy, and challenges," IEEE Communications Surveys & Tutorials, vol. 20, pp. 333-354, 2018.

[11] N. Z. Bawany and J. A. Shamsi, "SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks," Journal of Network and Computer Applications, vol. 145, p. 102381, 2019.

[12] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: rapid prototyping for software-defined networks," in Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, 2010, p. 19.

[13] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, et al., "ONOS: towards an open, distributed SDN OS," in Proceedings of the third workshop on Hot topics in software defined networking, 2014, pp. 1-6.

[14] Y. Shi, H. Zhang, J. Wang, F. Xiao, J. Huang, D. Zha, et al., "CHAOS: An SDN-Based Moving Target Defense System," Security and Communication Networks, vol. 2017, 2017.

[15] Z. Zhao, F. Liu, and D. Gong, "An SDN-based fingerprint hopping method to prevent fingerprinting attacks," Security and Communication Networks, vol. 2017, 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 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 579-587.

[17] A. Azzouni, O. Braham, T. M. T. Nguyen, G. Pujolle, and R. Boutaba, "Fingerprinting OpenFlow controllers: The first step to attack an SDN control plane," in 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1-6.

[18] M. Conti, F. De Gaspari, and L. V. Mancini, "A novel stealthy attack to gather SDN configuration-information," IEEE Transactions on Emerging Topics in Computing, 2018.

[19] S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," IEEE Transactions on Network and Service Management, vol. 14, pp. 1098-1112, 2017.

[20] A. Chowdhary, A. Alshamrani, D. Huang, and H. Liang, "MTD analysis and evaluation framework in software defined network (MASON)," in Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, 2018, pp. 43-48.

[21] D. Fleck, A. Stavrou, G. Kesidis, N. Nasiriani, Y. Shan, and T. Konstantopoulos, "Moving-target Defense against Botnet Reconnaissance and an Adversarial Coupon-Collection Model," in 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018, pp. 1-8.

[22] H. Jin, Z. Li, D. Zou, and B. Yuan, "DSEOM: A Framework for Dynamic Security Evaluation and Optimization of MTD in Container-based Cloud," IEEE Transactions on Dependable and Secure Computing, 2019.

[23] G. Lin, M. Dong, K. Ota, J. Li, W. Yang, and J. Wu, "Security Function Virtualization Based Moving Target Defense of SDN-Enabled Smart Grid," in ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, pp. 1-6.

[24] F. Song, Y.-T. Zhou, Y. Wang, T.-M. Zhao, I. You, and H.-K. Zhang, "Smart collaborative distribution for privacy enhancement in moving target defense," Information Sciences, vol. 479, pp. 593-606, 2019.

[25] K. Park, S. Woo, D. Moon, and H. Choi, "Secure cyber deception architecture and decoy injection to mitigate the insider threat," Symmetry, vol. 10, p. 14, 2018.

[26] A. Roy, A. Chhabra, C. A. Kamhoua, and P. Mohapatra, "A moving target defense against adversarial machine learning," in Proceedings of the 4th ACM/IEEE Symposium on Edge Computing, 2019, pp. 383-388.

[27] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Lisa, 1999, pp. 229-238.

[28] G. F. Lyon, Nmap network scanning: The official Nmap project guide to network discovery and security scanning: Insecure, 2009.