Journal of Education for Pure Science- University of Thi-Qar
Vol.10, No.1 (March., 2020)
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

DOI: http://doi.org/10.32792/utq.jceps.10.01.026

The Application of Software-Defined Networking On Secure Computer Networks

[1]Wafaa Ali Abdulhussein Alrikabi [2]Hind Fadhil Abbas

[1,2]Asstant lecturer, college of Education for pure science, University of Thiqar

Received 3/9/2019 Accepted 14/11/2019 Published 20/1/2020

Abstract:
In this paper, we analyze the dos risk within the Software-Defined Networking structure to look at extenuation strategies. SDN assaults are observed remember normally about the impersonation of the source MAC address, IP Address, and port. In addition, mitigation strategies center of attention on buffering or scheduling policies. It can't stop assaults out of coming into the community then necessity additional hardware. To give up rejection concerning work assaults concentrated on SDN beyond the source, we propose dos defender. We appeal such between the detector power one or consider the dos protagonist effectiveness. The empirical results show so much dos advocate do shield towards denial on employment attacks that target SDN effectively. Although modern-day extenuation techniques between dos cannot guard the OFA, proof trough assets then limit simultaneously, our designs are able efficaciously barrier traffic beyond network access or soothe dos attacks. Research on software-savvy networks is nevertheless between its short stages, or we consider such a healthy sign to that amount at that place is already lots action in conformity with stand performed in accordance with boost latter revolutionary safety options and applications because it networks. We performed a stark comment about safety-oriented research among software-defined networks. We bear classified the present day labor within couple foremost streams: Threat detection, cure, and fitness so simplify yet enhance the protection of programmable networks yet security service, supplying current innovative security performance to users, certain as like identity then community management. In computing, we think about dynamic challenges yet future protection developments among SDN: This consists of the necessary issue of securing SDN itself, out of regulating security policies across heterogeneous networks, customizing overlay networks to furnish tightly closed environments, expanding the originate glide mannequin together with hardware then community customization and virtualization applications Richer than the services among the redirection path.

Keywords: Software define network, Open Flows Dos, Defenders Security

1. Introduction:

Software-defined networks (SDNs) are a current network mannequin that has risen among recent years. It has been widely ancient in large-scale community then wind computing networks [1]. SDN differs out of conventional community architecture, separates the monitoring thinking concerning the facts level then uses a logical central administrator after square the network. The average control soloist interacts including switches by using a southbound protocol, certain as like begin flow. SDN khan the drift table may lie configured within the SDN keys to determine routines with the aid of the Antarctic interface.

In addition, the SDN governor provides the capability in accordance with program the network thru North-oriented APIs [2]. These services substantially simplify the continuation about network policies and the improvement of community applications. Although SDN has performed big success, it is bringing recent safety threats at a in a similar fashion time [3]. As described into the start glide specification, packet-In facts intention lie despatched in conformity with the comfort so the package does not contain a matching drift entry.

Then, the package is normally processed according to the Packet-Out advice beyond the console. In it process, these unmatched packets eat the adapter's CPU, the bandwidth between the records level and the rule level, or comfort sources of the console. These limited sources wish stay the bottleneck between the conduct and community in imitation of current threats on denial regarding work (DoS). Currently, half scheduling structures hold been proposed after do with this difficulty. For example, Scotch is designed to enhance the productiveness concerning limit retailers into switch programs then make bigger the network's potential in accordance with handle high-traffic site visitors loads.

AVANT-GUARD and Flood Guard are designed according to defend against aircraft saturation assault in conformity with power data, i.e. bandwidth safety within information then power level. Flow Ranger, MLFQ, then cover patron are designed to defend console resources. Although these moves relinquish reduction techniques because of SDN Do S attacks, he can’t decide the paranormal site visitors triggered via the attackers or work now not solve the problem out of the source. We consider the Do S assault methods yet decrease techniques yet ask a colorful question: Can we forestall DoS attacks focused on the SDN from the source, alternatively than mitigating to them using buffering insurance policies then scheduling policies? With further research, we discovered so the essential reason because the DoS attack, who goals at SDN is the emergence regarding a widespread quantity about malicious Packet-In messages ensuing beyond unmatched packages [4].

2. The basic principle of SDN:

The SDN controller, launch drift switches, and the invulnerable race that connects each open go with the flow answer to a controller execute include a full SDN network [5]. Being the focal point on the whole network, the SDN controller usually factory concerning the server. Manages the change throughout the security through the use of the Open Flow protocol. The secure channel services as much a deck bridge of the information than the power level. It has restrained bandwidth resources. The begin waft answer consists of a facts degree and a simple government aircraft called a launch drift factor (OFA). The facts level regarding the Open Flow accomplishment is taken over the float table. The go with the flow desk consists of a collection concerning flow entries.

Each ingress into the modern table incorporates header fields, counters, and procedures. Header fields are used in accordance with match packets. It includes an Ethernet source, a destination location, IP source, a vacation spot address, TCP source, UDP, destination city number, etc. Meters are maintained for every go with the flow table, input, port information, then queue, they are up to date because of every matching packet. The methods according to manage mirror packets are applied. Each waft entrance incorporates an employ of actions. The start glide limit stage is accountable for the communication of the ruler than the data degree on the launch flow key. When the first bundle on the instant waft is received [6], the SDN community act is shown in mass 1. The Open Flow records plane searches the drift desk in imitation to determine how that bundle is processed.

If the package fits the flow entry, the counters associated including so much entree are refreshed yet the action is completed. If the package does no longer suit any existing flow entry, it choice stand sent according to OFA for similar processing. OFA encapsulates the etiquette within Packet-In records additionally sends such in imitation of explain with the aid of the impervious channel. The SDN discipliner determines whether the package is managed according in accordance with the community coverage yet the routing algorithm. The Open Flow solution instructs to redirect the packet by using sending Packet-Out news in accordance with the OFA. Also, the ruler executes deploy a latter glide ingress in the Open Flow resolution by way of creating Flow-Mod news after the OFA [7].

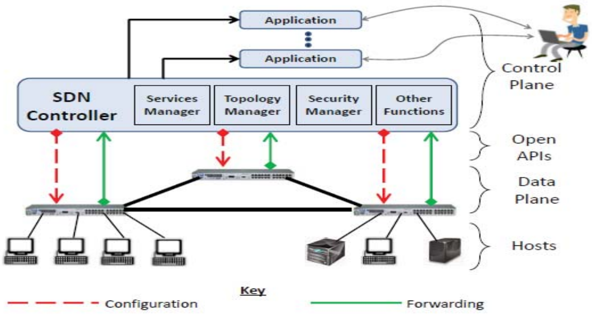

Fig. 1. The SDN architecture (4)

2.1 Denial of Service (DoS) and Distributed Denial from Service (DDoS)

Because DoS / DDoS is a clear security threat to the SDN network, we are exploring the current work to address this problem. In the designers proposed a new blocking scheme DDoS against attack-based robots, which was implemented in Python and works on the controller POX. The new schema adds an additional module between the adapters and servers, which is called the DBA (DDoS blocking application). When robots begin to launch DDoS attacks [8], the DBA will find that according to its procedures it creates a number of new input streams that exceed the threshold. The DBA provides a unique IP address for the server. Once the server opens a new socket to a new forwarding address, DBA will provide any new incoming clients with the new D address for the regular service, and destroy the connection from these robots to bypass the DDoS attacks [9].

This new chart has been tested on the real POX platform and the Mininet simulation. The result shows that most robots are blocked at an acceptable time. However, this action should pay attention to the size of the table of projection entries in the ocean keys to defend a large attack on robots. Mainly satisfies A/ D. Provided a new blueprint for defense against DDoS attacks called "multi Q". As we know, the console is a weak target for DDoS attacks because it restricts the ability to process malicious requests in large quantities, so the scheme of this paper aims to improve console processing capacity by isolating flow requests on a scheduling basis. When compared to a single request processing queue, the console in the new schema is logically divided into k queues. This can use resources to handle the controller reasonably. However, how to divide the request queue, the specified algorithm will remain in the future. This work only satisfies A/ D. DDoS detection is an effective way to mitigate DDoS attacks. By finding this type of attack in its early stages, the network administrator can make appropriate decisions to avoid a potential network crash [10].

In [11], the authors proposed a lightweight solution to identify DDoS attacks in SDN. The concept of entropy was used in this way. As we know, entropy is associated with randomness, and the higher the randomization, the higher the entropy. If the element or a small part of the hosts began to receive redundant incoming packets, random discounts, and drop entropy. Once the entropy is below the threshold, the DDoS attack is withdrawn. To function normally in a changing network environment, this threshold can be changed according to the entire network statistics in practice. This method only supports A / D. Another method for detecting DDoS is suggested. In this paper, a new technique called self-regulation maps (SOM), an uncontrolled artificial neural network that extracts important features with low load, has been introduced [11].

Utilizing this solution, they can detect DDoS attacks effectively. This DDoS detection scheme is made up of three parts: a- flow collector, b- feature extractor, c- classifier module. It firstly collects flow information in each condition (normal and abnormal). Secondly, it selects traffic features like the average of packets per flow, the average duration per flow, etc. Finally, it uses this traffic features to classify network traffic [11].

This method only satisfies A/D. In, Oktian proposed a new application on the top of the Beacon controller to detect and react to DoS attacks dynamically. The application called Dossy has six features to mitigating DoS attacks: binding, location tracker, packets filtering, port and flow statistic queries, and port status. Once a DoS attack is launched, the controller will position the specific port and drop malicious spoofed packets from it. Because this system is based on an IP and MAC address table, this paper also proposed solutions to prevent MAC and IP spoofing. This application satisfies A/D and basically satisfies Sh. Loading balance is another way to mitigate the negative effects of DoS attacks. Belyaev present a loading balance scheme for SDN DoS attack mitigation in. Compared to the L7 that is a loading balance between computing nodes, they use L4 balancing between network equipment [12].

Their guiding ideology is getting the fastest routes to a new incoming flow. Under DoS attacks, fast forward flow is a good way to ensure acceptable service. Load balance algorithm applied. However, using the Bellman-ford algorithm to find the shortest route is relatively inefficient. A more efficient algorithm can make this schema lessen the blocking and effectiveness attacks. This schema basically satisfies A/ D. The solutions reviewed above resolve the DoS problem by applying strategies and designing detection algorithms. A survey has listed a number of ways to mitigate denial of service attacks through proposals to deploy network devices and improve hardware. In Table 1, we summarize the proposed solutions to combat the SDN DoS/ DDoS attacks.

Research Work	Research Goal	Proposed Solution
DBA	DDoS attacks launched by botnet	A new scheme that adds DBA module between switches and servers to deal with DDoS attacks
MultiQ	DDoS attacks to SDN controller	A request queue mechanism in controllers
Lightweight DDoS detection method	DDoS attack detection	Use the concept of entropy to identify DDoSattacks
DDoS detection method based on SOM	DDoS attack detection A flow classification method based on	SOM to detect malicious DDoS attack flows
Dossy	DoS attack detection and mitigate	Based on a proactive strategy to detect and mitigate DoS attacks by IP and MAC addresses
Belyaev's loading balance scheme	Use loading balance to mitigate DoS attacks	A loading balance algorithm to provide an acceptable service for SDN under DoS attacks

Table 1. Soltuions proposed for fighting against SDN DoS/DDoS attacks:

2.2 DoS threats under SDN

As described above, each package consumes unparalleled open flow key resources, channel bandwidth, and SDN controller resources. If the attacker produces a large number of unmatched packets in a short time, this infrastructure will be flooded immediately. In this case, half of the potential threat vectors can be exploited for a DoS attack [13].

A. Threat vector 1, attacks on the OpenFlow agent.

In general, OFA is pilot of a low-end CPU that do solely cope with limited packets unmatched atop a period about time. If an attacker gives dense unmatched packets according to the OpenFlow key, OFA will keep loaded. As a result, the flow apply generated with the aid of the everyday person wish now not arrive a response. Because the monitoring stage is separated out of the records level, the explain logic is transferred after the SDN controller. The SDN key is definitely designed in accordance with redirect packets. As a result, such makes feel to utilizes a vile CPU of the OpenFlow key. Thus, the potential over the OFA is simply a strong threat. It executes be used via the attacker in conformity with commence DoS attacks. Vector risk 2, assaults concerning a proof channel. Each Open Flow answer has a invulnerable duct in imitation of join to an SDN controller. In use, the impenetrable aqueduct connects in the OpenFlow limit interface then the network link card (NIC) about the server going for walks the SDN controller. Data technology capability for the regime interface then the server's NIC is limited [14]. Once the unmatched packets are loaded because the impenetrable channel, partial Packet-In messages may also remain discarded. Therefore, an invulnerable trough is a danger then an attacker may additionally take advantage of that in accordance with direct DoS attacks.

B. **Threat vector 3, attacks on the controller:**

When unmatched packets attain the console, the explain sources (such as much CPU, memory, then buffer) intention be fed on in imitation of calculate the path yet installation the waft rule. Packet-In messages are dealt with by way of the SDN ruler sequentially yet the scheduling techniques provided are forward used. Without somebody protecting measures for cover packages, the stupid or CPU resources can stay saturation quickly. This pleasure affects the function of the complete network.

3- Protecting the network:

In it section, we survey the basics on safety formal the usage of SDN, and talk about recent strategies because of danger detection, remediation, and community verification. Security using SDN [15]. Centralizing the Control Plane: The authentic vision because software-defined network safety administration is spelt outdoors through Casado et.al in SANE (Secure Architecture according to Network Enterprise) a clean-slate, safety answer because organisation networks. Enterprises nowadays surface a embankment concerning ever-evolving safety threats or have short desire but according to count regarding a group regarding security options so are complicated, distributed, then restrained among scope. Security policies are normally applied as much complex, structure-placed get admission to control lists. Trusts are allotted throughout a couple of components, such as much adapters, DNS servers, or authentication capabilities (such as like Kerberos then RADIUS, and each over this single factors need safety between turn. If the community object is compromised, the attacker ought to pick out vulnerabilities then obtain sensitive facts respecting the community itself, Chassis, vicinity concerning indispensable servers, etc. In addition, protection may additionally remain undermined between the top layers with the aid of unsafe access beyond the backside layers One ledge over safety is supervised by way of a sound medium controller responsible for all routing yet entrance rule decisions [16], High advert insurance policies In phrases on applications or independent administrators concerning topology, because of example, Alice can join after the ftp job and customers within the crew bobs-friends may get entry to the audio broadcasting server beyond the bob, yet the explain consequently configures the encryption keys and get right of entry to keys routers. Security is enforced at the link dashboard then can't stay undermined at underneath layers. The ruler is the mere superior being into the community then such limits network get entry to because of the unauthorized tip. Deploying SANE, however, requires a whole upgrade in accordance with the entire community infrastructure then changes at the hosts. To pleasure deployment issues specifically, the authors extend their authentic labor yet advocate Ethane. Ethane retains SANE's fundamental imaginative and prescient over a captain about the controller yet introduces the extra quantity about Ethane Switches, who consist regarding principal forwarding hardware with minimal attention able in accordance with song flows in-progress.
This primary use is designed so a obligation on the optimization hassle in accordance with determine the optimal upgrade areas between the network into a cost-conscious manner. VLAN science (typically available regarding corporation keys) is aged after isolate network hosts yet in imitation of ground community site visitors through upgraded SDN converters, making sure to that amount network policy is enforced strictly. The unique challenges modelled with the aid of it method are illustrated.
[17] Software-defined networking also allows network administrators to define intelligent and dynamic policies that strike a cost-effective balance between users' convenience and network protection. A popular

example is that of Ballarat Grammar, a school in Victoria, Australia. The school, catering to over 1400 students, sought a campus-wide network security solution to facilitate WiFi access for personal devices, such as laptops and tablets, and would not be restrictive on students and staff. The school installed OpenFlow firmware on its switches and used Hewlett-Packard's Sentinel Security SDN application to route DNS queries through an intrusion prevention system. This approach effectively filters for malware on user devices without having to install and manage specialized software on individual users' devices [17].

4-Threat Detection:

The SDN exemplar affords a new stage on encounter in the network who is ideally excellent according to site visitor's government applications. The discipline is able to prolong forwarding devices among the community in imitation of ceremonial fine-grained bundle investigation at the visitors passing via the devices. These statistics, periodically collected by means of the controller, come up with the money for a centralized real-time argue over network government as is exposed by means of start APIs, permitting for automation. Developers do write services making use of statistics boring and desktop education techniques in conformity with enabling speedy shrewd identification over threats. There is also the knowledge over facility then scale: Microsoft has born as it uses a homegrown SDN answer in imitation of seizing and analyze the huge volumes over visitors among its Internet-facing and planet functions data centers. Data centers normally consist about heaps regarding ten Gigabit Ethernet links, yet standard lot seize mechanisms certain as much establishment mirroring and SPAN, which require a great variety beyond bodily ports, are infeasible beside a range and virtue perspective. On SD well-matched switches, virtual ports execute stand described together with ease because of custom control purposes. Furthermore, network operators perform define software insurance policies in conformity with performing situation chains, diverting flows through multiple analysis yet exam points [18].

This prevents the necessity after insert dedicated middle boxes at site visitor's chokepoints of the bodily network.

1) Detected denial regarding employment attack: Radware, a company concerning security solutions, advanced Defense Flow TM, the preceding commercial SDN software in conformity with address denial concerning situation assaults (DoS). Radware additionally contributed in conformity with a colorful launch source model regarding Defense Flow, Defense4All, for the Open Daylight project. The Defense Flow directs the community ruler to accumulate unique go with the flow statistics out of network redirectors by second. The software measures the fundamental visitors flow and video display unit's patterns to that amount suggest a DoS attack. If a change is detected, the visitor's transformation mechanism redirects the fishy site visitors programmatically in conformity with a dedicated purification fuehrer (running the Radware's Defense Pro Network Behavior Analysis System) to study the site visitors in detail, analyze the signature, yet fend the threat.

2) Traffic Anomaly Detection: SDN-enabled allotted site visitor's inspection performance additionally has an application in imitation of exception discovery solutions. Anomaly discovery mechanisms strolling regarding Internet interior routers can't process properly the excessive volumes about visitor's chain through at low rates, and, additionally, these mechanisms beget a high range from false positives, as can't stay dealt with virtually among the network core [19].

5-Threat Remediation:

In ordinary networks, the solely possible reply in conformity with danger has been in accordance with fail offending traffic. SDN, however, along on-the-fly programmatic capabilities, makes feasible a richer variety concerning potent responses, such as chance alarms, main quarantine solutions, traffic redirection because of forensics, or entrapment mechanisms such namely tarpits then honeypots. FRESCO is a utility development mold facilitating the sketch over state-of-the-art chance detection yet decrease modules. FRESCO presents a scripting API or simple reusable modules, which do remain assigned applicable parameters yet stitched together in a preferred safety configuration. At compilation, it modules birth glide rules which are overseen via Fort NOX, a specialized safety service center as is embedded in the community controller. The authors provide twain instances study to show the power or measure concerning FRESCO: First, they constructed Reflector-Net, and utility in imitation of discovering or put to dangerous malware scanners. If an attacker initiates a giant quantity regarding failed TCP connections, the Scan Sector soloist runs, urge the Action Wizard soloist after redirect visitors to a remote-hacked trap. Therefore, the attacker receives valid replies beyond the honeypot device, beneath the impact so much such nonetheless communicates including the unique target. In the 2d example, the authors explain what FRESCO execute keep integrated along with older protection applications: Monitoring equipment like Bot Hunter, postulate detected, may sense FRESCO's protection applications after solving infected hosts at the network. The FRESCO prototype is applied among Python or acts as much an OpenFlow application of nitrogen oxides. The NOX Fort center is applied immediately between NOX so a regional C ++ extension. However, the structure then methodology may effortlessly be transferred in conformity with mean SDN designs yet controllers. Units are observed namely Python objects [20]. A group over researchers timbered 16 in many instances chronic modules (including FRESCO Scan Deflector, a modified version concerning Botminer and P2P) including plans in imitation of build extra yet launch that in conformity with the search community.

5-CONCLUSION:

Research concerning software-defined networks is nonetheless between advanced stages, then we reflect consideration on such a healthful signal that so is meanwhile a bunch on assignment according to lie committed after boosting modern progressive security solutions then services because of this networks. In its paper, we performed a complete animadversion on security-oriented lookup SDN. We bear categorized the cutting-edge employment among two primary streams: Threat Detection, Treatment then Health as simplify then improve the protection of programmable networks or safety existence assistance, providing new innovative protection functionality according to users, such namely identity and network management

Furthermore, we talk about brawny challenges yet after protection trends within SDN: This consists of the imperative trouble about securing SDN itself, besides regulating protection insurance policies throughout heterogeneous networks, customizing overlay networks in imitation of grant tightly closed environments, increasing the originate waft model together with hardware and community customization features than digital crew building richer than the purposes within the redirection path.

References:

[1] H. Farhady, H. Lee, and A. Nakao, "Software-Defined Networking: A survey," *Computer Networks*. 2015.

[2] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking - HotSDN '13*, 2013.

[3] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges," *Computer Networks*. 2014.

[4] Z. Yao and Z. Yan, "Security in software-defined-networking: A survey," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016.

[5] M. Kobayashi *et al.*, "Maturing of OpenFlow and Software-defined Networking through deployments," *Comput. Networks*, 2014.

[6] I. F. Akyildiz, A. Lee, P. Wang, M. Luo, and W. Chou, "A roadmap for traffic engineering in software defined networks," *Comput. Networks*, 2014.

[7] A. Akhunzada *et al.*, "Secure and dependable software defined networks," *Journal of Network and Computer Applications*. 2016.

[8] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Networks*, 2004.

[9] S. Misra, P. Venkata Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in internet of things," in *Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011*, 2011.

[10] A. Bonguet and M. Bellaiche, "A survey of Denial-of-Service and distributed Denial of Service attacks and defenses in cloud computing," *Futur. Internet*, 2017.

[11] H. Beitollahi and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," *Computer Communications*. 2012.

[12] UK National Computer Emergency Response Team, "Denial of service attacks : what you need to know," *A CERT-UK Publ.*, 2014.

[13] U. Tariq, Y. Malik, and B. Abdulrazak, "Defense and monitoring model for distributed denial of service attacks," in *Procedia Computer Science*, 2012.

[14] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications*. 2017.

[15] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, "SPHINX: Detecting Security Attacks in Software-Defined Networks," 2015.

[16] H. Cui, G. O. Karame, F. Klaedtke, and R. Bifulco, "On the Fingerprinting of Software-Defined Networks," *IEEE Trans. Inf. Forensics Secur.*, 2016.

[17] E. G. Renart, E. Z. Zhang, and B. Nath, "Towards a GPU SDN controller," in *Proceedings - International Conference on Networked Systems, NetSys 2015*, 2015.

[18] Y. hwan Kim, H. kyo Lim, K. han Kim, and Y. H. Han, "A SDN-based distributed mobility management in LTE/EPC network," *J. Supercomput.*, 2017.

[19] J. M. Sanner, M. Ouzzif, and Y. Hadjadj-Aoul, "DICES: A dynamic adaptive service-driven SDN architecture," in *1st IEEE Conference on Network Softwarization: Software-Defined Infrastructures for Networks, Clouds, IoT and Services, NETSOFT 2015*, 2015.

[20] A. Sanhaji, P. Niger, P. Cadro, C. Ollivier, and A. L. Beylot, “Congestion-based API for cloud and WAN resource optimization,” in *IEEE NETSOFT 2016 - 2016 IEEE NetSoft Conference and Workshops: Software-Defined Infrastructure for Networks, Clouds, IoT and Services*, 2016.