Computers and Electrical Engineering 000 (2017) 1–19

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Distributed controllers multi-granularity security communication mechanism for software-defined networking[☆]

Fengjun Shang[*], Yan Li, Qiang Fu, Wenkai Wang, Jiangfan Feng, Li He

College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China

ARTICLE INFO

Article history:
Received 30 December 2016
Revised 4 July 2017
Accepted 4 July 2017
Available online xxx

Keywords:
Software defined network
Security architecture
Secure communication

ABSTRACT

For the multi-domain software defined network (SDN), different controllers are not able to directly communicate with each other due to the different distances among control planes. Therefore, the exchange of information among different domains is generally unsecure. The main contribution of this paper can be summarized into two parts. Firstly, architecture of multi-granularity security controller is proposed, which includes a basic control module and a multi-granularity security customized module. Secondly, a secure communication mechanism is proposed for distributed controller, where a prototype of this mechanism is implemented. In particular, this mechanism can make use of the border switch as inter-domain agents, where special packets are used by the controller to send messages to the secure tunnel. A two-step authentication of the controller can be provided by inter-domain agents and digital certificates. The experimental results demonstrate that the distributed controller secure communication mechanism is capable of effectively improving the security of SDN domain.

1. Introduction

After the development of OpenFlow [2] protocol by researchers from Stanford University, the software defined networking (SDN) [1] has emerged as a novel network structure. Due to requirements of the new architecture, researchers have proposed RCP [3], 4D [4], SANE [5] and Ethane [6] architectures by utilizing decoupling control plane and data plane. With the successful application of the OpenFlow protocol, the open network foundation (ONF) was established in 2011, where the SDN white paper is published [7]. By using SDN, the protocol no longer completely depends on equipment manufacturers to deploy and develop. Notably, the network is capable of obtaining highly customizable and intelligent network management in SDN. Currently, the inter-domain controller communication standard is missing in SDN. However, it is of significant importance to secure the inter-domain information, where the stability and reliability of multi-domain SDN can be achieved.

This paper is structured as follows. In Section 2, previous works are reviewed on the intra-domain security and inter-domain interconnection. In Section 3, the Multi-granularity security controller architecture is proposed. Moreover, secure communication mechanism of the distributed controller is proposed, where the prototype of this mechanism is implemented in Section 4. Finally, the conclusion is presented in Section 5.

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Zhihan Lu.

[*] Corresponding author.
E-mail address: shangfj@cqupt.edu.cn (F. Shang).

http://dx.doi.org/10.1016/j.compeleceng.2017.07.003
0045-7906/© 2017 Published by Elsevier Ltd.

2. Related work

2.1. Intra-domain security

The research of SDN security mainly includes security enhancement of the SDN architecture and application of SDN. In [8], an independent trust management or abnormal device detection is proposed to prevent malicious device attacks. Moreover, multi-trust anchor authentication center of the oligopoly or threshold cryptographic system is proposed to resolve security issues of the control plane communication including TSL/SSL defects, which may result in DoS and DDoS attacks. In [9], the security of the controller can be obtained by using replication, diversity, recovery mechanism, important information protection and priority based safety rules.

In [10], two architectures are proposed to protecting the security in SDN network, which can decouple and reconstruct the security control plane and data plane.

According to the investigation, researchers have proposed frameworks of security application development for SDN. However, the specific security issues in SDN are not adequately addressed. Therefore, a security controller architecture which has more comprehensive security features and customized security services are required to be designed, where a more flexible and effective SDN Intra-domain security can be upgraded.

2.2. Inter-domain interconnection

It should be noted that it is impossible to control the entire network due to limited resources of a single controller. Researchers have proposed a number of distributed controller solutions to improve the scalability of the control plane. Currently, researchers have investigated the interconnection mechanism of multi-domain SDN. In [11], a route transition scheme from traditional network to SDN is proposed, which is known as BTSDN. In BTSDN, the boundary of the SDN autonomous domain can adopt the BGP border router. In particular, the inter-domain runs the EBGP protocol, and the intra-domain runs the IBGP protocol based on the software router in the controller. The controller is able to indirectly control the border router by the OpenFlow switch. In [12], a BGP architecture, known as OFBGP, is proposed for the SDN, which is an upper layer application in the distributed controller. As a SDN software router, it can manage and control the intra domain and inter domain. In [13], Inter-domain Management Layer (IML) is proposed to horizontally divide the SDN resources, where management of network boundary and information sharing between domains can be facilitated. In [14], a new routing and switching scheme SDX is designed for SDN. In SDX, the exchange of routes is performed by Internet exchange point (IXP). All the SDN autonomous domains can send routing information to the IXP, where the IXP is able to obtain routing information from other domains. SDX can achieve fine-grained forwarding within the same domain in the multi-domain SDN by learning the whole network routing information. Due to the limited number of IXP, there is no access to IXP SDN domain, where the program is not be able to solve the routing exchange. In [15], SDN inter-domain interconnection mechanism is investigated. A east-west bridging scheme for heterogeneous NOS is proposed in SDN, where the information to be interacted is also designed. In our scheme, the inter-domain controller employs the point-to-point communication mode. In addition to routing information exchange, the network view can be shared with other autonomous domains to obtain a global view. In [16], a controller architecture, DISCO, is proposed in a distributed SDN multi-domain network to establish inter-domain interconnection with the east-west interface of controller.

Based on the OpenFlow protocol, a multi-granularity security controller architecture is designed for multi-granularity security controller. The security interconnection requirements for inter-domain controllers are analyzed in multi-domain environments, and the secure communication mechanism for distributed controllers is also designed. Based on granular computing in the controller, security services can be flexibly customized in the intra-domain and inter-domain. Therefore, a multi-granularity security architecture can be established.

3. Multi-granularity security controller architecture

3.1. Controller architecture design

3.1.1. Security scheme

3.1.1.1. Controller defense scheme. In general, OpenFlow Packet-In messages is used by the denial of service attacks to send unknown flow. If the controllers receive Packet-In messages, the controller can obtain the source switch information, the header of data packet and so on. A Packet-In message is defined as PacketIn = (in_sw, in_port, in_res, src_mac, dst_mac, src_ip, dst_ip, src_port, dst_port). In particular, in_sw represents the switches sending the message, in_port represents the switch port sending the message, in_res represents the reason of sensing the messages, src_mac represents the source physical address of the packet, dst_mac represents the destination physical address of the packet, src_ip represents the source IP address of the packet, dst_ip represents the destination IP address of the packet, src_port represents the source port of the transport layer, and dst_port represents the destination port of the transport layer. Based on the definition of the Packet-In message, Packet-In flow-based detection or machine-based detection can be used to identify and block malicious Packet-In messages. As a result, the controller can be protected against DoS attacks.

Please cite this article as: F. Shang et al., Distributed controllers multi-granularity security communication mechanism for software-defined networking✩, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.07.003