# Research and Solutions for DDoS Detection and Mitigation with Software Defined Networks

Branislav Mladenov[1]

.

*Abstract* – **In this paper several Distributed Denial of Service (DDoS) detection and mitigation solutions are provided. The detection is handled by Software defined network (SDN) network and the SDN controller takes actions so the malicious traffic to be filtered or isolated.**

*Keywords* – **SDN, DDoS attack, DDoS mitigation, Openflow**

## I. Introduction

Software defined network (SDN) is one of the most promising architecture that decouples control plane from data plane and centralize network management. Comparing with legacy networking it has many more advantages and provides flexibility and scalability of the network. The centralized SDN controller can easily detect and protect the network from many vulnerabilities and security problems that threats traditional networking. Based on its Application Programming Interface(API) and programmability it can take proper actions and defend the network in case of Distributed Denial of Service (DDoS) attacks. There are many solutions that can detect DDoS attacks and takes some actions but unfortunate even the attack is detected most common problem is that during the attack the internet service provider channel gets full so the access is blocked until the attack stops. Distributed Denial of Service (DDoS) attacks are one of the most challenging security threats today. Flooding corporate networks or web sites with huge amount of malicious traffic block their services. The main goal is to exhaust network or computer resources in order legitimate traffic not to reach its destination. SDN architecture provides many benefits with decoupling the control plane from data plane on one hand, but on the other hand we have a centralized infrastructure that can be attacked so whole network will be affected. In this article, solutions for fast detection on control plane or data plane level and taking counter measure for blocking the attack are proposed.

## II. DDoS type of attacks.

Denial of service attack method is most commonly used for service availability degradation of the target. There are several types of attacks and can be classified based on Open Systems Interconnection (OSI) model as: Layer 3 flood attacks, Layer 4 Transmission Control Protocol (TCP) state exhaustion attacks and Layer 7 application attacks [1].

Layer 7 application attacks are exploiting application level protocols like Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP) and they are on 24 % of DDoS attacks. These kinds of attacks are usually harder to detect and protect because the amount of traffic is not much more that the legitimate traffic. Layer 4 TCP attacks target to exhaust the resources on TCP level and takes round 20% of DDoS attacks. Both methods are not based on the volume of traffic rather on the combination of traffic that can affect the protocols. Few of the most dangerous DDoS attacks these days are: DNS torques water attack: flood attack targeting company DNS server with many lookup requests to consume DNS server resources; Secure Sockets Layer (SSL)-based DDoS attacks, they can be Hypertext Transfer Protocol Secure (HTTPS) flood or encrypted SYN flood attacks; permanent DDoS attack which damages the systems hard enough to break the hardware.

Layer 3 attacks are the most common attacks. The idea is to send a huge amount of User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) traffic from different sources facing the targeted host [2]. There is a huge increase of these kinds of attacks due to the increase of Internet of things (IoT) devices in 2017. There were 91% more attacks than 2016 [3] Today it is much easier to hack smart household devices like smart television, fridge or Closed-circuit television (CCTV) because most of them have never been updated with the latest Operating System version so their vulnerabilities have not been fixed.

## III. DDoS protection mechanism

There are many articles and researches for DDoS detection and mitigation. In general, there are two methods of detection [4]. First one is based on some well-known predefined protocol patterns. The second one is an anomaly based method which collects statistics of regular traffic and analyzes all the time. For both methods all incoming traffic is checked and if a deviation is detected, proper actions can be taken. Most commonly used devices for DDoS detections are web application firewalls (WAF) and Intrusion prevention systems (IPSs). WAFs are focused to detect layer 7 type of attacks while the IPS can detect all kind of protocols or patterns and try to block the malicious traffic while the legitimate traffic is passed. To learn which kind of traffic is legitimate and which is not the devices should be switched to a learning mode for several weeks before it is runt

[1] Branislav Mladenov is with the Faculty of Telecommunications at Technical University of Sofia 8 Kl. Ohridski Blvd, Sofia 1000 Bulgaria, E-mail: branislav.mladenov@gmail.com

into production. IPSs are smart devices and can block malicious traffic but unfortunately once the system detects the attack it is already too late because the IPS is deployed within customer's network and when the attack starts the whole internet bandwidth is allocated with malicious traffic and customer's services is totally blocked until the attack stops. Hosting companies are suffering from DDoS attacks because even only one of the customers has been attacked, all other customers are affected as well due to a reason that they share same internet service channel.

## IV. Security solution with SDN

Software defined network has many benefits than traditional networking and some of them can be successfully used for DDoS protection and mitigation [5]. Separation the control plane from data plane makes the controller really easy to detect and react to DDoS attack very quick and efficient. With its global flow monitoring, the centralized controller can see and analyze the attack which comes from different sources and enters from different locations of the network. The controller can communicate with external IPS applications via its southbound interface and to provide summarized information about incoming traffic so prevention systems will analyze and take a decision which flows are part of the attack and which are legitimate traffic. SDN controller can rapidly and precisely creates policies based on the information provided from IPS that can be applied on the edge of the network. With its programmable interface the controller can communicate with other controllers within the Autonomous system (AS) or with other controllers that manage networks closer to attack sources or Tier 3 internet service provider can send information to its Tier 2 services provider when the attack is detected. The centralized controller is able dynamically and quickly to add or delete rules that can speed up DDoS mitigation. Comparing with the traditional network all features of SDN controller reduces the cost, the speed of reaction and the lack of human mistakes.

## V. Security issues with SDN and DDOS

SDN network has many benefits that make network architecture more scalable, more secured and reduce cost it comes with its own disadvantages. SDN can be attacked on application layer, control layer or infrastructure layer [6]. All type of attacks targets resource exhaustion of SND infrastructure. Decoupling the control plane from data plane provides many features but in case of DDoS attack, the centralized SDN controller becomes a target because requests that will arrive on the edge switches will be new for them and not part of the switches Ternary Content Addressable Memory (TCAM) table so according to Openflow protocol version 1.3 the switch buffers the packet and ask the controller how to proceed with it [7]. During Infrastructure type of DDoS attack all malicious request will create a *packet_in* message that will be sent to the controller Fig.1. This can load the secured channel between the switch and the controller so no legitimate requests can be handled. On the other hand, the switch has a buffer with limited resources so in case of an attack it might be overloaded so again no new legitimate request can be processed [8]. SDN switch TCAM table has limited resources so during the attack it can be quickly filled up with malicious records. Control layer DDoS attacks are targeting the controller that has limited resources as well and if it has to process a huge number of requests its Central Processing Unit (CPU) and memory might be exhausted very fast. The communication between SDN controller and all switches is secured and encrypted which allocate much more resources for encryption and decryption of the traffic. Application DDoS attacks target the applications used by SDN controller and northbound API interface. Fig.1

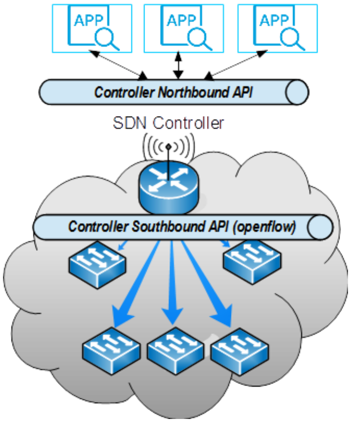
APP
APP
APP
Controller Northbound API
SDN Controller
Controller Southbound API (openflow)

Fig1. SDN architecture.

There are many proposed solutions that can detect a DDoS attack and protect SDN network. One of the proposals is based on sFlow protocol [9]. sFlow agent can be installed on each switch it can collect flow statistics and send them to sFlow collector which can analyze them. The sFlow collector can summarize and create rules for malicious traffic flows that can be configured from SDN controller. In order to protect the channel between switches and controller rate limits can be configured on that link, so in case of attack the channel and the controller will not be overloaded with malicious requests. SDN controller can detect DDoS attack very quickly if thresholds are set on its resources or based on a number of *packet_in* requests received per seconds.

## VI. Proposed solutions

In this section, several solutions for DDoS detection and mitigation are proposed.

### *A. First solution.*

This solution proposes automatic DDoS attack detection in customer's network with automatic internet service provider notification. The notification can be provided through dedicated for this purpose virtual local area network (VLAN) and Border Gateway Protocol (BGP) session. Once the ISP is notified it can forward the whole customer's traffic through its DDoS mitigation system to filter the malicious requests. Internet service provider's (ISP's) DDoS mitigation service is expensive so customers should use it only when there is an attack.

Based on the analysis in the previous section a DDoS attack can be detected fast either from the switches with sFlow protocol, or when the controller's thresholds are reached. The controller can automatically send a message to Internet service provider application which can activate its DDoS mitigation system. Fig.2

In traditional networking these functions are manual and the mitigation depends on the engineer on duty reactions. He or she has to be notified via monitoring system which may take 1 to 3 minutes and he or she should manually trigger the DDoS protections which may take 5 to 10 minutes. The proposed SDN solution has several benefits:

- Time for reaction. The time for reaction between the start of the attack and its mitigation is minimized because it is fully automatic. The detection can take up to 10 seconds and automatic notification less than a second.
- There are no manual actions which prevent human mistakes.
- Reduce cost. There is no need of engineer who monitors manual DDoS monitoring system. There is no need for additional DDoS monitoring system.
- Reduce cost of ISP's DDoS mitigation service because it is used during the attack only.

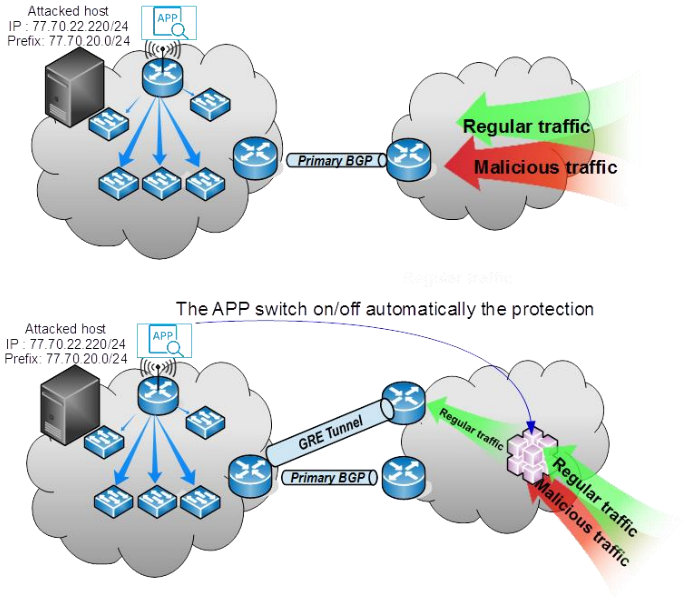

Fig.2 DDoS attack detection and notification.

*B. Second solution.*

This solution proposes automatic DDoS detection and changes traffic flow of attacked target. Hosting companies and cloud providers can be heavily impacted by the DDoS attack because all customers share one and the same internet service in most of the cases. The bandwidth is enough for legitimate traffic but in case of DDoS attack targeting only one customer, all other customers are affected when the channel gets full. If hosting company or cloud provider doesn't have DDoS protection provided from the ISP it is almost impossible to stop the attack before it affects the internet service channel. In most of the cases cloud providers have more than one channel for internet service so once the attack is detected and the target is identified, its prefix can be advertised via the second/backup internet service channel. This will not stop the attack but at least all other customers will not be affected anymore.

DDoS detection with SDN can be achieved very fast and based on the sFlow analysis the target can be identified in seconds. Once this is done the controller can automatically isolate the target via backup internet service provider link or can send commands to edge router that will advertise the targeted prefix via the secondary service provider link. Fig.3

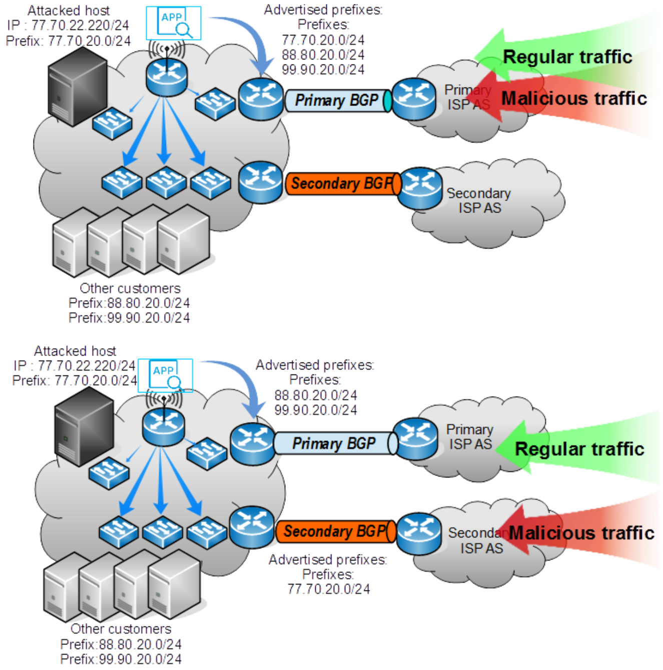

Fig.3. Advertising attacked prefix via secondary ISP.

In traditional networking, these activities can take more than 15 to 30 minutes and depends of manual actions of engineer on duty and its knowledge.

The proposed SDN solution has several benefits:

- Time for reaction. The time for reaction between the start of the attack and targeted destination traffic flow change is minimized because it is automatic. The detection can take up to 10 seconds and flow reroute can take less than a second.
- There are no manual actions which prevent human mistakes.
- Reduce cost. There is no need of engineer who manually has to change the flow of the targeted prefix.

### C. *Third solution*

It proposes DDoS mitigation that blocks the traffic as close as possible to the source of the attack. As we explained in the previous section the switches can identify the target and the sources via sFlow protocol. This information can be sent to a sFlow collector that can create a database of the affected sources which can be used for following purposes Fig.4:

- Flow blocking rules can be created based on the database. The rules can be used by other SDN controllers that are closer to the sources. This can stop the malicious traffic before it hits the destination network and will not load all service providers' networks between the source and target.
- It might be the case that malicious sources are not part of any SDN network but just a traditional network with next generation firewalls that have API interface. The application can track all new records of the database and create blocking rules that which be applied automatically to the firewall in an outbound direction so the malicious traffic will not exit its network.
- The database can be used anytime during an attack or it can be analyzed and if some of the sources are used several times for different DDoS attacks it can be marked as malicious source. Once such malicious sources are identified in the database they can be blocked permanently by internet service providers.

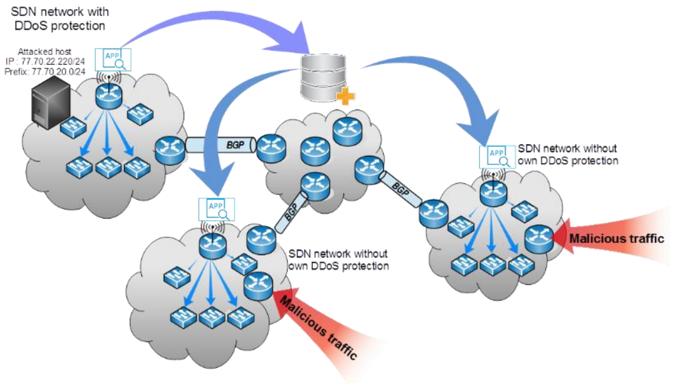

Fig.4 DDoS mitigation with malicious sources data base.

## VII. Conclusion

Denial of service attack is still one of the biggest internet security challenges these days. In this paper, we discussed what type of DDoS attacks are most commonly used and types of protection mechanisms.

With this paper, several solutions that can help to detect DDoS attacks faster than traditional networks are proposed. With SDN controller programmable interface, DDoS mitigation can be achieved in a second and can be blocked even closer to the source which will stop malicious traffic. All proposed solutions can reduce cost and network resources. On another hand SDN networks are still vulnerable to DDoS attacks but counter measures can be taken to protect the controller. The essential part of this is fast and accurate attack detection so with proper monitoring and applications companies can protect their network and services without affecting legitimate traffic. This paper provides just few SDN solutions that can be part of much bigger and efficient DDoS protection architecture.

## References

[1] M.Jeyaraman, R.Saravanaprabu "A Survey and New Perspectives on Classifying the DDOS Attack with Their Characteristics" International Journal on Recent and Innovation Trends in Computing and Communication , IJRITCC | August 2016, Available

[2] N. Dayal, P. Maity, S.Srivastava, R. Khondoker "Research trends in Security and DdoS" . SecurityComm.Networks2016; 9:6386–6411 . Published online 9 February 2017 in Wiley Online Library (wileyonlinelibrary.com).

[3] P.Lee, D. Stewart, "Global TMT Predictions 2017 Analysis" , August 2016

[4] S. Luo, Jun Wu, B. Pei. "A Defense Mechanism for Distributed Denial of Service Attack in Software-Defined Networks". Frontier of Computer Science and Technology (FCST), 2015 Ninth International Conference

[5] W. Xia, Y. Wen, C. Foh, D. Niyato, and H. Xie, "A survey on softwaredefined networking," IEEE Commun. Surveys & Tutorials, vol. 17, no. 1, pp. 27–51, First Quarter 2015.

[6] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for openflow networks," in Proc. First Workshop on Hot Topics in Software Defined Networks, 2012, pp. 121– 126.

[7] M. D. Yosr Jarraya, Taous Madi, "A survey and a layered taxonomy of software-defined networking," IEEE Commun. Surveys & Tutorials, vol. 16, no. 4, pp. 1955–1980, Fourth Quarter 2014.

[8] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network (SDN) and openflow: From concept to implementation," IEEE Commun. Surveys & Tutorials, vol. 16, no. 4, Fourth Quarter 2014.

[9] C. YuHunag, T. MinChi, C. YaoTing, C. YuChieh, and C. YanRen, "A novel design for future on-demand service and security," in Proc. 12th IEEE Int'l Conf. Commun. Technology, 2010, pp. 385–388.