Australian Journal of Basic and Applied Sciences
2018 November; 12(11): pages 25-28
DOI: 10.22587/ajbas.2018.12.11.6
Original Article
Journal home page: www.ajbasweb.com
AENSI Publications

Distributed Denial of Service Attack Categories in Software-Defined Networks

[1]Ahmed K. Al-Shammari, [2]P Ehkan, [3]Naimah Yaakob, [4]Layth A. Al dulaimi

[1.4] Research Student, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.
[2.3] Senior lecture, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.

Correspondence Author: Ahmed K. Al-Shammari, Research Student, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.
E-mail: ahmedkareemhamzah@gmail.com

Received date: 12 August 2018, **Accepted date:** 15 November 2018, **Online date:** 27 November 2018

Abstract

The Distributed Denial of Service (DDoS) attack is from Important and main threats to Internet based killer applications, such as E-commerce, online games and social networking sites. The detection of these smart attacks has become very necessary and prevented from attacks. Software-defined networks (SDNs), which are considered to be a network of future communications, have emerged that separate network monitoring and redirection. Have some Special features such as central control and programmability to combat DDOS attack. In this paper, we scan DDoS Attacks, classification and knowledge of their mechanisms, in order to succeed in the development of mechanisms to defend the features of the network environment for the future and we conclude that it leads to counter attack DDoS. According to the analysis, we pave the way to build a defensive mechanism for DDoS in SDN.

Key words: Software-Defined Networks; Distributed Denial of Service attacks, SDN, DDoS attack

INTRODUCTION

As the digital community is developing and everything is nearly associated to each other and available from all over. The network got to be difficult and Troublesome to be manage and controlled. Software-Defined Network (SDN) guarantees to disentangle administration, control of the organize, and make it adaptable by advancing a centralization control and characterizing the capacity to program the network. Software-defined network is archetypically built up from a colossal number of network devices like switch, router and different types of middle boxes like a firewall worked beneath centralized controller with a lot of complex protocols utilized to execute them (Nunes, Marc Mendonca, Xuan-Nam, Katia Obraczka, & Thierry Turletti, 2014). The logical thought behind SDN is to segregate control plane of the network which makes choices about how the packet flow is redirected in the network from the data plane which is utilized to forward the packet and allow to program network utilizing outside apparatuses (Qiao Yan, F. Richard Yu, & Qingxiang Gong, 2016).

Denial of Service (DoS) attacks are the foremost undermining challenge to Internet security nowadays (Kshira Sagar Sahoo, Ranjan Kumar Behera, Bibhudatta Sahoo, & Mayank Tiwary, 2018) . The attacker DoS and Distributed Denial of Service (DDoS) depends on sending an overwhelming number of packets to the virtual exhaustion of victim resources, such as memory, CPU and network bandwidth. Subsequently, requests from users cannot be handled favorably because there are no system resources available. Faced with this type of attack, it proposed significant mitigation techniques (Somani, Manoj Singh Gaur; , Sanghi, Dheeraj;, Conti, Mauro;, & Buyya, Rajkumar, 2017) . Traditionally, DoS attackers target the server, which is giving a benefit to its consumers. Acting like legitimate customers, DOS attackers try to dump the active server in such a way that the service it becomes unavailable due to a large number of pending requests the waiting list is overflowing.

A diverse flavor of DoS is Distributed DoS, or DDoS, where attackers are a gather of machines targeting a specific service (Saman Taghavi Zargar, James Josh, & David Tipper, 2013). There is a great rise in the number of detailed occurrences of DDoS, making them one of the most important and deadly threat among many (SteveMansfield-Devine, 2015).

In this paper, we aim to provide a review of DoS and DDoS attacks in the SDN environment. We also distinguish these attacks with conventional DoS attacks and overview various contributions in this space and classify them. For this reason, we prepare a detailed classification of these works to provide assistance to understand this survey.

1.1 DDoS Defense

SDN separates the control plane from the data plane and the following allows the network operator to direct individual flows automatically via its interface to central programming (M. Jarschel, 2014) . This allows the implementation of the following comprehensive security policy to improve public network security.

Consequently, utilizing SDN, (S. K. Fayaz, 2015) proposed a DDoS defense framework named Bohatei. This system is scalable because the algorithm manages its own resources controlling the network to avoid bottlenecks in the control level and data level. In expansion, it exploits the network virtualization function (NFV) (Q. Duan, 2016) capability to flexibly develop virtual machine defense (VM) resources at sites that are in need of it. Add to that, based on SDN and NFV, a adaptable security arrangement was given for enterprise systems with more prominent adaptability and lower operational costs (C. Lorenz, 2017).

Taking advantage of the central programming capability and control of the SDN by the Internet network, (R. Sahay, 2015) proposed a self-management system, which provides service to the Internet (ISP) and its own customs cooperation companies to mitigate DDOS attack. The ISP collects risk data given by

Citation: Ahmed K. Al-Shammari, *et al.*, Distributed Denial of Service Attack Categories in Software-Defined Networks, Australian Journal of Basic and Applied Sciences. 12(11): 25-28. DOI: 10.22587/ajbas.2018.12.11.6

clients, at that point it configures the security policy and and update the flow tables in the network accordingly. If the customer handles the flow legitimately, the ISP alone will be marked with a high priority. High priority flows will get better quality tracks.

Although the advantages of SDN (such as programming, logical central control and flexibility) make it easy to detect defense DDoS attacks in traditional networks, and the separation of the control and data plane in the SDN enters new Attack Threats. For example, in the openflow based SDN, when it receives a new packet switch, checks it first whether there is a flow rule fixed in its Ternary Content Addressable Memory (TCAM) flow table is identical to this package first. If a match is found, the packet is redirected through flow rule. Otherwise, the buffers switch this packet and move the packet in a message to a new request controller flow rule. The control unit then responds with a message and the flow controller to instruct all the sharing keys with the rules to handle this new package (Gu, 2013). Attackers can take advantage of this feature of SDN to launch a DDoS attack on the switch, the data to the control channel, and the control unit, as shown in Figure 1.

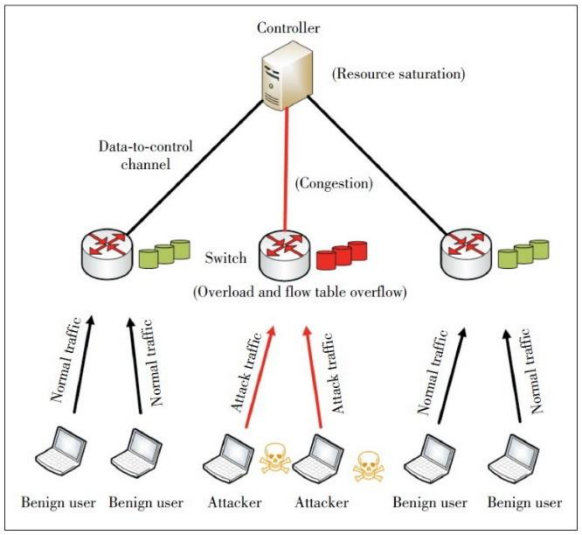

Fig 1: DDoS Attack in SDN

ATTACKERS' INCENTIVES

Distributed Denial of Service attackers are as a rule spurred by different incentives. We can categorize Distributed Denial of Service attackers based on the inspiration of the assailants into five fundamental categories as shown in the table 1.

Table 1: Attackers in basic categories

Type	motivation
1. Revenge	Attackers for this category of individuals are generally frustrated with the potential for low technical skills usually performing attacks as a response perceived injustice.
2. Mental Challenge	Attackers of this category attacks the focused on frameworks to try and learn how to dispatch different attacks. They are more often than not youthful hacking enthusiasts who need to appear off their capabilities. At present, there are many easy-to-use attack tools and a rent conviction that computer enthusiasts can even take advantage of in order to launch a successful DDOS attack.
3. Financial gain	These attacks are a major concern for businesses, since of the nature of their motivation, attackers of this category are more often than not the foremost specialized and the foremost experienced attackers. Attacks that are propelled for money related pick up are frequently the foremost unsafe and most serious attacks.
4. Cyberwarfare	Attackers of this category usually belong to military or terrorist organizations from a country and politically motivated to launch a large-scale attack a group of critical passages from another country (http://www.sbsun.com/ci 21392063/us-general-we-hacked-enemy, n.d.), (http://www.gideonrasmussen.com/article-14.html, n.d.) Potential targets for such attacks, But executive departments, not limited to civilians and Financial agencies and organizations in the public and private sectors (for example, National and commercial banks), energy and water infrastructure, telecommunications and mobile services Service Providers. Cyberwar attackers can be considered as very well prepared people with sufficient resources. Attackers Spend a great deal of time and resources in order Disable services, which may cripple the severity Country and has significant economic implications.
5. Ideological belief	Attackers who have a place to this category are propelled by their ideological convictions to attack their targets (N. Fultz, 2009). This category is as of now one of the major motivating forces for the aggressors to dispatch DDoS attacks.

DDoS ATTACKERS CLASSIFICATION

One of the essential steps towards deploying a comprehensive DDoS defense mechanism is to understand all the aspects of DDoS attacks. We review various ddos incidents of each type, some of which have been reviewed previously and well, and analyzed In (Reiher, April 2004), (U. Tariq, 2006), (C. Douligeris, 2014) Distributed Denial of Service attackers attacks can be classified into type based on the target protocol level:

1- Application-level DDoS flooding attacks:

These attacks focus on the disruption of services that are legitimately used by exhaustion of the resources provided by the server. DDoS on a standard application Attacks generally consume less transmission capacity than stealthier In nature compared to volumetric attacks because they are Very comparable to the movement of traffic. DDoS flood attacks on a level application are quite common the same effect on the services they target is specific Application properties such as Session Initiation Protocol (SIP), DNS or HTTP (Yadong Wang, 2017).

i. HTTP flooding attacks: There are four types of attacks :

A. Asymmetric attacks: In this category of attack, the attackers send sessions that have high load requests. At this point, we count a few of the famous attacks in this type.

Citation: Ahmed K. Al-Shammari, *et al.*, Distributed Denial of Service Attack Categories in Software-Defined Networks, Australian Journal of Basic and Applied Sciences. 12(11): 25-28. DOI: 10.22587/ajbas.2018.12.11.6

- *Faulty Application*: In this attack, attackers will benefit from sites with bad designs or dishonorable integration with databases.
- *Multiple HTTP get-post flood*: This attack is also a variation of HTTP get -post flood attack. At this point, the attacker creates multiple HTTP requests are made by configuring a single package with multiple included requests and without issuing them one by one within one HTTP session. In this way the attacker can still shuffle and keep high loads on target server victim of attacker with low packet attack rate making the attacker invisible in his attack and so to the netflow abnormality the techniques used to detect such an attack.

B. Request flooding attacks: In this type of attack, attackers will send sessions with more requests from the usual flood attack leads to DDoS on Server.
C. Slow request-response attacks: In this type of attack, attackers send sessions that have high load requests. There are a numeral of famous attacks in this type that we are explanation in the following.

- *Slowloris attack*: Slowloris may be a HTTP-based attack that can be dropped web server employing a constrained of devices or even one machine. The attacker sends two HTTP requests that are continuously grow fast, update slowly, never close.
- *HTTP fragmentation attack*: Comparable to Slowloris, the objective of this attack is to bring down a Web server by holding up the HTTP connections for a long time without raising any alerts.
- *Slowreading attack*: another type of attack in this category, which slowly reads the response instead of slowly sending applications. This attack accomplishes its reason by set the smallest frame size received from the target server send the buffer.
- *Slowpost attack*: In this type is very similar attack is for Slowloris to send HTTP its location commands Slowly to drop Web servers.

D. Session flooding attacks: In this type of attack, session call request rates from attackers are higher of requests from legitimate users; next, this Exhausts server resources and causes DDoS to flood Attack on the server.

ii. Reflection-amplification based attacks: These attacks use the same methods that their peers use at the network / transport level. For example, the attack uses DNS amplification Techniques of reflection and amplification. Attackers create small DNS queries with fake IP source Addresses that can generate a large amount of network traffic Since DNS response messages may be much larger than DNS query messages.

2- Network/transport-level DDoS flooding attacks: this is Most attacks have been launched using TCP, ICMP UDP, and DNS protocol packets. There are four types of attacks in this type.

A. Flooding attacks: Attackers focus on disrupting the legitimate user connection by exhausting the network bandwidth of the victim (eg, DNS flooding, UDP flooding, ICMP flooding, etc.
B. Reflection attacks: Attackers are frequent send fake requests instead of direct requests for reflections; next, these reflectors send their responses to victim and exhaust resources.
C. Protocol exploitation attacks: The attackers exploiting certain features or executing bugs from some victim protocols for excessive consumption of victim Resources.
D. Amplification attacks: Attackers exploit services to create large messages or multiple messages each message they receive amplifies the traffic towards the victim.

The classification of the type of Distributed Denial of Service attacks is that DDoS, like most malware security threats, multidimensional. Classifications be able to summarized in Figure 2

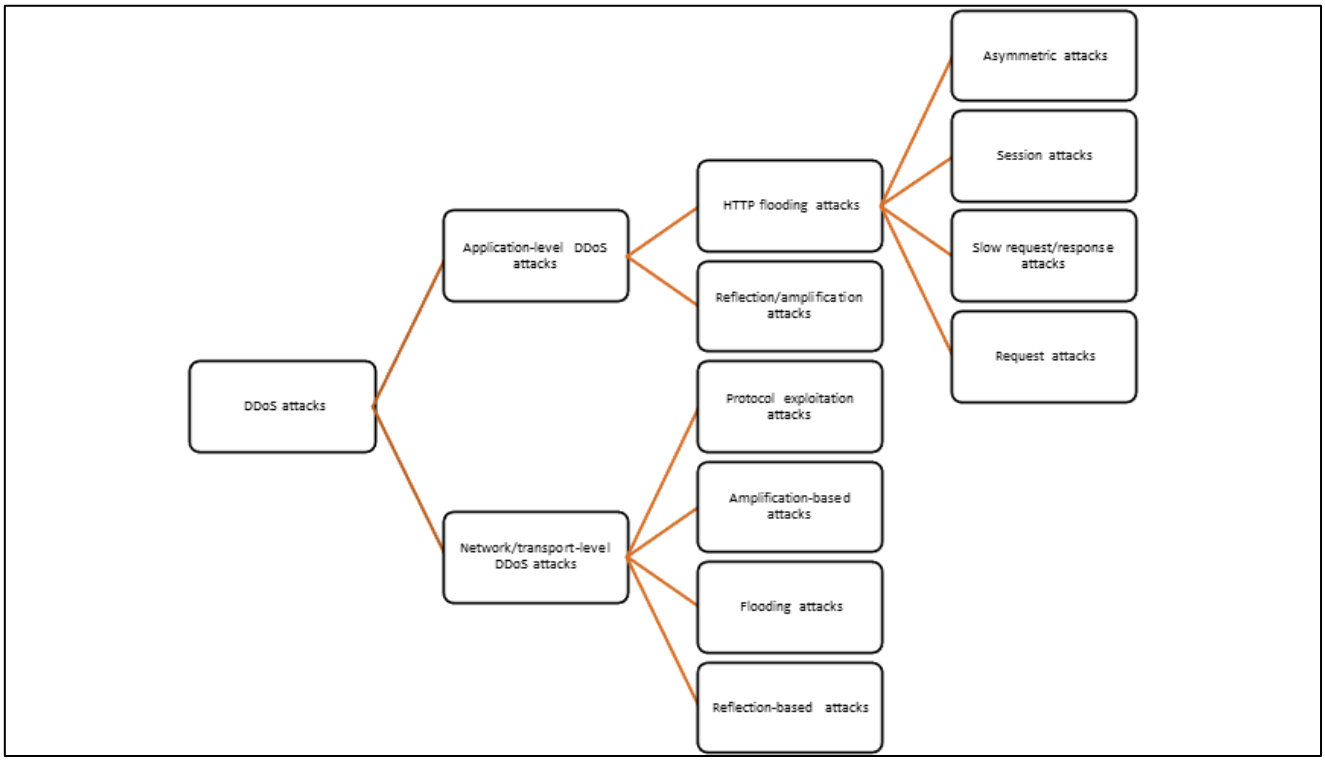

Fig 2: A type structure of DDoS attacks.

Citation: Ahmed K. Al-Shammari, *et al.*, Distributed Denial of Service Attack Categories in Software-Defined Networks, Australian Journal of Basic and Applied Sciences. 12(11): 25-28. DOI: 10.22587/ajbas.2018.12.11.6

CONCLUSIONS

In this paper, we have presented DDoS Attacks in the SDN network, we do this analysis of DDoS attacks so that researchers interested in Ballet defense can defend DDoS attacks. Enhance any mechanism to your network and find the SDN Advantages of building an automatic defense for DDoS Attacks. In the future, we aim to analyze several possible scenarios of DDoS attacks on the SDN network and analyze the results in detail in order to create a unique model for the defense of the court in order to avoid providing all sources of legitimate network users fairly.

REFERENCES

C. Douligeris, a. A. (2014). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, Vol.44, No. 5, pp. 643-666.

C. Lorenz, D. H. (2017). An SDN/NFV‐enabled enterprise network architecture offering fine ‐ grained security policy enforcement. *IEEE Communications Magazine*, vol. 55, no. 3, pp. 217-223.

Gu, S. S. (2013). Attacking software‐defined networks: a first feasibilitystudy. *ACM SIGCOMM Workshop SDN* (pp. pp. 165-166). Hong Kong, China,: ACM SIGCOMM.

http://www.gideonrasmussen.com/article-14.html. (n.d.).

http://www.sbsun.com/ci 21392063/us-general-we-hacked-enemy. (n.d.).

Kshira Sagar Sahoo, Ranjan Kumar Behera, Bibhudatta Sahoo, & Mayank Tiwary. (2018). Distributed Denial-of-Service Threats and Defense Mechanisms in Software-Defined Networks: A Layer-Wise Review. *taylor & francis*, 35.

M. Jarschel, T. Z. (2014). Interfaces,attributes, and use cases: a compass for SDN. *IEEE*, vol. 52, no. 6, pp. 210-217,.

N. Fultz, a. J. (2009). Towards a Model of Distributed Security Attacks, In Financial Cryptography and Data Security. *Roger Dingledine and Philippe Golle (Eds.). Lecture Notes in Computer Science*, (pp. vol. 5628, Springer-Verlag, pp. 167-183). Berlin,Heidelberg.

Nunes, B. A., Marc Mendonca, Xuan-Nam, Katia Obraczka, & Thierry Turletti. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *Communications Surveys & Tutorials, Volume: 16, Issus:3*.

Q. Duan, N. A. (2016). Software‐defined network virtualization: an architectural framework for integrating SDN and NFV for service provisioning infuturenetworks. *IEEE Network*, vol.30,no.5,pp.10-16.

Qiao Yan, F. Richard Yu, & Qingxiang Gong. (2016). Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. *IEEE Communications Surveys & Tutorials (Volume: 18, Issue: 1*, 602 - 622.

R. Sahay, e. a. (2015). Towards Autonomic DDoS Mitigation using Software Defined Networking. *NDSS Workshop on Security of Emerging networking Technologies*.

Reiher, J. M. (April 2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communications* , vol.34, no. 2, pp. 39-53.

S. K. Fayaz, Y. T. (2015). Bohatei: flexible and elastic DDoS defense. *Usenix Conference on Security Symposium*, (pp. pp. 817-832). Washington, D. C.

Saman Taghavi Zargar, James Josh, & David Tipper. (2013, March 28). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046 - 2069.

Somani, G., Manoj Singh Gaur; , Sanghi, Dheeraj;, Conti, Mauro;, & Buyya, Rajkumar. (2017). DDoS Attacks in Cloud Computing :Issues, Taxonomy, and Future Directions. *Elsevier,Computer Communications,, 107*, Pages 30-48. Retrieved from http://dx.doi.org

SteveMansfield-Devine. (2015). The growth and evolution of DDoS. *Elsevier, 2015*(10), 13-20.

U. Tariq, M. H. (2006). A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques,. *ADMA LNAI*, pp 1025-1036.

Yadong Wang, L. L. (2017). A novel approach for countering application layer DDoS attacks. *IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. Chongqing, China: IEEE.