Optical Fiber Technology 39 (2017) 37–42

Contents lists available at ScienceDirect

Optical Fiber Technology

journal homepage: www.elsevier.com/locate/yofte

Regular Articles

Exploring machine-learning-based control plane intrusion detection techniques in software defined optical networks

Huibin Zhang, Yuqiao Wang, Haoran Chen, Yongli Zhao*, Jie Zhang

Beijing University of Posts and Telecommunications, Beijing 100876, China

ARTICLE INFO

Keywords:
Optical networks
Control plane
Intrusion detection
Machine learning

ABSTRACT

In software defined optical networks (SDON), the centralized control plane may encounter numerous intrusion threatens which compromise the security level of provisioned services. In this paper, the issue of control plane security is studied and two machine-learning-based control plane intrusion detection techniques are proposed for SDON with properly selected features such as bandwidth, route length, etc. We validate the feasibility and efficiency of the proposed techniques by simulations. Results show an accuracy of 83% for intrusion detection can be achieved with the proposed machine-learning-based control plane intrusion detection techniques.

1. Introduction

Software Defined Optical Networks (SDON) is a network architecture, applying the concepts and techniques of software defined networks (SDN) to optical transport networks [1,2]. It gradually becomes the trend of future optical network, as it provides fast and customizable services while achieving the goals of high resource utilization and flexible service supply [3–6]. In control plane of SDON, the controller serves as the main component. On account of the centralized control plane, it brings about advantages like constructing a flexible, open and intelligent optical network architecture for services by logically controlling the network resources and statements. The control plane realizes the flexible service access and the unified hardware control through its two interfaces, i.e., open southbound interface (SBI) and northbound interface (NBI), respectively.

However, the centralized control plane makes it vulnerable to numerous intrusions, as once the controller is hijacked by the attacker, the whole network will be faced up with an out of order circumstance. Therefore, the secure operations of both the controller and the network are compromised. Specifically, an attacker pretending to be a customer is able to intrude the controller by maliciously occupying or delete a massive number of connections or light paths in a short period of time, causing resource exhaustion, service disruptions [7], etc. How to tackle this secure problem in SDON control plane and ensure the stable network operation becomes a significant problem.

A common method used by network managers to detect illegal intrusion in control plane is called security rule matching. It does so by initializing a security-rule list and comparing each security rule in the list with incoming service request to check violations. The security-rule list can be further categorized into blacklist and whitelist based on the content of the security rules. Blacklist includes the behaviors and characteristics of all potential attacks and malfunctions. It resembles a collection of symptoms used to diagnose disease. However, the downside is that the full knowledge of complex and continuously changing attacks can be hard to obtain. Whitelist, as opposed to blacklist, includes the rules regarding normal system behaviors and functions. The main disadvantage of the whitelist is the lack of scalability and flexibility, because any change requires additional operating expense (OPEX) cost. Alternatively, data analysis using machine learning techniques can be another promising method of detecting intrusion, as proposed in [8]. As another example, Ref. [9] suggested a real real-time intrusion detection system with host-based data collection and processing. Note that existing intrusion detection techniques mostly focus on examining break-ins at compute level. However, SDON control plane requires detection occurring at network level. What is also worth noticing is that there are increasingly more researches focusing on analyzing optical network by means of machine learning techniques [10–14]. Hence, machine learning techniques could provide effective means to detect intrusions in the control plane of SDON [15]. To the best of our knowledge, we proposed for the first time, two 48977551609090machine-learning-based control plane intrusion detection techniques for SDON, which are point-anomaly-based scheme and sequence-anomaly-based scheme.

The rest of the paper is organized as follows. We present SDON control plane architecture in Section 2. Some control-plane security issues are described in Section 3. In Sections 4 and 5, we present two machine learning techniques for intrusion detection in the SDON control plane. In order to validate the efficiency and feasibility of our

* Corresponding author.
E-mail address: yonglizhao@bupt.edu.cn (Y. Zhao).

http://dx.doi.org/10.1016/j.yofte.2017.09.023
Received 16 July 2017; Received in revised form 8 September 2017; Accepted 27 September 2017

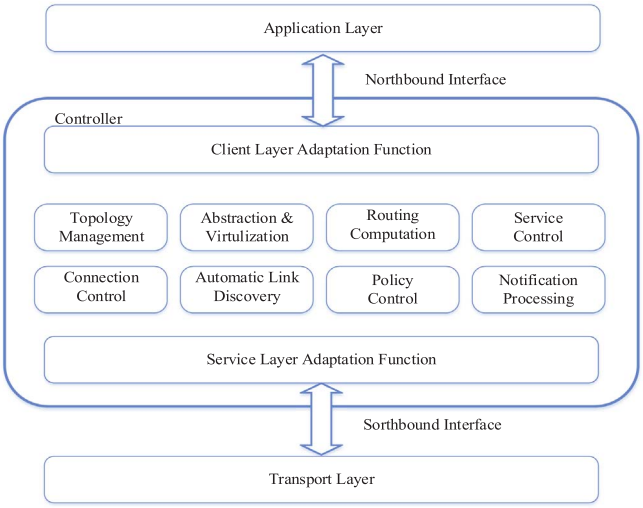

Fig. 1. Functions of SDON controller.

techniques, we use some service features, e.g., bandwidth and route length. Simulation results show an accuracy of 83% in the intrusion detection can be achieved in Section 6. Section 7 concludes the paper.

2. SDON control plane architecture

SDON migrates from original distributed control architecture to centralized control architecture, thus dismissing a number of service routing protocols, and simplifying the network [16–18], for the reason that path computing and path establishing can be completed in the controller. The main function of the controller is to manage the data forwarding of the transport plane through the programmable SBI and support applications developing with NBI. It also allows multi-layer control for resource optimization [17,19,20].

The SDON controller is a software entity that oversees transport-plane resources and opens the network control ability through standard interfaces. The controller integrates a series of functions such as topology resource management, topology abstraction and virtualization, routing computation, service and connection control, etc., as shown in Fig. 1. With the assistance of the service layer adaptation function, the controller obtains the resource information of the transport plane and achieves the connection control function. Then it provides services for the application plane by taking advantages of the client layer adaptation function.

(1) Topology management: obtains the network topology information including node switching capability, maximum and available bandwidth, link weight, shared risk link group (SRLG) information, link running status, etc.
(2) Abstraction and virtualization: abstracts some features of the network topology resources while hiding features that are independent of the selecting standards.
(3) Routing computation: computes end-to-end path for service connections.
(4) Service/call control: supports service establishment, modification and release functions.
(5) Connection control: establishes the required transport connection according to the service request, allocate resources, and complete the connection establishment, modification and release according to connection request parameters.
(6) Automatic link discovery: obtains the link information between two nodes by running the automatic discovery protocol on them.
(7) Policy control: provides appropriate business, security and survivability policies based on different management requirement and customer applications.
(8) Notification processing: notifies upper layer about network-status changes.

Here, the client layer adaptation function can provide the APIs for the customers after abstracting and virtualizing the resource topology in the transport plane according to the customers' demand. In addition, the client layer adaption function also has the responsibility to maintain the session with customers, as well as verify the identity of the customers.

SDON controller manages network elements (the smallest element that can be inspected and managed in network management). The communication channel between the controller and transport plane switches is called control channel. The controller communicates with the transport plane elements over the control channel by using the control protocol. Consequently, it is significant to establish and maintain the control channel between the controller and network elements, for the reason that if there exist a failure on it, the whole network will be down and out of control.

3. Potential intrusion threats

Control plane is a critical part in SDON architecture. Once it is under attack, most services can't be guaranteed. Here, we talk about some potential intrusion threats that the SDON control plane may encounter [21–24].

3.1. Unauthorized access

An attacker can get the access to control plane unauthorized by means of technical or nontechnical approaches, resulting in information leak and distortion. Control plane is connected to applications, network resources, etc. If the controller is impersonated, the attacker will gain access to network resources and will operate the network. Besides, if there is an unauthorized application trying to access the control plane with northbound API, the control plane is also under the intrusion threat.

3.2. Data leakage

In the southbound of SDN, OpenFlow switches process different category of signaling messages (including messages about cookies, flags, ports etc.), some of which are sent to the controller. An attacker can fake such packages after learning its patterns and features, such as changing the status flag in a signaling data package. These crafted packages form massive number of requests and take up large portion of network resources, thus causing Denial of Service (DoS) attack (a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet) [25,26].

3.3. Data modification

As mentioned previously, the controller can manage the traffic in transport plane by means of programming the network devices. If controller is hijacked, the whole network will be out of control. Then, attacker can modify the flow rules in network elements so that package forwarding strategy will change and cause a chaos in SDON.

3.4. Denial of service

One of the most distinctive features in SDON architecture is central controlling, which is also a vital weakness in terms of security. The controller communicates with network elements with the help of southbound API, and an attacker may make use of it to oversee the data packages with specific flow rules then flood them to the controller. It is often common that distributed DoS attack is used in traffic attack.