InSAVO: Intra-AS IP Source Address Validation Solution with OpenRouter

Tao Feng, Jun Bi, Hongyu Hu, Guang Yao, Peiyao Xiao
Network Research Center, Tsinghua University, Beijing, China
Department of Computer Science, Tsinghua University, Beijing, China
Tsinghua National Laboratory for Information Science and Technology (TNList), Beijing, China
fengt09@mails.tsinghua.edu.cn, junbi@tsinghua.edu.cn, huhongyu@cernet.edu.cn, {yaog, xiaopy}@netarchlab.tsinghua.edu.cn

Abstract—In this demo, we introduce an OpenFlow extension and implementation in a commercial router, named OpenRouter. We demonstrate a solution of intra-AS IP source address validation with OpenRouter to show OpenRouter is a feasible and evolvable paradigm for software-defined network. This demo illustrates that OpenRouter not only solve some limits in current network architecture with software-defined networking features, but also give a tradeoff between software-defined features and evolution cost by means of software image update using existing hardware of a router.

Keywords—OpenFlow; OpenRouter; SDN; IP source address validation

I. INTRODUCTION

Software-defined networking (SDN) has become a promising trend for future Internet development. Current researches mainly focus on flow management, security and QoS using OpenFlow [1] switch in data center network or campus network. But in the production network where routers are dominant, some of the challenges in the implementation and deployment of SDN are the integration of existing protocols inside a network device with new protocols, the tradeoff between hardware cost and deployment profit of network evolution to SDN.

Intra-AS source address validation is defined in Source Address Validation Architecture (SAVA) [3]. Central control mechanism is a good way to validate IP source address in an AS because the mechanism can get a global forwarding path and then resolve false positive of filtering information caused by asymmetric routing more than ingress filtering. Forwarding path information is calculated with routing and interface information. In the current network architecture, SNMP polling to get the two types of information will result in false positive of filtering information due to not get routing change information in time. And it is very complicated to implement the protocol with multi protocols due to information retrieval with SNMP, packet sampling with xFlow and filtering rules issue with Telnet. In the future network architecture, VAVE [4] is a source address validation solution by calculate forwarding path with OpenFlow/NOX architecture. The calculation of the forwarding path of VAVE makes use of FlowTable in OpenFlow switch and routing protocols running on an outside controller. But the application of VAVE faces deployment problems in the current network which routers are dominant and many operational routing protocols running inside of a network device.

OpenRouter [2] is an OpenFlow-extended router based on a commercial router, which can not only provide software-defined abilities to introduce some new network features by extending OpenFlow, but also give a tradeoff between existing hardware and evolution cost by software update inside a network device. In this demo, we will demonstrate OpenRouter using a solution of intra-domain source address validation to illustrate that OpenRouter is a feasible and evolvable paradigm for SDN.

II. SYSTEM ARCHITECTURE

The system architecture is composed of an OpenRouter, a NOX [5] which is one of OpenFlow controller and an intra-AS source address validation protocol, named InSAVO protocol app, as shown in Fig. 1.
A. **OpenRouter**

OpenRouter can notify routing change information and sampling packet message by setting up interfaces with Routing Table Management (RTM) and xFlow (sFlow or NetFlow which depends on a vendor implementation). The notification messages are encapsulated with OpenFlow protocol to support standard information transmission and network state information sharing with protocols running inside/outside a router. FlowTable is implemented using existing hardware of ACL&QoS and FIB in OpenRouter to enable software-defined features only updating software image of a router. Network data structure is redesigned and reconstructed with Type-Length-Value (TLV) format to support user-defined combination and extension of header fields and actions of OpenFlow. IP address length and match structure of FlowTable is extended to 128 bits to support IPv6 forwarding rules.

B. **NOX**

NOX can receive and process routing information, interface information and sampling packets from OpenRouter, then distribute information to the InSAVO protocol app. NOX can encapsulate control rules from InSAVO protocol app to FlowTable format and issue them to OpenRouter. Three new modules are implemented to process sampling packet message, network state message and control rule message by means of a message-event pattern in order to improve the efficiency of information process and distribution.

C. **InSAVO Protocol APP**

InSAVO Protocol App can calculate forwarding path and filtering information in filtering generator module according to routing and interface information from OpenRouters in an AS. InSAVO can issue filtering information in the way of active control based on forwarding path and positive control based on the validation of sampling packet according to management requirement.

III. **DEMOSTRATION**

In this demo, we will present both live demo and video demo to illustrate the advantages of OpenRouter. An implementation of OpenRouter using a commercial router (DCRS 5980/5950) will be shown in the conference.

A. **The Topology of Demonstration**

In this live demo, the topology is divided into two parts, as shown in Fig. 2. The network in Tsinghua with 10 OpenRouters is configured to run OSPF protocol as an AS. NOX and InSAVO are running on two servers respectively. Packet generator is used for generating spoofing packets to the server A. Video server is used for generating video traffic to show bandwidth change intuitively caused by spoofing packets. The network in the conference with 2 laptops is used to show video client and InSAVO user interface.

B. **Two Scenes of Demonstration**

1) **Source Address Validation:** Packet generator generates IP spoofing packets to server A. The quality of video in video client is declined. After turning on the function of InSAVO, the quality of video in video client is recovered. In the user interface of InSAVO, the OpenRouter connected with packet generator is marked as red color. This scene shows InSAVO works well with OpenFlow in place of SNMP/xFlow/Telnet.

2) **Forwarding Path Re-Calculation:** When the link between the two OpenRouters is down, the message of link down notification can be sent to NOX by OpenRouter as soon as possible. The user interface of InSAVO can show the change of network topology and re-calculate forwarding path and filtering information. This scene shows InSAVO can response quickly to network state change with OpenRouter.

ACKNOWLEDGMENT

This work is supported by National Science Foundation of China under Grant 61073172, Program for New Century Excellent Talents in University, Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 200800030034.

REFERENCES


