An Empirical Review of DDOS Attack Mitigation System on SDN Using Cloud Environment

S. Annie Christila
Dept. of Computer Science, Christ (Deemed to be University), Bengaluru, Karnataka, India.
E-mail: annie.s@res.christuniversity.in

Dr.R. Sivakumar
Dept. of Computer Science, Christ (Deemed to be University), Bengaluru, Karnataka, India.
E-mail: sivakumar.r@christuniversity.in

Received August 07, 2021; Accepted November 24, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19022

Abstract

The separation of the control plane and the network data plane from the network defined by the software is making it easier for network management. As a result, SDN can be used in a variety of network settings, including network hiring networks. However, the construction of the novel network raises new security issues. Dedicated Shared Denial (DDoS) is easy to distribute and hard to protect on standard networks; on SDN networks, it can bypass the central controllers and bring the entire network down. Cloud computing has emerged as a modern and exciting computer space over the past decade, providing an affordable and awesome computer space. SDN technology combined with cloud computing highlights the challenges of cloud communication and enhances cloud adaptability, configuration, intelligence, and extreme density. Sensitive features of SDN, such as global network coverage, software-based traffic analysis, integrated network management, etc., greatly enhance the acquisition of DDoS cloud capabilities and scalability capabilities. In this study, a major effort was made to compare the various solutions currently available for programs to reduce DDoS attacks in cloud environments using SDN and provided performance tests such as detection rate, recovery time and False positive Rate.

Keywords

Cloud Computing, Software-Defined Networking (SDN), Dedicated Shared Denial (DDoS).

Introduction

As cloud computing provides demanded, uncluttered, and transparent computer services, a growing number of businesses are using this data transformation by simultaneously

changing their data and applications, creating another Internet-based infrastructure, Software-Defined Networking (SDN). When cloud computing simplifies managing storage and computational information, SDN was introduced to overcome another time-consuming problem that hinders the emergence of today's Internet, namely, complex network management. SDN is proposed to be the future generation Internet framework, and organizations such as Google have already used it in their data centers. As a result, the dawn of a new era in which cloud computing and SDN work together to provide business IT services is imminent.

Traditional infrastructure has not met the requirements such as dynamic management, high connection speed cloud computing, accessibility, optimization and bandwidth. SDN, therefore, flexible, programmatic, and powerful technology, arises as an alternative to traditional networks. SDN architecture comprises of control aircraft, data and applications. Switches and routers are also some of the devices included in its data planes. The plane was designed and operated by a control aircraft. Control flight oversees the management of transfer devices found in the data plane. The controller, which plays its role as a network brain, is situated on this plane. In-flight data devices enable packet transfers in accordance with the rules of the controller. In-flight flight connects to devices located in the network infrastructure via the controller Hameed et al. [2018].

Open Flow protocols are often used on SDN networks to link switches to SDN administrators. Switches that use packet messaging to complain to the controller and request new flow rules for any data flow that is difficult to handle in OpenFlow [10]. As a result of DDoS attacks, switches can create large amounts of packet messages to the controller, which will overload CPU and memory, and cause the controller to fail manage packets based on the flow input found in the controller, minimizing DDoS attacks on SDN is very difficult. In normal flow, IP addresses are almost uniformly distributed, but the attacker can impersonate normal traffic to defeat controllers Kreutz et al. [2014].

The main contribution of this paper is to compare different DDoS attack detection and mitigation systems in the SDN-based cloud environment proposed by multiple authors. Section II studies the outline of DDoS attacks and attackers, Section III describes various methods of DDoS attack detection and mitigation systems. Section IV provides a comparison analysis followed by conclusion in Section V.

Cloud and SDN Defense against DDoS Attacks

Cloud and SDN environments can be affected in two ways. It can come from the inside out, it can be inside and out and it can be inside the same system. Outside Internal - Attacks can

point to the gateway of cloud internet or servers. When a VM becomes a victim it can affect other VMs that are present in the same body system. A VM within a cloud can point to another VM within the same cloud environment. Each attack situation is similar to a specific attacker with a specific location and goal. Attackers can be categorized internally, externally, by Malicious, Rational, Active or Passive Lonea et al. [2013].

1. Types

i. DDoS Attacks

a. Volumetric Attacks

The objective is flooded with heavy traffic in a volumetric-based attack, with the aim of exhausting its bandwidth. As a consequence, the bandwidth of the attacked target is clogged. Attacks of this size are calculated in bytes per second. Flooding attacks, such as the User Datagram Protocol (UDP) flood and the Internet Control Message Protocol (ICMP) flood, are examples of these types of attacks.

b. Protocol-based Attack

Through leveraging network protocols, attacks deplete the resources of computers. It makes the network stacks or the underlying operating system inaccessible by crashing them. These attacks are based on a mixture of traffic that can influence the application, rather than on the amount of traffic. Packets per second are used to calculate their magnitude. Some examples include the SYN flood, Ping of Death, and Smurf attacks.

c. Application Layer Attack

Using application layer protocols, attackers attempt to crash the application or the underlying server. Requests per second are used to gauge the severity of such assaults. Hypertext Transfer Protocol (HTTP) flooding and slow Loris are examples of such attacks. Application layer protocols are used in just 24% of DDoS attacks. In 2014, the largest DDoS attack to date was carried out by flooding DNS requests against a Hong Kong-based news channel. This assault lasted several months and had a maximum effect of 500 Gbps.

ii. Attackers

a. Insider vs. Outsider

Insider is a member of the network under attack: he is a logged-in user with privileged access to sensitive information. An insider attacker may potentially run arbitrary commands

on behalf of a legitimate Cloud user. Since the latter will be considered an intruder by the network, the insider will cause more harm than the outsider. Furthermore, he will have less tools from which to launch an offensive.

b. Malicious vs. Rational

Malicious attackers have a broad target of causing damage to the network or its users (employees or customers of the network). Whatever the cost or the repercussions, he can use any means to accomplish his target, and such attackers are normally more difficult to avoid or monitor because they lack logic. Fair attackers, on the other hand, can be more predictable about how they carry out attacks and which specific targets they hit. A rational attacker may be a competitor looking to establish a business threat or an organisation waging an ideological DoS or DDoS against a corporation or government.

c. Active vs. Passive

Active attackers initiate attacks by sending packets or signals consciously or unconsciously, whereas passive attackers may simply listen in. Victims may be unaware that their computer is being controlled by a master machine, forcing it to participate in the attack.

Cloud computing Defense against DDoS Attack

- Today, attackers can perform a variety of DDoS attacks including resource-focused and performance-oriented attacks from anywhere in the world. We need to take into account all the possibilities whether the attackers can stay in a private network, in a social network, or both. To date, we have found that cloud tracking files that affect DDoS security attacks Mso et al. [2019].
- Users do not control the network. It's the cloud providers control the network with accounting tools like portable servers. Which is different from the system model in traditional DDoS protection, in which application servers are protected within a secure network. The distribution of resources and the migration of portable equipment are new changes in the network's climate resources in the sinner's mind.
- In addition, the allocation of resources and processes for the migration of virtual machines is faster. DDoS attack protection should always be able to adapt to the dynamic changes of the network environment and still have a high level of recovery and fast response capabilities.
- The same network infrastructure is shared by all cloud users. This raises the need to break the network's reliability, which means it has not yet been considered for

traditional DDoS protection from attack. An entity must verify its DDoS detection / protection functions without touching or touching other cloud users.

DDoS Defense against SDN

A two-tier load balancing solution for SDN networks used to increase system survival time during DDoS attacks. Load balancing did not reduce DDoS attacks but they were able to increase the survival time by splitting the load. An expiration method has been used to eliminate the input of false flow tables by the attacker to close the communication channel of the switch control and clog the TCAM memory memory. The shut-off time is explicitly used for non-standard error-free flow or DDoS packets whose sole purpose is to override OF-switch power. SDN is valid in the context of DDoS protection and provides local processing for change. The switches directly control the rental of the relevant features through a systematic process, thereby reducing the computer load on the controller. Accurate results are then included in the entropy based algorithm for detecting attacks on the controller. This work in its current form is very basic without extensive testing Taghavi Zargar et al. [2013].

DDOS attack Detection and Mitigation System

Model 1: Using SVM to Detect DDoS Attack in Cloud Environment Using SDN Network (Li et al. [2018])

The novel's approach to environmental protection uses the SDN network. The first step is to collect data using key attributes such as IP source, local IP and port. The author also uses an entropy method to calculate the allocation of each item. Secondly, the author uses a nonlinear SVM algorithm to find out what is happening in DDoS. SDN is used to manage a network in a cloud environment, the controller being the victim. The author has proposed a method that uses a machine-readable framework. It collects traffic data from pack-in messages, and extracts a number of important features, based on the machine learning framework, such as srcIP (source IP address), srcPort (source port), desIP (destination IP address), desPort (end of hole) etc. Entropy is used to measure the distribution of these substances. The test also shows that SVM is a better framework for detecting DDoS attacks on the SDN network, having the model with general and unusual traffic data and having a comparison of it to other machine learning algorithms, DDoS attacks can occur in any hole of any button, so the purpose of getting DDoS is to detect attacks and get switches and ports.

If a random variable X has N different values and their probability is p1， p2…pn, then the entropy of X can be calculated by formula

$$H(X)=-\sum p_i * \log p_i \quad (1)$$

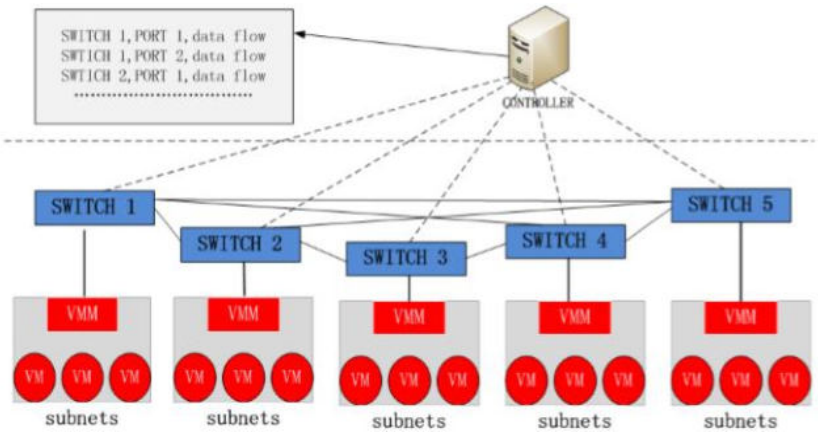

Figure 1 SVM based DDoS attack Model

Standard traffic should be activated as background traffic to simulate a real network environment. TCP syn flood is a popular DDoS attack that causes the receiver's resources to be depleted. The receiver will respond to the ICMP flood and will use the receiver's resources (CPU and Memory). SVM is a stronger framework for detecting DDoS attacks in SDN networks, according to the experiment.

Model 2: Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing (Bhusan et al. [2018])

SDN detection in the cloud environment by analyzing the suitability and risk of SDN introduced. Subsequently, an Information Distance based method is used to detect DDoS attacks in an SDN-based cloud environment. They also performed tests simulated and demonstrated the functionality of the proposed algorithm. Installing SDN in computer cloud computing can simplify cloud computing and improve management, control, power flexibility, and cloud computing. Global SDN network overview, network planning, and traffic-based traffic analysis are used effectively to detect and reduce DDoS attacks Global network information helps network administrators to develop appropriate network security policies. Having the right security policy always has the advantage of detecting and minimizing DDoS attacks.

Generalized information entropy of order α and is given as

$$H_\alpha(P) = 1/(1-\alpha)\log_2(\sum p_k{}^\alpha) \quad (2)$$

Information divergence is the measure of divergence between probability distributions P and Q.

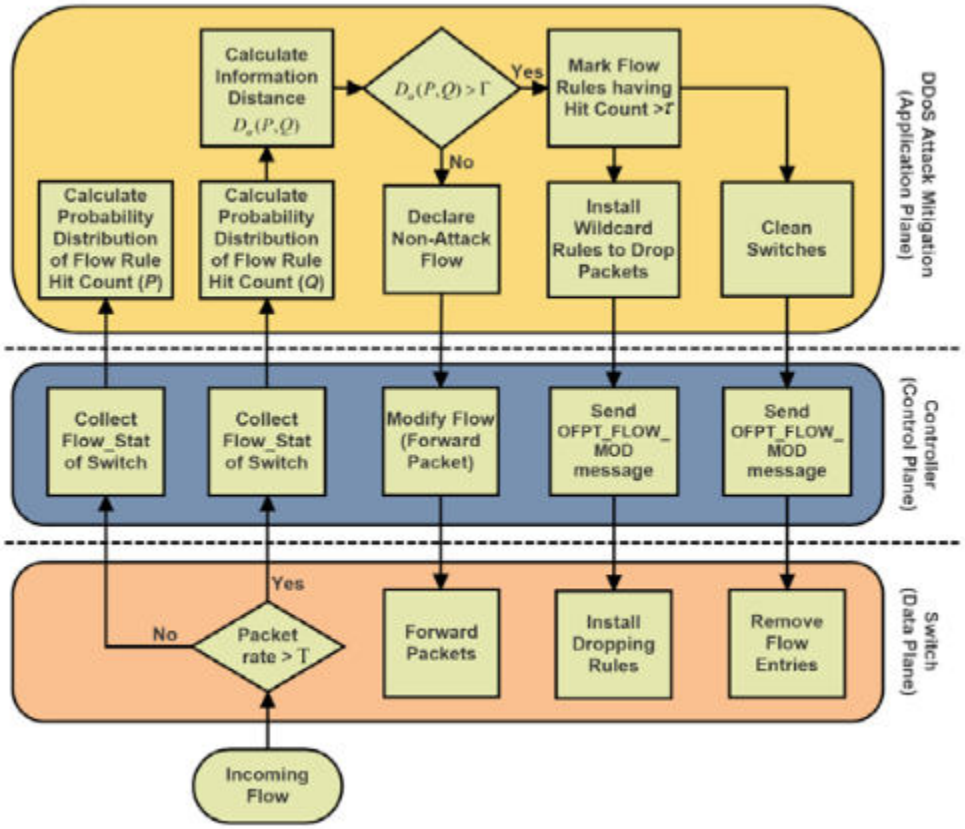

Figure 2.SDN based DDoS attack model

Mininet used to emulate the networks with POX as the controller platform. The performance of the proposed approach is evaluated by measuring information distance of suspicious traffic (both legitimate traffic and attack traffic) with the non attack traffic. The information distance is more than 3 always for attack traffic. When tested with legitimate traffic the information distance is always less than 1. Also, attack detection rate is measured as 90% time correctly.

Model 3: DDoS attack Protection in the era of Cloud Computing and Software Defined Networking (Wang et al. [2015])

The potential for protection against DDoS attacks in this new paradigm is discussed and proposed for the development of invasive DDoS mitigation systems and flexibility that use SDN technology which addresses new security challenges caused by cloud computing. SDN and cloud computing offer a unique opportunity to improve DDoS attack protection in the enterprise network. The proposed framework is being developed and performing

simulation tests using the Amazon EC2 cloud service. By the very fact that their system functions well under the new network system and includes computer restrictions and high connectivity are a clear sign that the system works well. It is a major requirement for DDoS protection in cloud computing and SDN.

Hybrid cloud shares include public and private clouds. The Hybrid cloud allows companies to keep their sensitive programs and data private while exposing others to the public. Analyzes the impact of cloud protection combined with DDoS attacks. The security provided by the cloud provider can monitor attack traffic. In spite of this protection, more advanced attacks, such as application layer attacks that target specific applications, may downplay the normal cloud protection provided. And a new building block to reduce DDoS attacks, called DaMask is being proposed with the help of changes from the cloud provider. The key functions of DaMask are to detect and respond to DDoS. In most cases the network traffic data is low in size and the number of cases is much higher than the features. Sometimes the type of package attack cannot be known by the recovery model unless the package is an old type of attack. Through further analysis the type of package can be determined.

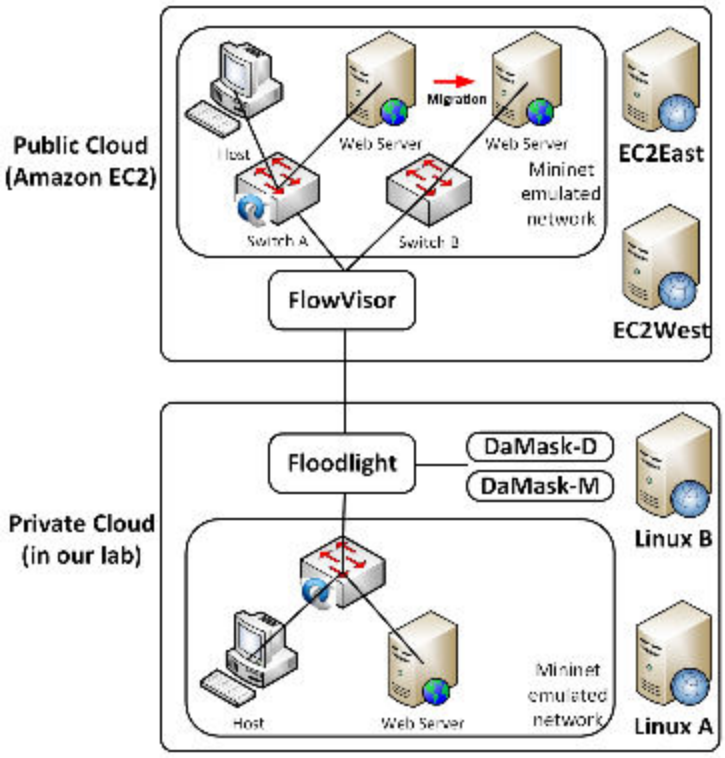

Figure 3 Cloud and SDN based DDoS attack model

The result of the analysis is then used to update the acquisition model through the model renewal process. Amazon Web Service EC2 is used as a standard cloud computing on their board. Normal test mode makes the network visible on a computer. The Floodlight controller and DaMask modules used in Linux B. modules. DaMask connects to the controller via Floodlight APIs. The results show that more than one connection is only related to the time travel between the server using FlowVisor in the public cloud and the server that controls network control in the private cloud. This is because the network controller receives the message size. Therefore, the connection header always remains when the network connection status is stable.

Model 4: Defending Cloud Computing Environment against the Challenge of DDoS Attacks based on Software Defined Network (Tsai et al. [2014])

Three modules are provided to detect and minimize the formation of SDNs with early detection clouds without affecting resources. Cruel packets are found prematurely. In the first module, Dynamic entropy detection with a separation algorithm is used. Entropy is calculated per window with a typical number of 10 windows compared to a small deviation to detect the most dangerous attacks. The decline in the value of entropy indicates an attack. This behavior is applied and creates a reduction process. Snor integration module is used to monitor network traffic. The third level of deep protection with a firewall based firewall that creates a firewall to protect attackers.

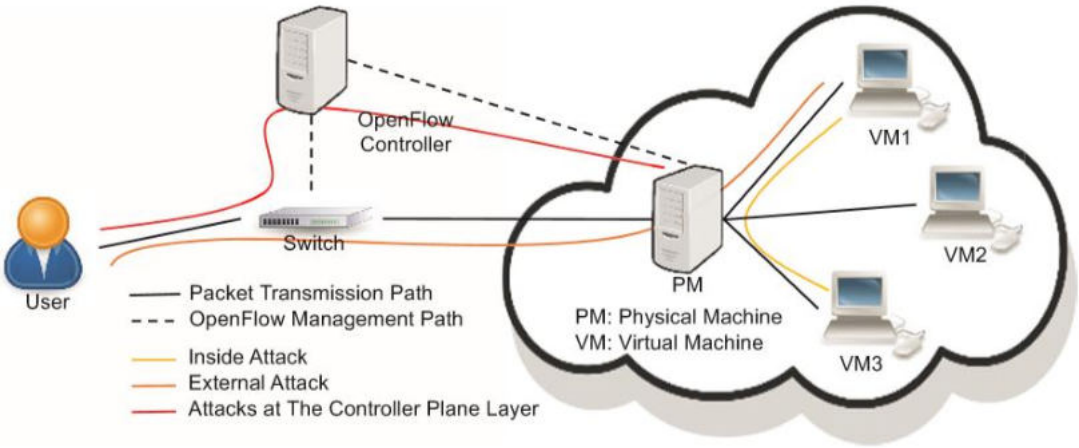

Figure 4 Dynamic entropy based attack model

Ryu controller is used as SDN to manage network devices, software based open vs witch (OVS) which handles the packets flexibly, Kernel based virtual machine (KVM) which acts as hypervisor and a Snort which is a network intruder detection system as a testbed. Scapy tool used to generate the traffic like a real world scenario.

Comparative Analysis

Table 1 Models used

S. No	Title	Models Used
1	Using SVM to Detect DDoS Attack in cloud environment using SDN Network	Entropy is used for detection Machine Learning algorithm is used for mitigation
2	Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing	Information entropy/ Information Divergence is used for detection Removing rule from flow entry and adding wild card rule is the mitigation
3	DDoS attack protection in the era of Cloud computing and Software Defined Networking	DaMask-D, a network attack detection system, and DaMask-M, an attack reaction module Attack detection system built on probabilistic inference graphical model (maximum posterior - MAP query).
4	Defending Cloud Computing Environment Against the Challenge of DDoS Attacks Based on Software Defined Network	Dynamic entropy detection with a classification algorithm / NIDS.

Table 2. Models Comparison

S. No	Title	Algorithms	Detection Rate	Detection Time	False Positive Rate
1	Using SVM to Detect DDoS Attack in cloud environment using SDN Network	Decision Tree	57%	6.6s	43%
		KNN	62%	1.8 s	38%
		Random Forest	74%	6.7 s	26%
		SVM	93%	3.4 s	7%
2	Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing	Information Divergence	90%	1.5 s	10%
3	DDoS attack protection in the era of Cloud computing and Software Defined Networking	Building new model based on new observation data	89.30%	1.8 s	10.70%
4	Defending Cloud Computing Environment Against the Challenge of DDoS Attacks Based on Software Defined Network	Mean deviation of entropy / NIDS	100%	-	-

In Model 1, three indicators: PR (Rate Precise Rate), RR (Recall rate) and F1 score are used to evaluate the proposal to reduce DDoS attacks. The level of accuracy is the ratio between the real deal and the total true and false benefits. The level of memory is defined as the ratio

between true goodness and the sum of real benefits and false errors. Other machine learning algorithms, decision tree, naïve bayes, KNN, random forest are used to analyze network traffic and detect DDoS attacks. It has been concluded that SVM is the best that can detect DDoS attacks in a short period of time with a high degree of accuracy.

In Model 2, a simple and easy-to-use DDoS system is proposed to use SDN. Using the proposed method, the distribution opportunities are calculated when the flow input resistance exceeds the limit value. The range of information is calculated by the newly distributed distribution opportunities and the calculated opportunities during normal traffic. Higher data range is an indication of DDoS attacks. The range of information is more than 3 times the number of attacks. When tested in official traffic the range of information is always less than 1. Attack rate is estimated and this method detects DDoS attacks 90% of the time correctly.

In Model 3, Discusses the impact of cloud computing and SDN on DDoS defense defense. SDN can help with protection against DDoS attacks. With a few changes needed in the current design of cloud computing, and SDN-based networks allow companies to successfully deploy cloud protection systems without affecting other cloud users, this model is effective in addressing the new challenges proposed.

In Model 4, an effective and easy-to-deliver DDoS delivery system uses SDN. Using the proposed method, entropy is calculated for all windows. A typical value of 10 windows compared to the mean deviation of the entropy values to obtain a more accurate attack. A sharp decrease / increase in the value of the entropy indicates an attack. In testing, the value of entropy dropped from 1.6 to 1.2 when the attacker was out. When tested by an internal attacker the value dropped from 1.6 to 0.4. Recovery occurs in a matter of seconds (250 packs in the case of external pockets and 150 pockets in the case of internal).

Conclusions and Future Research

Both Cloud computing and SDN are gaining increasing popularity and emerging as future business IT solutions. In this case the security of the business network becomes more critical. In this study we analyzed 4 different solutions proposed for the problem of DDoS attack detection and mitigation problems in cloud environments using SDN. Various DDoS attacks have been described. The authors have widely used the Entropy method and the range of information to detect attacks. We highlighted the authors of the algorithms used to detect DDoS attacks. The authors verified the methods using a virtual network, open flow switches and road generators. We conducted a comparative study of these solutions and

provided performance tests such as acquisition rate, recovery time and False positive Rate. We have systems in place to emphasize machine learning and in-depth learning of feature planning, preventing SDN cloud environments from DDoS attacks and the use of clever tactics will promote better false values and better use of resources.

References

Bhushan, K., & Gupta, B.B. (2018). Detecting DDoS attack using software defined network (SDN) in cloud computing environment. *In 5th international conference on signal processing and integrated networks (SPIN),* 872-877. http://doi.org/10.1109/SPIN.2018.8474062

Hameed, S., & Ahmed Khan, H. (2018). SDN based collaborative scheme for mitigation of DDoS attacks. *Future Internet, 10*(3). http://doi.org/10.3390/fi10030023

Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14-76. http://doi.org/103.10.1109/JPROC.2014.2371999

Li, D., Yu, C., Zhou, Q., & Yu, J. (2018). Using SVM to detect DDoS attack in SDN network. *In IOP Conference Series: Materials Science and Engineering, 466*(1). http://doi.org/10.1088/1757-899X/466/1/012003

Lonea, A.M., Popescu, D.E., & Tianfield, H. (2012). Detecting DDoS attacks in cloud computing environment. *International Journal of Computers Communications & Control, 8*(1), 70-78. http://doi.org/10.15837/ijccc.2013.1.170

Manso, P., Moura, J., & Serrão, C. (2019). SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. *Information, 10*(3). http://doi.org/10.10.3390/info10030106

Zargar, S.T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials, 15*(4), 2046-2069. http://doi.org/10.1109/SURV.2013.031413.00127

Tsai, S.C., Liu, I.H., Lu, C.T., Chang, C.H., & Li, J.S. (2017). Defending cloud computing environment against the challenge of DDoS attacks based on software defined network. *In Advances in Intelligent Information Hiding and Multimedia Signal Processing,* 285-292. http://doi.org/10.1007/978-3-319-50209-0_35

Wang, B., Zheng, Y., Lou, W., & Hou, Y.T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks, 81,* 308-319. http://doi.org/10.1016/j.comnet.2015.02.026