Demonstration of OpenFlow-Controlled Cooperative Resource Allocation in a Multi-Domain SD-EON Testbed across Multiple Nations

Cen Chen(1), Shoujiang Ma(1), Xiaoliang Chen(1), Zuqing Zhu(1)*, Lei Liu(2), Xiaotao Feng(2), S. J. B. Yoo(2)

(1) University of Science and Technology of China, Hefei, Anhui 230027, China. *Email: zqzhu@ieee.org
(2) University of California, Davis, Davis, CA 95616, USA. Email: sbyoo@ucdavis.edu

Abstract *We propose an inter-domain protocol (IDP) that enables cooperative resource allocation for secure and impairment-aware lightpath provisioning across multiple domains. The proposed IDP is implemented and experimentally demonstrated in a China-USA multi-domain control-plane SD-EON testbed.*

Introduction

Flexible-grid elastic optical networks (EONs) improve spectral efficiency and bring intelligence into the optical layer. When coupling with software-defined networking (SDN), they function as software-defined EONs (SD-EONs) that provide service providers the flexibility to customize their infrastructure dynamically according to application requirements. Previously, people have reported several interesting network control schemes in OpenFlow (OF) controlled SD-EONs [1,2]. With the developments of SD-EONs, there will be an increasing demand to facilitate lightpath provisioning across multiple domains to extend service reach. In line of this, previous studies have demonstrated a few network orchestration schemes for multi-domain SD-EONs [3,4]. As utilizing spectrum resources efficiently in multi-domain SD-EONs is essential for agile network orchestration, it is desired that we enable cooperative routing and spectrum assignment (RSA) for intelligent multi-domain lightpath provisioning. However, to the best of our knowledge, the protocol design and experimental study on this topic have not been fully explored yet.

In this paper, with an OF-controlled SD-EON framework, we propose an inter-domain protocol (IDP) that enables multi-domain RSA for secure and impairment-aware lightpath provisioning. Specifically, we design the IDP to let the OF controllers (OF-Cs) of different domains determine a lightpath's RSA cooperatively with considerations of both the transparent (*i.e.*, the lightpath going through domains all-optically) and the translucent (*i.e.*, the lightpath experiencing optical-to-electrical-to-optical (O/E/O) conversions in between domains) options. Moreover, as the proposed IDP does not disclose each domain's spectrum usage information completely, enhanced security is achieved to protect SD-EONs against cross-domain physical-layer attacks. The proposed IDP is implemented and experimentally demonstrated in a multi-nation control-plane SD-EON testbed that consists of two geographically-distributed domains located in China and USA.

Operation Principle

Fig. 1(a) shows the detailed procedure of the inter-domain protocol (IDP) to provision a lightpath across multiple SD-EON domains. The control plane of each domain consists of one controller (OF-C) and a few OF agents (OF-AGs). The OF-AGs are used to configure the bandwidth-variable wavelength-selective switches (BV-WSS') in the data plane according to the flow-entries from its OF-C. Each flow-entry contains a lightpath's configuration on the corresponding BV-WSS, including the input and output ports, starting frequency of the occupied block of frequency slots (FS') , number of FS' and *etc*. Each OF-AG talks with its OF-C using the extended OF protocol demonstrated in [2], while the OF-Cs communicate with each other for settling a multi-domain lightpath's RSA with our proposed IDP.

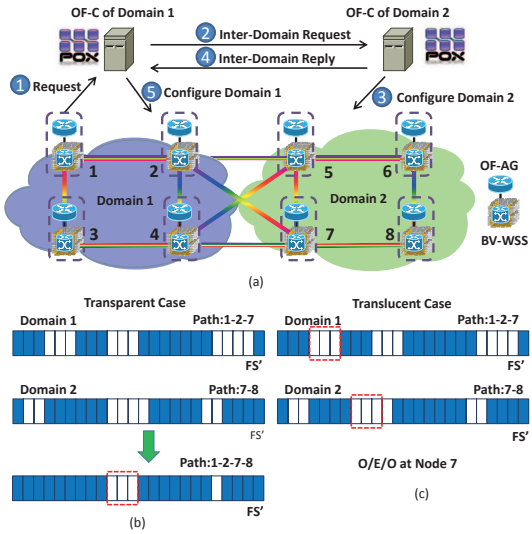

Fig. 1: Multi-domain lightpath provisioning, (a) network architecture and detailed procedure, and examples of (b) transparent and (c) translucent multi-domain RSA schemes.

A multi-domain lightpath can be denoted as $LR(s,d,B,\Delta t)$, where s and d are the source and destination nodes, respectively, B is its bandwidth requirement in Gb/s, and Δt is the holding time. Then, in order to provision an LR from *Domain* 1 to *Domain* 2, we have (note that the OF-C in *Domain* x is referred as OF-C-x, *e.g.*, OF-C-1 is for the OF-C in *Domain* 1),

Step 1: When $LR(s,d,B,\Delta t)$ comes in *Domain* 1, the OF-AG on s builds a *Packet-In* message and sends it to OF-C-1. OF-C-1 finds that LR is for multi-domain, and performs RSA calculation. Here, we assume that OF-C can get the "destination domain" where d of a multi-domain LR locates by checking a local routing table.

Step 2: OF-C-1 computes the shortest paths that each

is from s to an approachable ingress node of the destination domain (*e.g.*, *Node* 5 in *Domain* 2), gets the spectrum usages on them, and randomly selects a few available FS-blocks that each is large enough to accommodate B. The paths and the selected FS-blocks on them are treated as the RSA candidates in *Domain* 1, which are encoded in an *Inter_Domain_Request* message and sent to OF-C-2.

Step 3: For each RSA candidate in *Domain* 1, OF-C-2 calculates the shortest path from the encoded ingress node to d, and gets the usable FS-blocks on it, as the RSA candidates in *Domain* 2. After processing all the candidates in *Domain* 1, OF-C-2 tries to merge the two domains' RSA candidates and checks whether LR can be setup all-optically end-to-end. Basically, it checks 1) whether the merged end-to-end path satisfies the quality-of-transmission (QoT) requirement, and 2) whether there is a common available FS-block that can accommodate B. If LR can be set up all-optically, OF-C-2 finalizes LR's end-to-end RSA. Otherwise, OF-C-2 turns to the translucent option, randomly selects an RSA candidate in *Domain* 1, and calculates LR's RSA within *Domain* 2 by assuming that an O/E/O conversion will be performed at the corresponding ingress node. Then, after finalizing the end-to-end RSA, OF-C-2 instructs the related OF-AGs to assemble LR's portion in *Domain* 2, which is done by distributing the corresponding flow-entries with the *Flow_Mod* messages.

Step 4: OF-C-2 encodes the finalized RSA within *Domain* 1 in an *Inter_Domian_Reply* message and sends it to OF-C-1. The message contains all the necessary information for assembling LR's portion in *Domain* 1, including the RSA and the modulation format.

Step 5: OF-C-1 receives the *Inter_Domain_Reply* message, and instructs the related OF-AGs to assemble LR's portion in *Domain* 1 accordingly. Then, LR is provisioned successfully.

Note that if any of the aforementioned steps fails due to insufficient resources, LR will be blocked. In **Steps 2-3**, we protect the privacy of each domain by using the approach that randomly selects intra-domain RSA candidates to tell the peer-domains. Basically, we try to avoid disclosing all the intra-domain spectrum usage information to other domains, as a malicious user can use it to launch physical-layer attacks. Figs. 1(b) and 1(c) show the examples of LR's end-to-end RSAs for the transparent and translucent schemes, respectively.

The detailed structures of the *Inter_Domain_Request* and *Inter_Domain_Reply* messages are shown in Fig. 2. In Fig. 2(a), the first three fields of *Inter_Domain_ Request* are for LR's basic information, while the rest ones encode the RSA candidates in the source domain. The field structure of each RSA candidate is also shown in Fig. 2(a), where the first sub-field stores the ingress node in the destination domain, the second one is for the length of the path from s to that ingress node, and the rest ones are for the selected usable FS-blocks on that path. Note that in this work, we adopt impairment-aware modulation selection for lightpaths. Specifically, with B as the bandwidth requirement, the number of FS' we need to assign is $n = \lceil \frac{B}{m \cdot C_{grid}^{BPSK}} \rceil$, where C_{grid}^{BPSK} is the capacity that a 12.5-GHz FS provides with BPSK, and m is the modulation-level, where $m = 1, 2, 3$ and 4 represents BPSK, QPSK, 8-QAM and 16-QAM, respectively. We assume that $C_{grid}^{BPSK} = 12.5$ Gb/s and each modulation-level can support a maximum transmission reach based on the network status. Therefore, when selecting the usable FS-blocks for an RSA candidate in the source domain, we consider the worst case, assume that BPSK is used, and ensure that the size of each FS-block is larger than $n = \lceil \frac{B}{C_{grid}^{BPSK}} \rceil$ FS'. While LR's actual modulation-level in the source domain is determined by the destination domain based on the all-optical transmission reach (*i.e.*, the end-to-end path length in the transparent scheme, and the path length from s to the ingress node in the translucent one).

In Fig. 2(b), the first field of *Inter_Domain_Reply* indicates whether a valid RSA can be found in the destination domain, the second one is the ID of the RSA candidate in *Inter_Domain_Request* that the destination domain selects, and the rest ones are for the information of LR's RSA in the source domain. With this design, the source domain does not know whether LR is established transparently or translucently across the domains. It only knows the RSA and modulation-format from s to the destination domain's ingress node, while how LR is handled after that node is hidden from it.

Examples on Wireshark captures for the *Inter_ Domain_Request* and *Inter_Domain_Reply* messages in our experiments are shown in Figs. 3 and 4, where we observe that OF-C-1 suggests 4 RSA candidates in *Inter_Domain_Request*, while *Inter_Domain_Reply* indicates that OF-C-2 finally selects the first candidate and determines the modulation format as BPSK.

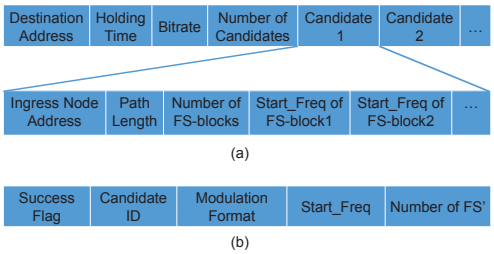

Fig. 2: Messages defined for the inter-domain protocol (IDP), (a) *Inter_Domain_Request*, and (b) *Inter_Domain_Reply*.

Experimental Setup and Results

In our implementation, each OF-AG is realized with Open-vSwitch running on a high-performance Linux server, and each OF-C is implemented based on the POX platform. Within each SD-EON domain, the OF-C connects to all the OF-AGs directly. We then perform experiments on OF-controlled cooperative resource allocation in the multi-domain SD-EON control plane testbed shown in Fig. 5. The testbed consists of two domains, and they are located in the University of Sci-

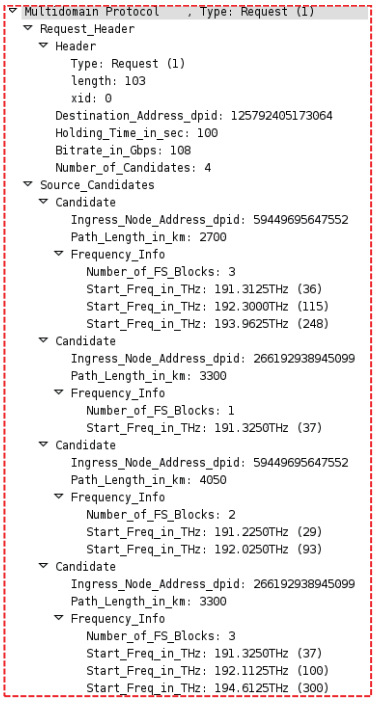

Fig. 3: Wireshark capture of an *Inter-Domain-Request* message.

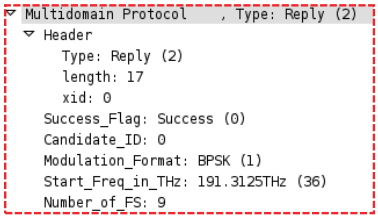

Fig. 4: Wireshark capture of an *Inter-Domain-Reply* message.

ence and Technology of China (USTC Domain) and the University of California, Davis (UCD Domain), respectively. Each domain includes 7 OF-AGs and there are 4 inter-domain links. The OF-Cs in the two domains communicates with each other through the Internet with the proposed IDP to facilitate the cooperative RSA. We assume that each fiber link in the data-plane accommodates 358 FS'. On each of the 14 OF-AGs in the setup, lightpath requests are generated according to the Poisson traffic model with the destination addresses randomly selected. The bandwidth requirement of each request is uniformly distributed within [25, 500] Gb/s.

The Wireshark captures for messages used to provision a LR across the two domains are shown in Fig. 6, where the subplots in Figs. 6(a) and 6(b) are obtained in the USTC and UCD domains, respectively. We observe that it takes the two OF-Cs $\sim$272 msec to exchange the IDP messages, while the total latency for setting the multi-domain lightpath up is $\sim$520 msec. The experiments also measure the requests' blocking probability in the multi-domain SD-EON and the results are plotted in Fig. 7. Note that in order to obtain each data point in Fig. 7, the OF-Cs serve 4000 lightpath requests from the OF-AGs in the two domains.

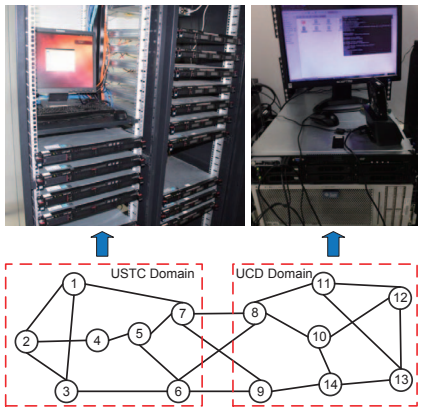

Fig. 5: Experimental Setup.

Time	Source	Destination	Protocol	Length	Info
12.112979	192.168.102.216	192.168.102.205	OF-Extension	196	50201 > 6655 [Type:PacketIn]
12.359287	192.168.102.205	169.237.74.17	Multidomain	169	35518 > 2334 [Type:Request]
12.631108	169.237.74.17	192.168.102.205	Multidomain	83	33797 > 2334 [Type:Reply]
12.631835	192.168.102.205	192.168.102.217	OF-Extension	162	6655 > 48678 [Type:FlowMod]
12.632043	192.168.102.205	192.168.102.217	OF-Extension	74	6655 > 48678 [Type:Barrier_Request]
12.632180	192.168.102.205	192.168.102.216	OF-Extension	178	6655 > 50201 [Type:FlowMod]
12.632353	192.168.102.205	192.168.102.216	OF-Extension	74	6655 > 50201 [Type:Barrier_Request]
12.632409	192.168.102.217	192.168.102.205	OF-Extension	74	48678 > 6655 [Type:Barrier_Reply]
12.632742	192.168.102.216	192.168.102.205	OF-Extension	74	50201 > 6655 [Type:Barrier_Reply]

(a)

Time	Source	Destination	Protocol	Length	Info
4.979523	222.195.92.10	169.237.74.17	Multidomain	169	35518 > 2334 [Type:Request]
4.983435	169.237.74.17	169.237.74.247	OF-Extension	162	6655 > 39165 [Type:FlowMod]
4.983770	169.237.74.17	169.237.74.246	OF-Extension	162	6655 > 33674 [Type:FlowMod]
4.983837	169.237.74.17	169.237.74.247	OF-Extension	74	6655 > 39165 [Type:Barrier_Request]
4.984082	169.237.74.17	169.237.74.246	OF-Extension	74	6655 > 33674 [Type:Barrier_Request]
4.984093	169.237.74.247	169.237.74.17	OF-Extension	74	39165 > 6655 [Type:Barrier_Reply]
4.984122	169.237.74.17	222.195.92.10	Multidomain	83	33797 > 2334 [Type:Reply]
4.984294	169.237.74.246	169.237.74.17	OF-Extension	74	33674 > 6655 [Type:Barrier_Reply]

(b)

Fig. 6: Messages captured by Wireshark in (a) USTC domain and (b) UCD domain for setting up a multi-domain lightpath.

Conclusions

We proposed and demonstrated an inter-domain protocol (IDP) to enable secure and impairment-aware lightpath provisioning in multi-domain SD-EONs.

Acknowledgments

This work was supported in part by the Projects NCET-11-0884, NSFC 61371117, WK2100060010, and the Strategic Priority Research Program of CAS (XDA06010302).

References

[1] R. Casellas et al., "Control and management of flexi-grid optical networks with an integrated stateful PCE and OpenFlow controller," J. Opt. Commun. Netw., Vol. **5**, p. A57 (2013).
[2] S. Ma et al., "Demonstration of Online Spectrum Defragmentation Enabled by OpenFlow in Software-Defined Elastic Optical Networks," Proc. OFC'14, W4A.2, San Francisco (2014).
[3] Y. Yoshida et al., "First international SDN-based network orchestration of variable-capacity OPS over programmable flexi-grid EON," Proc. OFC'14, Th5A.2, San Francisco (2014).
[4] Y. Yu et al., "Field demonstration of DC resource migration via multi-domain software defined transport networks with multi-controller collaboration," Proc. OFC'14, W1E.2, San Francisco (2014).

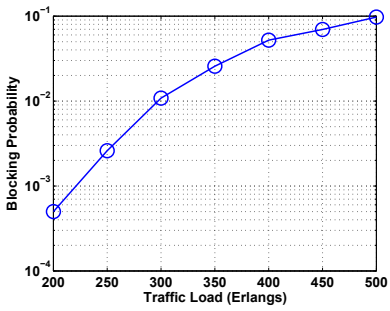

Fig. 7: Experimental results on blocking probability.