Future of DDoS Attacks Mitigation in Software Defined Networks

Martin Vizváry, Jan Vykopal

Institute of Computer Science, Masaryk University, Brno, Czech Republic
{vizvary|vykopal}@ics.muni.cz

Abstract. Traditional networking is being progressively replaced by Software Defined Networking (SDN). It is a new promising approach to designing, building and managing networks. In comparison with traditional routed networks, SDN enables programmable and dynamic networks. Although it promises more flexible network management, one should be aware of current and upcoming security threats accompanied with its deployment. Our goal is to analyze SDN accompanied with OpenFlow protocol from the perspective of Distributed Denial of Service attacks (DDoS). In this paper, we outline our research questions related to an analysis of current and new possibilities of realization, detection and mitigation of DDoS attacks in this environment.

Keywords: Software Defined Networking, SDN, Distributed Denial of Service Attack, DDoS, OpenFlow, security, detection, mitigation

1 Introduction

Even though computing has advanced over the past decades, the networking principles have remained mostly unchanged. Traditional networks are built using switches and routers. Every vendor uses a proprietary operating system and configuration in these network devices. Emerging clouds and Internet of Things demand scalable and dynamic networks. However, building a suitable network with centralized management in such a heterogeneous environment is very expensive. One new architecture that replaces traditional networking is Software Defined Networking (SDN). SDN abstracts network control from the underlying infrastructure of the network. This abstraction enables applications and network services to treat the network as one logical entity. This could increase the potential for the better mitigation of security threats.

A DDoS attack is an attempt to make a network or server resource unavailable to its intended users. The attack is relatively easy to perform, hard to defend against, and the attacker is rarely traced back. The target of a DDoS attack could be any online business, government or critical infrastructure. Increasing numbers of DDoS attacks in current networks also increases the awareness of them and makes them a major threat to today's networks. The deployment of SDN will not stop attackers, however, it could make mitigation techniques more effective and their deployment more flexible.

Our research will be dedicated to an analysis of security challenges in SDN from the point of view of DDoS attacks. Although SDN promises more flexible network management, one should be aware of current and upcoming security threats accompanied with the deployment of SDN. The abstraction of data and control plane devices introduces new potential threats.

The remainder of this paper is organized into four sections. Section 2 briefly describes the state of the art in SDN. Section 3 states our hypothesis and research questions. Section 4 outlines the scientific approach. Section 5 summarizes this paper.

2 Software Defined Networking

SDN is an emerging network architecture. It is supported by many large companies listed on Open Networking Foundation[1] list [3], e. g., Google [4] or Cisco Systems [2]. SDN is based on the abstraction of a data plane from a control plane. This abstraction makes networks more programmable and flexible. Figure 1 describes the basic SDN architecture.

The control plane consists of one or more SDN controllers. The controller maintains a global view of the network. It defines the forwarding rules of the devices in the data plane and performs all complex functions. All devices in the data plane are remotely configured by the controller via well-known and vendor-neutral API. It allows the controller to manage different types of devices from different vendors. The data plane contains simple forwarding devices, e. g., switches. From the point of view of the controller, devices in the data plane could act as a single logical entity. These devices forward all traffic according to rules in flow tables. If there is not a matching forward rule for a packet, the packet is forwarded to the controller. The communication between the controller and data plane devices needs a suitable standard. Such standard seems to be the widely supported OpenFlow protocol [6]. It provides an open and standard way for a controller to direct communication with a network device in the data plane.

Many SDN and OpenFlow security challenges have been proposed in the literature [8]. We will focus on DDoS attacks since they have become a major threat in modern-day networks. Due to the centralization of controller and flow table limitations in data plane devices, there is an increased potential for new DDoS attacks in SDN networks as well.

3 Hypothesis and Research Questions

Our hypothesis is that *SDN provides an ideal platform for distributed detection and mitigation of DDoS attacks*. SDN emerges as a promising network paradigm. The new concept of networking guarantees programmable and dynamic networks. They could react faster and with better efficiency to necessary changes in

[1] The organization dedicated to the promotion of SDN through open standards development

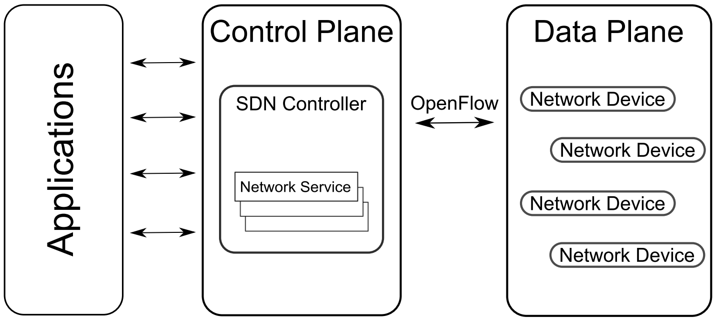

Fig. 1. Software Defined Networking architecture schema

networking. This could help to mitigate the DDoS attack. However, the attacks could also take advantage of the overhead of the SDN controller. We split our research into the following three research questions:

1. *What differences does SDN bring compared to traditional networks and its monitoring?*

   This research question aims to gain an understanding of SDN that separates the networking into the data and control plane. We will analyze and compare the differences between SDN and current networks. The research will also cover the analysis of monitoring possibilities in SDN.

2. *What are SDN specific security vulnerabilities both on the data and control planes? In particular, what known or new vulnerabilities of SDN can be abused by attackers in DDoS attacks?*

   The goal of this question is to analyze possible abusive attributes of the data and control plane. At first, we will focus on open-source solutions, e. g., Open vSwitch [1]. We will analyze possibilities of DDoS attacks abusing data and control plane devices as a bottleneck, reflector or amplifier. Abstraction of the control plane from the data plane might cause serious overhead when there are too many requests from the data plane. Also the misconfiguration or direct abuse of the central controller or one of the data plane devices could cause denial of network access for users.

3. *How to optimally mitigate DDoS attacks in Software Defined Networks?*

   The main goal of this question is to find a method to optimally mitigate spoofed and non-spoofed DDoS attacks in a SDN environment. We will analyze different DDoS attack methods and propose the optimal way for mitigating attacks. We will also pay attention to the trace-back of the source of an attack using the advantages of the SDN architecture.

4 Scientific Approach

In our research, we will focus on security challenges in DDoS attacks detection and mitigation in SDN environment. At first, we will create a state of the art in SDN network monitoring and security. This analysis will provide required understanding of the SDN and related issues.

Next, we will analyze attack, defense and monitoring mechanisms in current networks and the possibility of their deployment in SDN environment. Monitoring is nowadays mostly done at the host or network level in attacked networks. There are many variants of DDoS attacks as well as defense mechanisms against them proposed for current networks [10]. We believe that those methods could be adopted in SDN. Flow-based techniques are mostly used for the detection of DDoS attacks. Due to the flow-based nature of SDN, it is possible to make detections in both planes. However, detection mechanisms deployed in the controller without proper aggregation of network traffic could overload the communication among control and data plane. Also, the flow table in a network device has limitations. Shin et al. [9] proposed that some of these issues could be resolved by adding some minimal intelligence to the data plane devices.

The main goal of our research is to mitigate the attack using SDN architecture. For the sake of simplicity, we consider two groups of DDoS attacks. The first group targets the computing power. The second group exceeds available bandwidth. The first group could be mitigated using a SDN infrastructure of the attacked organization. We could use all network devices as one logical switch to load balance the network traffic through the network. This load balancing of attack traffic gives us the possibility to configure as many filtering rules as possible to maximize the amount of dropped malicious traffic. However, for the second group, this option is not effective. We have to stop the attack closer to the source of traffic, e. g., country of origin, or ISP of the attack source. Even though this mitigation technique requires a cooperation of involved providers in the route of the attack and complex reconfiguration of ISP routing tables, the flexible SDN environment could make this reconfiguration easier. The first SDN application that programs networks for DoS security against network flood attacks is Radware DefenseFlow [7]. However, it is not a "pure" SDN solution and it still has to cooperate with dedicated mitigation hardware.

At last, to prove our hypotheses, we will prepare a pure SDN infrastructure. We will use an environment prepared in Cybernetic Proving Ground (CPG) project [5]. In this environment, we will create set of synthetic and real traffic based data sets and experimentally verify the hypothesis.

5 Summary

Research questions 1 and 2 aim to obtain a thorough understanding of SDN in the context of DDoS attacks. It is crucial to understand SDN for answering the third research question. Our goal in research question 3 is to find the optimal way to mitigate DDoS attack using the SDN infrastructure. The main goal should be achieved within a period of three years as a part of a PhD thesis.

Acknowledgments

This material is based upon work supported by Cybernetic Proving Ground project (VG20132015103) funded by the Ministry of the Interior of the Czech Republic.

References

1. Open vSwitch – An Open Virtual Switch. Project website. http://openvswitch.org/ [Accessed Jan 27, 2014].
2. Cisco. Software-Defined Networking: Why We Like It and How We Are Building On It. White paper, Cisco Systems, San Jose, CA, USA, 2013.
3. Open Networking Foundation. Member Listing – Open Networking Foundation. Website. https://www.opennetworking.org/membership/member-listing [Accessed Jan 21., 2014].
4. Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jon Zolla, Urs Hölzle, Stephen Stuart, and Amin Vahdat. B4: Experience with a Globally-Deployed Software Defined Wan. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, pages 3–14, New York, NY, USA, 2013. ACM.
5. Daniel Kouřil, Tomáš Rebok, Tomáš Jirsík, Jakub Čegan, Martin Drašar, Martin Vizváry, and Jan Vykopal. Cloud-based Testbed for Simulation of Cyber Attacks. In *Proceedings of the 2014 IEEE Network Operations and Management Symposium, NOMS 2014*, 2014. To appear.
6. Open Networking Foundation. Software-Defined Networking: The New Norm for Networks. White paper, Open Networking Foundation, Palo Alto, CA, USA, 2012.
7. Radware. DefenseFlow – Software Defined Networking Application. Product website. http://www.radware.com/Products/DefenseFlow/ [Accessed Jan 21., 2014].
8. Sandra Scott-Hayward, Gemma O'Callaghan, and Sakir Sezer. SDN Security: A Survey. In *Proceedings of the Software Defined Nnetworks for Future Networks and Services (SDN4FNS), 2013*, pages 1–7, 2013.
9. Seungwon Shin, Vinod Yegneswaran, Phillip Porras, and Guofei Gu. AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-defined Networks. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer Communications Security*, CCS '13, pages 413–424, New York, NY, USA, 2013. ACM.
10. S.T. Zargar, J. Joshi, and D. Tipper. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *Communications Surveys Tutorials, IEEE*, 15(4):2046–2069, 2013.