Control Plane Robustness in Software-Defined Optical Networks under Targeted Fiber Cuts

Jing Zhu*,†, Carlos Natalino†, Lena Wosinska†, Marija Furdek†, Zuqing Zhu*
*School of Information Science and Technology, University of Science and Technology of China, Hefei, China
†Optical Networks Laboratory (ONLab), KTH Royal Institute of Technology, Sweden
*Email: zhujinng@mail.ustc.edu.cn, {carlosns, wosinska, marifur}@kth.se, zqzhu@ieee.org

***Abstract*—The Software-Defined Optical Networking (SDON) paradigm enables programmable, adaptive and application-aware backbone networks. However, aside from the manifold advantages, the centralized Network Control and Management in SDONs also gives rise to a number of security concerns at different network layers. As communication between the control and the data plane devices in an SDON utilizes the common optical fiber infrastructure, it can be subject of various targeted attacks aimed at disabling the underlying optical network infrastructure and disrupting the services running in the network.**

In this work, we focus on the threats from targeted fiber cuts to the control plane (CP) robustness in an SDON under different link cut attack scenarios with diverse damaging potential, modeled through a newly defined link criticality measure based on the routing of control paths. To quantify the robustness of a particular CP realization, we propose a metric called Average Control Plane Connectivity (ACPC) and analyze the CP robustness for a varying number of controller instances in master/slave configuration. Simulation results indicate that CP enhancements in terms of controller addition do not necessarily yield linear improvements in CP robustness but require tailored CP design strategies.

***Index Terms*—Control plane robustness, Physical-layer security, Software-defined optical networks, Targeted fiber cuts.**

I. Introduction

Optical backbone networks are the critical communication infrastructure supporting a variety of vital network services. In order to enable programmable, scalable and flexible network control and management (NC&M), Software-Defined Networking (SDN) has been proposed to decouple the network control and data planes (CP and DP), such that the NC&M tasks are handled by logically centralized controllers while the DP devices only take care of packet forwarding/data transmission [1, 2]. Hence, implementing Software-Defined Optical Networks (SDONs) enables flexible and programmable optical backbone networks, and significantly shortens the time-to-market of new services [3, 4]. Similar to its packet-based counterparts, the CP of an SDON uses centralized controllers to collect the statuses and configure the operation of DP devices (*e.g.*, optical transponders and switches) [5].

One of the essential aspects in SDON planning is the CP design [6]. As each fiber link in an SDON can carry Tb/s traffic, a well-designed CP should be able to simultaneously satisfy the requirements on low communication latency and high reliability of the control channels [7]. In general, the CP comprises one or multiple controller instances and each of them controls a subset of DP devices. Each DP device can connect to multiple controller instances, typically two, with one serving as master and the other as slave (Fig. 1). Several studies have addressed resilient SDN control plane design [6, 8–11]. Nevertheless, all these studies only considered CP disruptions due to random failures, whereas the failure scenarios due to deliberate attacks are not yet addressed.

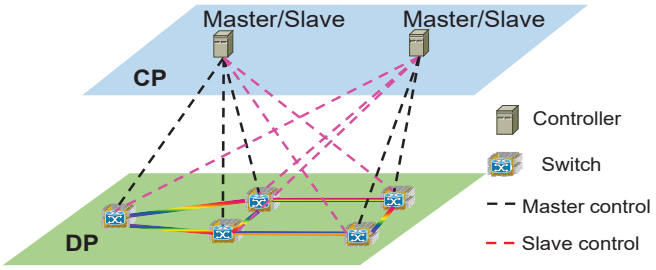


Fig. 1. Example of an SDON

Optical networks are subject to physical-layer vulnerabilities which can be leveraged by malicious users to launch attacks aimed at service disruption [12]. In SDON, such attacks can affect not only the data plane communication, but may seriously disrupt the control plane as well. The damaging potential of attacks can be boosted by design of attack techniques, e.g., by targeting the most critical components. In particular, we focus on deliberate fiber cut attacks where an attacker cuts the most critical links in an effort to maximize the communication disruption. Targeted fiber cuts have a larger disruptive effect than random failures [13], and are more challenging to address through careful network design. As the network 'brain', the robustness of the control plane is an important prerequisite for robust SDON deployment.

In our previous work [14], we have investigated the robustness of data plane communication to targeted link cuts. In this paper, we consider the threats from targeted fiber cuts to the control plane and evaluate the CP robustness in an SDON from the perspectives of connectivity and transmission distance. Our evaluation is based on two newly proposed metrics: *(i)* a link criticality measure that quantifies the importance of links to support the CP connections and *(ii)* the Average Control Plane Connectivity (ACPC) that evaluates the robustness of a specific CP realization (*i.e.*, the controller placement and the routing of control channels over the optical fiber topology. We consider

two attack scenarios: one, where the attacker is not aware of the CP realization and, thus, uses general knowledge of the topology to select the targeted links to cut; and the other, where the attacker is aware of the CP realization and, thus, selects the most critical fibers to cut. Extensive simulation experiments are conducted for three realistic backbone topologies, where we analyze the CP robustness depending on the number of controller instances in the network and assess whether adding master/slave controller configuration to the switches can enhance the CP robustness. Results show that adding controller instances or considering master/slave configuration might not always lead to an increase in CP robustness, especially when the knowledge of the CP realization is available to the attacker.

The remainder of the paper is organized as follows. Section II reviews the related work. The proposed control plane connectivity measures are presented in Section III. Sections V and IV analyze network performance in the two considered attack scenarios, while Section VI provides concluding remarks.

II. Related Work

Since the inception of SDN, there have been intensive efforts on control plane design. The fundamental problem of CP design, *i.e.*, how many controllers to deploy and where to place them, has been addressed in [15]. A comprehensive survey on fault management in SDN can be found in [16]. Control plane resiliency was investigated under various failure scenarios in [6, 8–11]. In [8], the authors proposed a method for controller placement aimed at maximizing the number of protected SDN switches. The work in [9] compared several controller placement schemes in terms of CP connectivity. The study in [10] considered failures of fiber links, switches and controllers, and designed an algorithm for Pareto-optimal controller placement with load balancing. Resilience from cascading controller failures was addressed in [11], by designing several algorithms to balance and redistribute the load among controllers. In [6], a survivable CP establishment scheme was proposed to protect SDONs against single node failures, utilizing a mutual backup model for the controllers. However, these studies did not consider failure scenarios caused by malicious man-made attacks.

In addition to CP, people have also considered the availability of the DP of SDONs with the assumption of random fiber failures [17–20], and addressed how to mitigate physical-layer attacks in DP in various optical networks [21–23]. Robustness of large-scale network topologies in the presence of targeted attacks was evaluated in [24]. Santos *et al.* [25] investigated the identification of critical nodes in a telecommunication network, *i.e.*, nodes whose removal would minimize the network connectivity. The work in [14] studied the robustness of optical content delivery networks in the presence of targeted fiber cuts, gauged by average content accessibility. As the aforementioned investigations only addressed survivability issues concerning the data plane, they cannot be directly mapped to assess the control plane robustness in SDONs. Attacks aimed at disabling control plane elements were investigated in [26], where the authors proposed a cost-efficient controller assignment algorithm to protect an SDN with multiple controllers from Byzantine attacks targeting controllers and control channels. They assumed that the attacker has complete knowledge about the CP realization, *i.e.*, the controller location and connectivity. The assumption of complete CP realization knowledge might not always be applicable because network operators typically try to prevent disclosing operational details. In this paper, we consider both cases, *i.e.*, the scenario where the attacker is aware only of the network topology, and the case where the attacker is also aware of the CP realization.

III. Control Plane Connectivity Measures

We consider a backbone SDON with topology modeled as a graph $G(V, E)$, where V denotes the set of nodes hosting switching elements, and E the set of undirected fiber links. We assume that the CP and DP of the SDON are supported by the same physical infrastructure, which means that the controllers are co-located with the optical switches, while the control channels share fiber links with data plane connections (*i.e.*, in-band control). There are $|U|$ controller instances in the SDON, and the set U ($U \subset V$) represents their locations. To realize CP resiliency, each controller manages several optical switches, and each switch may connect to one or two controller instances, *i.e.*, one master and one slave [7]. To reduce the control latency, each optical switch is assumed to connect to the physically closest controller instances.

In a targeted fiber link cut attack, the attacker deliberately chooses certain fiber links to cut according to some attacking priorities, and the extent of the attack can be quantified with a ratio of cut links. If the set of intact fiber links upon an attack is denoted with E', the cut ratio can be expressed as:

$$r = \frac{|E| - |E'|}{|E|}. \tag{1}$$

Note that the targeted fiber cuts can disrupt the connectivity between switches and controllers, among the switches, and among the controllers. We focus on the case where the connectivity between switches and controllers is disrupted, which affects CP robustness in the SDON, *i.e.*, the survivability of the control channels [6]. Here, we assume that the connectivity between a switch and its controller is lost if no path exists between them in $G(V, E')$ after the attack.

The following notations are used throughout the paper to assist CP robustness evaluation in SDONs.

- $x_{u,v}$: boolean variable that equals 1 if the optical switch at node v connects to the controller at node u, and 0 otherwise.
- $P_{u,v}$: the shortest path between the controller at node u and the optical switch at node v before the attack.
- $z_{u,v,e}$: boolean variable that equals 1 if link e is traversed by $P_{u,v}$, and 0 otherwise.
- $y_{u,v,r}$: boolean variable that equals 0 if, after an attack with cut ratio r, the connectivity between the optical switch at node v and the controller at node u is lost, and 1 otherwise.

- $P_{u,v,r}$: the shortest path between the controller at node u and the optical switch at node v after an attack with cut ratio r.
- $d_{u,v,r}$: the transmission distance of path $P_{u,v,r}$.

Using these notations, we define three metrics to measure link criticality with respect to the control plane, and to evaluate the CP robustness after an attack with cut ratio r.

1) Link Criticality (L_c)

If the attacker is aware of the CP realization, the cut fiber links can be selected according to their importance to the CP. In this case, the attacker can target the most critical fiber links in an effort to maximize effectiveness of the attack. So far, there are no metrics that define the criticality of a link based on its importance to the CP. Therefore, we define link criticality L_c metric to quantify the importance of each link in the network based on the traversing control channels. The links that carry the largest numbers of control channels are considered to be the most critical. Formally, the metric is defined as:

$$L_c(e) = \sum_{u \in U, v \in V} x_{u,v} \cdot z_{u,v,e}. \tag{2}$$

2) Average Control Plane Connectivity (ACPC)

The ACPC quantifies the portion of network switches that can still connect to any of their controller instances (master or slave) after an attack. Formally, the ACPC after an attack with cut ratio r can be calculated as:

$$ACPC(r) = \frac{\sum_{u \in U, v \in V} x_{u,v} \cdot y_{u,v,r}}{|V|}. \tag{3}$$

3) Average Transmission Distance (ATD)

Besides connectivity, the latency of control channels is also a critical enabler of the efficient operation of an SDON. In optical networks, a significant portion of latency is related to the propagation of the optical signal in the fiber. Hence, transmission distance is a major factor for the latency. We define the ATD as:

$$ATD(r) = \frac{\sum_{u \in U, v \in V} d_{u,v,r} \cdot x_{u,v} \cdot y_{u,v,r}}{|V|}. \tag{4}$$

Note that ATD is computed only for working control paths, *i.e.*, those disrupted by the attack are not taken into account.

TABLE I
TOPOLOGY CHARACTERISTICS

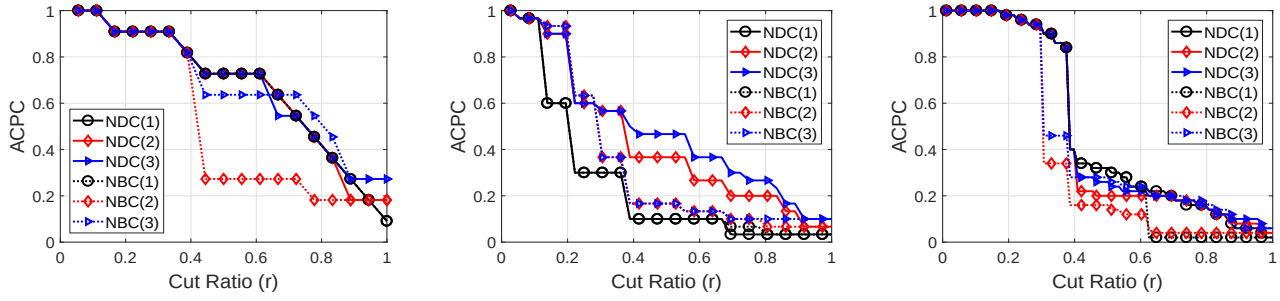
Topology	Nodes	Links	Degree (± Deviation)	Diameter (hops)
Sprint [29]	11	18	3.27 (± 1.42)	4
USNET [30]	30	36	2.4 (± 0.6)	11
Germany [31]	50	88	3.5 (± 1.04)	9

IV. ATTACK SCENARIO WITH NO CP REALIZATION KNOWLEDGE

Our simulation experiments are carried out using a custom-built Java-based tool that leverages GraphStream [27] for graph manipulation. We consider three realistic topologies whose characteristics are summarized in Table I. We consider two controller placement schemes, *i.e.*, the Node Degree Centrality (NDC) and the Node Betweenness Centrality (NBC). The NDC scheme places the controller instances at the nodes with higher nodal degree. The NBC scheme places the controller instances at the nodes with higher node betweenness centrality, which refers to the number of all-node-pairs shortest paths traversing a node [28]. We first analyze how the number of controller instances in an SDON affects the CP robustness in the case where each optical switch only connects to its master controller (*i.e.*, no slave controller is used). Then, we investigate whether considering master/slave controller configuration improves the CP robustness.

This section considers the less sophisticated attack scenario denoted as unavailable knowledge scenario (UKS) where the attacker has the knowledge of the physical network topology ($G(V, E)$), but does not know the details of the CP realization. According to [28], one effective scheme for selecting the most critical links is utilizing the link betweenness centrality, which is defined as the number of the shortest paths between all node pairs that traverse a specific link. Hence, in UKS, we assume that the attacker aims at maximizing the disruption potential of the attack by targeting the fiber links with higher link betweenness centrality.

Fig. 2 shows the results of ACPC for the UKS with single switch-controller assignment. It means that each switch is statically assigned to one (the closest) controller, and does not connect to any other controller even in the presence of attacks. Here, the curves in each plot correspond to a controller



(a) Sprint (b) USNET (c) Germany

Fig. 2. ACPC in the UKS scenario with single switch-controller assignment.

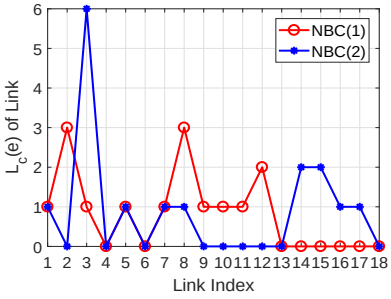


Fig. 3. $L_c(e)$ in Sprint topology with controllers placed according to NBC.

TABLE II
LINKS TO BE CUT WITH $r = 0.5$ IN SPRINT (CP CRITICAL LINKS IN RED)

Scenario	Link Index
UKS(1)	[1, 2, 3, 5, 8, 12, 14, 15, 17]
UKS(2)	[1, 2, 3, 5, 8, 12, 14, 15, 17]

placement scheme with a certain number of controllers, e.g., "NDC(1)" represents the case where the SDON has one controller placed according to the NDC scheme. We observe that for a given number of controllers and a placement scheme, ACPC decreases for higher cut ratio r until it reaches the minimum, where the controller(s) are reachable only by its local optical switch(es) placed at the same node. However, there is a large variation in the impact of link cuts depending on the network topology. For instance, in USNET, when there is one controller, a drastic ACPC decrease occurs at around $r = 0.2$, while for Sprint and Germany the ACPC it does not drop significantly until about $r = 0.4$. The lower connectivity of USNET (as listed in Table I) makes this topology more vulnerable to targeted fiber cuts.

Interestingly, note that **in UKS with statically assigned single switch-controller assignment, a larger number of controllers does not guarantee a higher ACPC, and in some cases, ACPC can degrade with the number of controllers.** For example, in Fig. 2(a), when up to 7 links are cut ($r \leq 0.39$), the ACPC results are the same regardless of the number of controllers for both placement strategies. When we have r within $[0.44, 0.61]$, the ACPC for NBC(1) is higher than that for NBC(2). The same phenomenon can be observed by comparing the ACPC results for NDC(1) and NDC(3) at $r = 0.67$. These situations occur because when a controller is added to the network, the routing of control paths changes significantly. The control channels tend to be distributed more evenly over the links, which makes targeted attacks based on link betweenness centrality more effective.

To verify our analysis above, we collect the results of $L_c(e)$ in Sprint for the scenarios that place 1 and 2 controllers with the NBC scheme, and plot them in Fig. 3. We also list the links that are selected by the link betweenness centrality with $r = 0.5$ in UKS scenarios in Table II. By checking the results in Fig. 3 and Table II, we find that with 1 and 2 controllers, the link betweenness centrality selects 6 and 7 truly critical links for the control plane, respectively. Hence, **placing more controllers in an SDON that assigns single controllers statically might not improve the robustness of the SDON**.

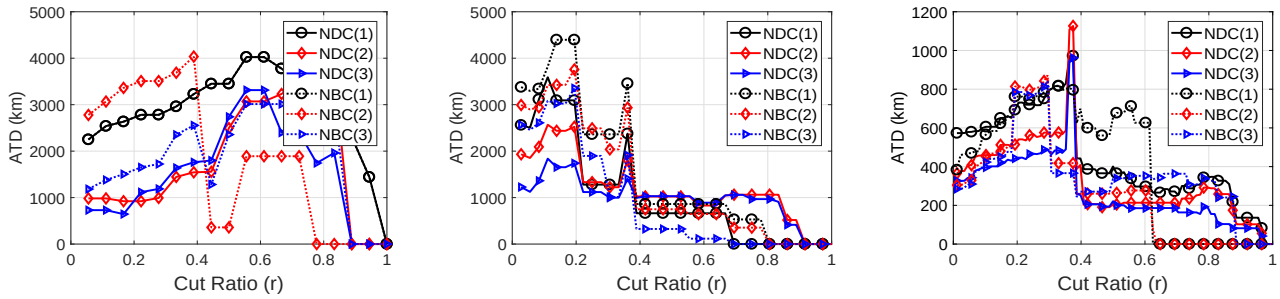
The ATD values for UKS with single switch-controller assignment are plotted in Fig. 4. A general observation is that CP needs to use longer paths as links are cut, leading to an increase in ATD. Recall that only working control paths are accounted. By ignoring the disrupted control paths, it is possible to measure the ATD for the control paths that remain connected. The drops in ATD showed in Fig. 4 are associated with drops in ACPC for the same cut ratio, *i.e.*, cutting links tends to disrupt control path of the farthest switch(es), which leads to a decrease in the ATD for the remaining working control paths. For instance, in Fig. 4(a), when r increases from 0.06 to 0.11, the value of ACPC is 1 although there is an increase in ATD. Nevertheless, when r changes from 0.39 to 0.44, ATD for both NBC(2) and NBC(3) decreases due to a drop in ACPC, which accounts for the fact that the topology is no longer fully connected, and thus the survived control channels can only take relatively shorter paths.

We also analyze whether CP robustness can be improved by considering a master/slave controller configuration for each optical switch. The number of controller instances placed in the network is set to 3, and the master/slave controller configuration is adopted by assigning two controllers to each optical switch. Each controller instance can act as master and slave simultaneously, *i.e.*, it can be the master for some switch(es) and the slave for others. Fig. 5 shows the ACPC for the cases with single or master/slave switch-controller assignment. It can be observed that considering master/slave controller assignment tends to increase the ACPC. However, such benefits are observed at different cut ratios depending on the network topology. These results suggest that **by considering master/slave controller configuration in UKS, the ACPC can be enhanced**. This can be easily understood since in UKS, the importance of links targeted by the attack is independent of the existence of slave controllers.

V. ATTACK SCENARIO WITH FULL CP REALIZATION KNOWLEDGE

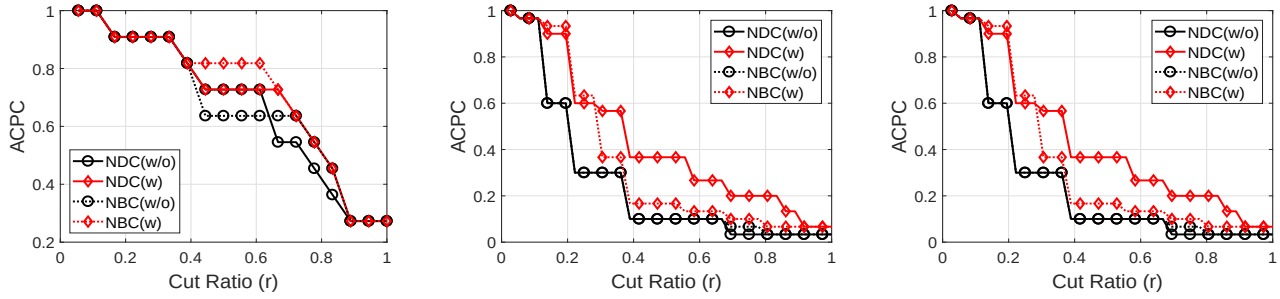
In this section, we analyze the available knowledge scenario (AKS), where we assume that the attacker knows the details of the CP realization and is able to calculate $L_c(e)$. In this way, the attacker can simply choose the $\lfloor r \cdot |E| \rfloor$ links with higher $L_c(e)$ to cut. Apart from the link selection strategy, this experiment follows the same setup as that in Section IV.

Fig. 6 shows the obtained ACPC for AKS with statically assigned single controller. In AKS, the general trend of ACPC with respect to r is similar to that of the UKS scenario. When comparing the curves for different number of controllers, we can see that **adding more controllers does not always improve the ACPC**. However, gains can be observed in most cases. For instance, for Sprint and USNET, higher gains are observed when moving from 1 to 2 controller instances. Further addition of controllers still provides gains, but less pronounced. For example, the results in Fig. 6(a) indicate that for $r = 0.17$ and the NBC placement scheme, the ACPC decreases when the number of controllers increases from 2 to 3 (compare the curves of NBC(2) and NBC(3)). Moreover,



(a) Sprint (b) USNET (c) Germany

Fig. 4. ATD for UKS with single switch-controller assignment.



(a) Sprint (b) USNET (c) Germany

Fig. 5. Comparison of the ACPC for UKS with single and master/slave switch-controller assignment (3 controllers in the SDON).

in Fig. 6(a), the ACPC obtained for NBC(2) and NBC(3) is the same when r changes within $[0.22, 0.39]$, while for $r = 0.5$, the ACPC for NBC(2) is higher than that of NBC(3). This phenomenon can be explained as follows. When more controllers are placed in the SDON, the control channels of switches to different controllers may traverse the same links. Hence, when these links are cut, the control channels can be interrupted. In Fig. 6, we observe that this phenomenon occurs more frequently in Sprint and Germany than in USNET. This is because they have larger deviations on nodal degree, which makes link sharing among control channels more common.

The ATD for AKS follows similar trends as in the UKS case, and is omitted for conciseness. Fig. 7 shows the ACPC for scenarios with single and master/slave switch-controller assignment when there are 3 controllers in the SDON. The comparison of the cases with single or master/slave controllers indicates that **considering master/slave controller configuration might not improve ACPC if the attacker has the knowledge of the CP realization**. At certain values of r, adding slave controllers can even degrade ACPC. For instance, when r ranges within $[0.06, 0.28]$ in Fig. 7(a), there is no improvement on ACPC for both controller placement schemes after considering a master/slave controller configuration. This can be explained by the fact that considering master/slave controller configuration generates more control channels and in turn makes certain links more vulnerable to targeted fiber cuts by increasing their $L_c(e)$.

VI. Conclusion

This paper considered the threats from targeted fiber cuts and evaluates control plane robustness in SDONs in terms of Average Control Plane Connectivity (ACPC) and Average Transmission Distance (ATD). Two attack scenarios were considered with different extents of control plane realization knowledge available to the attacker, and the impact of the number of controller instances to CP robustness was assessed. Moreover, two controller assignment configurations were considered: single or master/slave switch-controller assignment. For attacks with unknown CP realization and single controller configuration, adding more controllers did not guarantee an increase in ACPC, but adopting master/slave controller configuration benefited the CP robustness. When the attacker had the CP realization details, considering master/slave configuration or adding more controllers did not ensure improved ACPC. The extensive simulation results indicated strong necessity to protect the information related to the CP realization.

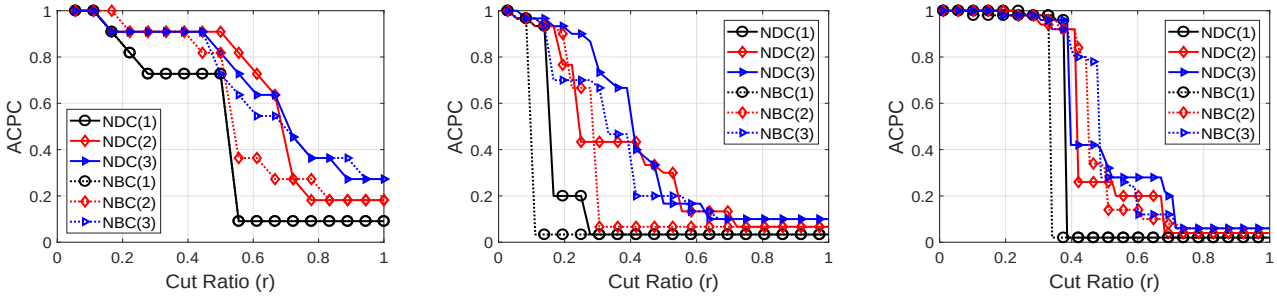
Acknowledgments

This work was supported in part by the NSFC Project 61701472, CAS Key Project (QYZDY-SSW-JSC003), NGBWMCN Key Project (2017ZX03001019-004), China Postdoctoral Science Foundation (2016M602031), and Fundamental Research Funds for the Central Universities (WK2100060021).

C. Natalino, L. Wosinska and M. Furdek are supported in part by the RESyST project funded by the Unity through Knowledge Fund of the Croatian Ministry of Science, and the COST Action 15127 RECODIS.

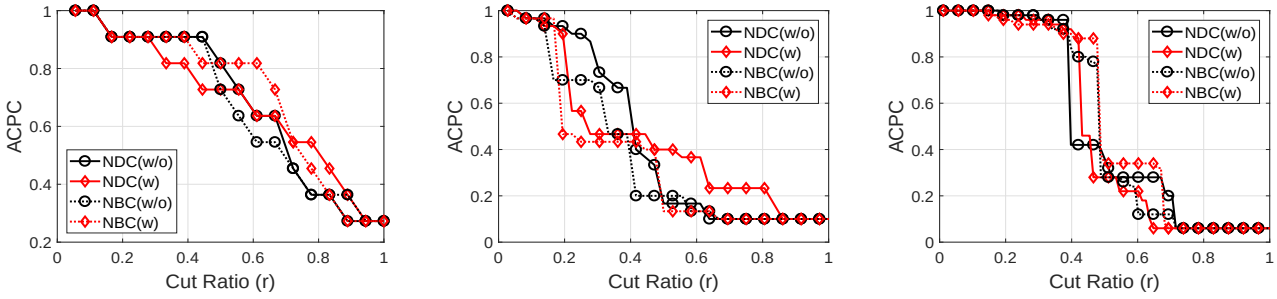
References

[1] D. Kreutz *et al.*, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, pp. 14–76, Jan. 2015.



(a) Sprint (b) USNET (c) Germany

Fig. 6. Results on ACPC for AKS with single switch-controller assignment.



(a) Sprint (b) USNET (c) Germany

Fig. 7. ACPC for the AKS scenario with single and master/slave switch-controller assignment (3 controllers in the SDON).

[2] S. Li *et al.*, "Protocol oblivious forwarding (POF): Software-defined networking with enhanced programmability," *IEEE Netw.*, vol. 31, pp. 12–20, Mar./Apr. 2017.

[3] Z. Zhu *et al.*, "Demonstration of cooperative resource allocation in an OpenFlow-controlled multidomain and multinational SD-EON testbed," *J. Lightw. Technol.*, vol. 33, pp. 1508–1514, Apr. 2015.

[4] C. Chen *et al.*, "Demonstrations of efficient online spectrum defragmentation in software-defined elastic optical networks," *J. Lightw. Technol.*, vol. 32, pp. 4701–4711, Dec. 2014.

[5] Z. Zhu *et al.*, "OpenFlow-assisted online defragmentation in single-/multi-domain software-defined elastic optical networks," *J. Opt. Commun. Netw.*, vol. 7, pp. A7–A15, Jan. 2015.

[6] B. Zhao, X. Chen, J. Zhu, and Z. Zhu, "Survivable control plane establishment with live control service backup and migration in SD-EONs," *J. Opt. Commun. Netw.*, vol. 8, pp. 371–381, Jun. 2016.

[7] X. Chen *et al.*, "Leveraging master-slave openflow controller arrangement to improve control plane resiliency in SD-EONs," *Opt. Express*, vol. 23, pp. 7550–7558, Mar. 2015.

[8] N. Beheshti and Y. Zhang, "Fast failover for control traffic in software-defined networks," in *Proc. of GLOBECOM*, pp. 2665–2670, Dec. 2012.

[9] Y. Hu *et al.*, "Reliability-aware controller placement for software-defined networks," in *Proc. of IFIP/IEEE IM*, pp. 672–675, May 2013.

[10] D. Hock *et al.*, "Pareto-optimal resilient controller placement in SDN-based core networks," in *Proc. of ITC*, pp. 1–9, Sept. 2013.

[11] G. Yao, J. Bi, and L. Guo, "On the cascading failures of multi-controllers in software defined networks," in *Proc. of ICNP*, pp. 1–2, Oct. 2013.

[12] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, pp. 110–117, Aug. 2016.

[13] R. Albert, H. Jeong, and A. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–382, Jul. 2000.

[14] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek, "Content accessibility in optical cloud networks under targeted link cuts," in *Proc. of ONDM*, pp. 1–6, May 2017.

[15] B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," in *Prof. of HotSDN*, pp. 7–12, Aug. 2012.

[16] P. Fonseca and E. Mota, "A survey on fault management in software-defined networks," *IEEE Commun. Surveys Tut.*, vol. 19, pp. 2284–2321, Fourth Quarter 2017.

[17] X. Chen *et al.*, "Availability-aware service provisioning in SD-EON based inter-datacenter networks," *Photon. Netw. Commun.*, vol. 31, pp. 543–549, Jun. 2016.

[18] X. Chen, F. Ji, and Z. Zhu, "Service availability oriented p-cycle protection design in elastic optical networks," *J. Opt. Commun. Netw.*, vol. 6, pp. 901–910, Oct. 2014.

[19] X. Chen *et al.*, "Flexible availability-aware differentiated protection in software-defined elastic optical networks," *J. Lightw. Technol.*, vol. 33, pp. 3872–3882, Sept. 2015.

[20] W. Hou *et al.*, "Novel framework of risk-aware virtual network embedding in optical data center networks," *IEEE Syst. J., in Press*, 2018.

[21] J. Zhu, B. Zhao, and Z. Zhu, "Attack-aware service provisioning to enhance physical-layer security in multi-domain EONs," *J. Lightw. Technol.*, vol. 34, pp. 2645–2655, Jun. 2016.

[22] J. Zhu and Z. Zhu, "Physical-layer security in MCF-based SDM-EONs: Would crosstalk-aware service provisioning be good enough?" *J. Lightw. Technol.*, vol. 35, pp. 4826–4837, Nov. 2017.

[23] J. Zhu, B. Zhao, and Z. Zhu, "Leveraging game theory to achieve efficient attack-aware service provisioning in EONs," *J. Lightw. Technol.*, vol. 35, pp. 1785–1796, May 2017.

[24] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, "Attack robustness and centrality of complex networks," *PLoS ONE*, vol. 8, pp. 1–17, Apr. 2013.

[25] D. Santos, A. Sousa, and P. Monteiro, "Compact models for critical node detection in telecommunication networks," in *Proc. of INOC*, pp. 1–10, Feb. 2017.

[26] H. Li, P. Li, S. Guo, and A. Nayak, "Byzantine-resilient secure software-defined networks with multiple controllers in cloud," *IEEE Trans. Cloud Comput.*, vol. 2, pp. 436–447, Oct. 2014.

[27] Y. Pign, A. Dutot, F. Guinand, and D. Olivier, "Graphstream: A tool for bridging the gap between complex systems and dynamic graphs," in *Proc. of ECCS*, pp. 1–10, Sep. 2007.

[28] D. Rueda, E. Calle, and J. Marzo, "Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements," *J. Netw. Syst. Manag.*, vol. 25, pp. 269–289, Apr. 2017.

[29] S. Knight *et al.*, "The internet topology zoo," *IEEE J. Sel. Areas Commun.*, vol. 29, pp. 1765–1775, Oct. 2011.

[30] J. Simmons, *Optical Network Design and Planning*, 2nd ed. Springer, 2014.

[31] S. Orlowski, M. Pióro, A. Tomaszewski, and R. Wessäly, "Sndlib 1.0: Survivable network design library," in *Proc. of INOC*, pp. 1–11, Apr. 2007.