How to Survive Targeted Fiber Cuts: A Game Theoretic Approach for Resilient SDON Control Plane Design

Jing Zhu, Marija Furdek, Carlos Natalino, Lena Wosinska, Zuqing Zhu

How to Survive Targeted Fiber Cuts: A Game Theoretic Approach for Resilient SDON Control Plane Design*

Jing Zhu[1][0000−0001−8451−9173], Marija Furdek[2][0000−0001−5600−3700], Carlos Natalino[2][0000−0001−7501−5547], Lena Wosinska[2][0000−0001−6704−6554], and Zuqing Zhu[1][0000−0002−4251−788X]

[1] University of Science and Technology of China, Hefei, Anhui 230027, China
zqzhu@ieee.org
[2] Chalmers University of Technology, 412 96, Gothenburg, Sweden
furdek@chalmers.se

Abstract. Software-defined optical networking (SDON) paradigm enables programmable, adaptive and application-aware backbone networks via centralized network control and management. Aside from the manifold advantages, the control plane (CP) of an SDON is exposed to diverse security threats. As the CP usually shares the underlying optical infrastructure with the data plane (DP), an attacker can launch physical-layer attacks to cause severe disruption of the CP.
This paper studies the problem of resilient CP design under targeted fiber cut attacks, whose effectiveness depends on both the CP designer's and the attacker's strategies. Therefore, we model the problem as a non-cooperative game between the designer and the attacker, where the designer tries to set up the CP to minimize the attack effectiveness, while the attacker aims at maximizing the effectiveness by cutting the most critical links. We define the game strategies and utility functions, conduct theoretical analysis to obtain the Nash Equilibrium (NE) as the solution of the game. Extensive simulations confirm the effectiveness of our proposal in improving the CP resilience to targeted fiber cuts.

Keywords: Software-defined optical networks · control plane resilience · targeted fiber cuts · non-cooperative game.

1 Introduction

As the underlying infrastructure of backbone networks, optical networks support diverse vital network services and require efficient network control and management (NC&M) [11]. The widely accepted software-defined networking (SDN)

* This work was supported by the NSFC projects 61871357 and 61701472, CAS key project (QYZDY-SSW-JSC003), and NGBWMCN key project (2017ZX03001019-004). M. Furdek, C. Natalino, and L. Wosinska are supported in part by the COST Action 15127 RECODIS.

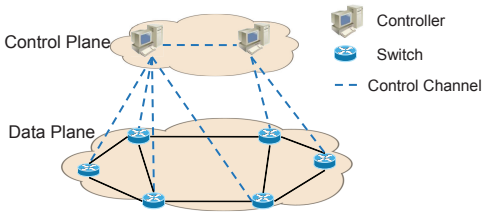


Fig. 1: The data and the control plane of an SDON.

paradigm decouples the network control and the data planes (CP and DP) [12]. In SDN, NC&M is carried out by logically centralized controller(s) in the CP, while the DP devices only need to execute packet forwarding/data transmission tasks. The controller(s) collect the status of DP devices to maintain a global view of the network, and then intelligently instruct the devices to perform corresponding tasks [10]. By implementing SDN in optical networks, software-defined optical networks (SDONs) have the programmability and application-awareness that allow operators to flexibly customize networks and significantly expedite the launch of new services [25, 20, 26].

One of the essential problems in SDON planning is the design of the CP. As shown in Fig. 1, the CP of an SDON is generally composed of one or more controllers, each of which controls a subset of optical devices (e.g., optical transponders and switches) via signalling in control channels. As the traffic in each fiber link can reach Tb/s or even Pb/s, the CP should be well-designed to meet the requirements of low communication latency and high reliability [3]. To this end, previous studies investigated the disruptions due to random failures (e.g., random link cuts), and proposed several CP design schemes [9, 1, 23, 13, 7, 21, 22, 5, 4]. Nevertheless, they overlooked the threats from deliberate attacks disrupting the underlying network infrastructure.

Although logically decoupled, the CP and the DP of a backbone SDON typically share the same fiber infrastructure, which is vulnerable to various physical-layer attacks [19]. Targeted fiber cuts can result in severe disruption of the CP by interrupting communication among CP elements or increasing latency to an unacceptable level. Existing CP design schemes that protect from random failures do not guarantee robustness to targeted cuts. Unlike random cuts which are usually accidental, targeted cuts can be launched with embedded intelligence to boost the efficiency of the attack and aggravate its effects. A common attacker's strategy would be to sever the fiber links which are most critical for network operation. As existing CP design schemes usually use the shortest paths to route the control channels, they may concentrate on links with high betweenness centrality [17], which can be easily identified by attackers as possible targets. Therefore, preparing for the attackers' likely strategies of targeting links when disrupting the CP is paramount for resilient CP design. Hence, the problem can be viewed as a game between two rational entities (i.e., the CP designer and the attacker). To solve it, a game theoretic approach is needed, which, to the best of our knowledge, has not yet been applied for CP design.

In this paper, we consider an SDON under the threat from targeted fiber cuts, and address the problem of robust CP design with a game theoretic approach. We model the problem as a non-cooperative game between the CP designer and the attacker, and define the game strategies and the utility functions for both players. In the game, the designer tries to design the CP such that the damage from targeted fiber cuts is minimal, while the attacker aims at cutting the most critical links to maximize CP disruption. To solve the game, we conduct theoretical analysis to obtain the Nash Equilibrium (NE), which is widely accepted as the solution of a game [16]. Simulation results confirm that under the guidance of the NE, the designer can mitigate the damage from attacks. This verifies the effectiveness of our proposal in increasing resilience of the CP under targeted fiber cuts.

The rest of the paper is organized as follows. Section 2 reviews the related work. The CP design problem as a non-cooperative game is described in Section 3. In Section 4, we analyze the NE to solve the game. Simulations are performed and the results are discussed in Section 5. Finally, Section 6 concludes the paper.

2 Related Work

Extensive efforts have been carried out to improve the performances and availability of the CP. The basic CP design problem of deciding how many controllers to deploy and where to place them has been formulated in [3]. In [9, 1, 23, 13, 7, 21, 22, 5, 4], the authors studied resilient CP design under various failure scenarios, which can be classified into controller failures, switch failures and link failures. To address controller failures, researchers have considered managing each switch by multiple controllers [9, 1, 23, 13, 7]. In [9], the authors applied Byzantine fault tolerant mechanism and studied the assignment of controllers to switches. CP design algorithms with various primary-backup models for controllers have been investigated in [1, 23]. In [13], both Byzantine fault tolerant mechanism and primary-backup model were used when addressing controller-switch mapping. To address switch failures, tree-like CP design that maximizes single-node failure survivability was proposed in [21]. Assuming both switches and links can fail, the work in [22] proposed a controller placement scheme aimed at minimizing the connectivity loss between controllers and switches, while the study in [5] compared different controller placement schemes in terms of CP connectivity. For similar assumptions, the authors of [4] introduced a Pareto-optimal framework for CP design to balance communication latency and resiliency. Nevertheless, none of these studies considered failures caused by deliberate physical-layer attacks.

A relatively straightforward method of attacking the optical infrastructure is disabling the fibers or optical nodes[19]. The impact of such attacks on the DP has been investigated in [8, 18, 15]. The study in [8] evaluated the robustness of large-scale network topologies under targeted attacks. In [18], the authors identified the critical nodes/links in a topology, whose removals would minimize the network connectivity. The work in [15] studied how targeted fiber cuts affect the

robustness of fiber-based content delivery networks. Given the CP, our previous work [24] evaluated the CP robustness under targeted fiber cuts. These investigations suggested that the intelligence of attackers in selecting targets plays an important role, and this motivates us to leverage game theory for CP design. Game theory is a powerful mathematical tool to analyze the competition and cooperation among rational decision-makers, and has been used to solve the problems of network topology design in [14, 2]. In [14], a multi-player game was formulated to assist each node with neighbor selection in order to optimize link establishment price, path delay and proneness to congestion. A dynamic game for network topology design was modeled in [2], where the designer and attacker add and remove links so as to maximize their utilities in terms of considered network properties (e.g., connectivity) and operational costs.

3 Game Model for Control Plane Design

We consider a backbone SDON, whose optical infrastructure carries the mutually disjoint control and data plane. The physical topology is modeled as an undirected graph $G(V, E)$, where V and E represent the sets of nodes and undirected fiber links, respectively. Each node $v \in V$ hosts an optical switch and/or a network controller. The subset of nodes that host controllers is denoted by U, where the number of controllers $|U|$ is given *a priori*. Each edge $e \in E$ denotes a fiber link that can carry data and/or control channels (i.e., in-band control). The set of links that carry control channels is denoted by L. Consequently, U and L constitute the CP topology $G^c(U, L)$. Each controller manages a cluster of switches, while, for simplicity, we assume that each switch is under control of a single controller[3]. As an attacker can launch fiber link cut attacks aimed at disrupting the CP property (e.g., connectivity and communication latency) to the largest extent, a designer needs to design a resilient CP by carefully determining the sets U and L. In general, fiber cuts can disrupt the communication between switches and controllers, among the switches, and among the controllers. Here, we focus only on the communication between switches and controllers. The problem of designing a resilient CP can be viewed as a two-player non-cooperative game between the designer and the attacker as shown in Fig. 2. In the game, the players' strategies and utility functions are as follows.

The finite strategy space of the designer is denoted as $S^d = \{s_1^d, s_2^d, \cdots\}$, where s_i^d refers to a specific CP design strategy of determining U and L. An example strategy s_i^d is to minimize $|L|$, as proposed in [6]. By implementing a strategy s_i^d, the designer obtains a CP solution at the cost D_i, which relates to $|L|$ and can be expressed as:

$$D_i = f_1(|L|). \tag{1}$$

Here, $f_1(\cdot)$ is assumed to be a linear increasing function of $|L|$, as a higher number of links included in the CP would increase both its capital and operational expenses [6]. Meanwhile, the attacker aims at maximizing CP disruption

[3] In more sophisticated scenarios, an optical switch can be assigned to multiple controllers to improve CP resiliency.

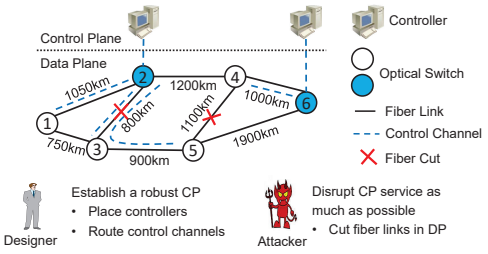


Fig. 2: An example of a non-cooperative game between the network designer and the attacker.

by deliberately cutting n critical links, whose set is denoted as E_c ($|E_c| = n$). The finite strategy space of the attacker is denoted as $S^a = \{s_1^a, s_2^a, \cdots\}$. An example strategy s_j^a is to select links whose removal minimizes the connectivity of $G^c(U, L)$, i.e., maximizes the number of disconnected controller-switch pairs. Each s_j^a corresponds to a cost A_{ij}, which is also related to the designer's strategy s_i^d. For instance, in the simple SDON example shown in Fig. 2 for $|U| = 2$, the designer has established a CP by placing two controllers at nodes 2 and 6, and routing the control channels over the paths marked by the dashed lines. In this case, assuming $n = 1$, the attacker is likely to cut link 2-3.

The cost A_{ij} relates to both n and the geographical distribution of the links in E_c, and can be written as:

$$A_{ij} = f_2(n, \sum_{e_1, e_2 \in E_c} x_{e_1,e_2}), \tag{2}$$

where x_{e_1,e_2} is a boolean variable with value equal to 1 if two links e_1 and e_2 do not share any end-nodes and 0 otherwise. $f_2(\cdot)$ is a linear increasing function of n and x_{e_1,e_2} which ensures that cutting more, and non-adjacent links is more costly. Once the designer and the attacker select s_i^d and s_j^a to take their actions, the SDON is left with a CP affected by n fiber cuts. The CP's property in terms of controller-switch connectivity and communication latency can be described by:

$$P_{ij} = f_3(c(n), l(n)). \tag{3}$$

In Eq. (3), $c(n)$ and $l(n)$ are two CP metrics defined in [24], i.e., the average CP connectivity and the average CP transmission distance after n link cuts, respectively. $f_3(\cdot)$ is a linear function of $c(n)$ and $l(n)$, which decreases with $c(n)$ and increases with $l(n)$. Upon an attack, the attacker obtains a gain of P_{ij} while the designer suffers a loss of P_{ij}. Based on D_i, A_{ij} and P_{ij}, the utility functions F_{ij}^d and F_{ij}^a of the designer and the attacker, respectively, can be calculated as:

$$F_{ij}^d = -\alpha \cdot P_{ij} - D_i, \qquad F_{ij}^a = \beta \cdot P_{ij} - A_{ij}. \tag{4}$$

where α and β are constant coefficients. In the game, both players are rational in choosing strategies to benefit themselves unilaterally, i.e., to maximize their own expected utilities.

Table 1: Game in Strategic Form

	s_1^a	s_2^a	$\cdots$
s_1^d	$(F_{11}^d\ ,\ F_{11}^a)$	$(F_{12}^d\ ,\ F_{12}^a)$	$\cdots$
s_2^d	$(F_{21}^d\ ,\ F_{21}^a)$	$(F_{22}^d\ ,\ F_{22}^a)$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$

Table 1 shows the game in strategic form. For example, when the two players act with strategy profile $(s_2^d,\ s_1^a)$, their utilities would be F_{21}^d and F_{21}^a, respectively. Assuming that s_2^d creates the CP solution shown in Fig. 2 and s_1^a cuts links 2-3 and 4-5, all nodes can still connect to their own controllers, but nodes 3 and 5 have to use longer paths for control channels, resulting in $c(2) = 1$ and $l(2) = 1458$ km. Therefore, we obtain $F_{21}^d = -\alpha \cdot f_3(1, 1458) - f_1(4)$ and $F_{21}^a = \beta \cdot f_3(1, 1458) - f_2(2, 1)$.

4 Nash Equilibrium for Control Plane Design

In the described game, each player tries to find their own best response to their opponent's strategy. Therefore, to obtain the design scheme that leads to a resilient CP, we need to find the strategy profile in which neither the designer nor the attacker can increase their utilities by unilaterally adjusting their own strategies, which is essentially the Nash equilibrium (NE) [16]. In an NE, the designer's strategy is precisely the solution of the CP design problem. As each player in the game has a finite strategy space, the game admits at least one mixed-strategy NE [16]. To obtain it, we formulate the game as optimization problems of the two players, and analyze their best response functions to derive the general form of the NE. Then, we adapt the formulations of the optimization problems to obtain the NE with a simplex-based method.

Notations and Variables:

- $\boldsymbol{\Phi}^d/\boldsymbol{\Phi}^a$: the utility matrix of the designer/attacker.
- ϕ^d/ϕ^a: variable, the expected utility of the designer/attacker.
- $\mathbf{y}^d$: variables, the vector of probability distribution $(y_1^d, y_2^d, \cdots)^T$ to indicate how the designer selects strategies[4], (e.g., y_1^d is the probability that the designer selects strategy s_1^d).
- $\mathbf{y}^a$: variables, the vector of probability distribution $(y_1^a, y_2^a, \cdots)^T$ to indicate how the attacker selects strategies, (e.g., y_1^a is the probability that the attacker selects strategy s_1^a).
- $\mathbf{y}_*^d/\mathbf{y}_*^a$: variables, the best response function of the designer/attacker.
- $\mathbf{z}^d/\mathbf{z}^a$: auxiliary variables, the vector with the form similar to $\mathbf{y}^d/\mathbf{y}^a$.

For the designer, we can formulate the game as the following optimization problem.

[4] The superscript T in $(y_1^d, y_2^d, \cdots)^T$ represents the transposition operator.

Objective:

$$\textit{Maximize} \quad \phi^d = (\mathbf{y}^d)^T \cdot \Phi^d \cdot \mathbf{y}^a. \tag{5}$$

Constraints:

$$\begin{cases} \mathbf{y}^d \geq \mathbf{0}, \quad \mathbf{1}^T \cdot \mathbf{y}^d = 1, \\ \Phi^d \cdot \mathbf{y}^a \leq \mathbf{1} \cdot \phi^d. \end{cases} \tag{6}$$

The designer tries to maximize the objective function in (5) under the constraints in (6). The first two equations in (6) are the nonnegativity and regularity constraints for the probability distribution vector of strategy selection, while the third one ensures that the designer cannot increase their utility by changing the strategy.

Analogously, for the attacker, the game can be formulated as the following optimization problem.

Objective:

$$\textit{Maximize} \quad \phi^a = (\mathbf{y}^d)^T \cdot \Phi^a \cdot \mathbf{y}^a. \tag{7}$$

Constraints:

$$\begin{cases} \mathbf{y}^a \geq \mathbf{0}, \quad \mathbf{1}^T \cdot \mathbf{y}^a = 1, \\ (\Phi^a)^T \cdot \mathbf{y}^d \leq \mathbf{1} \cdot \phi^a. \end{cases} \tag{8}$$

Eqs. (7)-(8) express the attacker's objective function and constraints, respectively.

Using the above formulations, the best response functions of both players can be expressed as:

$$\mathbf{y}^d_*(\mathbf{y}^a) = \arg\max_{\mathbf{y}^d} \left(\phi^d\right), \tag{9}$$

$$\mathbf{y}^a_*(\mathbf{y}^d) = \arg\max_{\mathbf{y}^a} \left(\phi^a\right). \tag{10}$$

Specifically, given that the attacker selects strategies with $\mathbf{y}^a$, the designer uses (9) to obtain the best response $\mathbf{y}^d_*$. Similarly, the attacker leverages (10) to get their best response $\mathbf{y}^a_*$ to designer strategy $\mathbf{y}^d$. Hence, by definition, the NE can be derived as $(\mathbf{y}^d_*, \mathbf{y}^a_*)$, where $\mathbf{y}^d_*$ provides the solution of the CP design problem. In order to find $(\mathbf{y}^d_*, \mathbf{y}^a_*)$, we first adapt the above formulations of optimization problems by introducing $\mathbf{z}^d = \frac{\mathbf{y}^d}{\phi^a}$ and $\mathbf{z}^a = \frac{\mathbf{y}^a}{\phi^d}$.

The designer's optimization problem can be expressed as:

Objective:

$$\textit{Maximize} \quad \phi^d = \frac{1}{\mathbf{1}^T \cdot \mathbf{z}^a}. \tag{11}$$

Constraints:

$$\begin{cases} \mathbf{z}^a \leq \mathbf{0}, \\ \Phi^d \cdot \mathbf{z}^a \geq \mathbf{1}. \end{cases} \tag{12}$$

The attacker's optimization problem is adapted as:

Objective:

$$Maximize \quad \phi^a = \frac{1}{\mathbf{1}^T \cdot \mathbf{z}^d}. \tag{13}$$

Constraints:

$$\begin{cases} \mathbf{z}^d \geq \mathbf{0}, \\ (\Phi^a)^T \cdot \mathbf{z}^d \leq \mathbf{1}. \end{cases} \tag{14}$$

By applying the simplex-based Lemke-Howson algorithm in [16], we solve the problems in (11)-(14) in a coordinated way for $\mathbf{z}^d$ and $\mathbf{z}^a$. Hence, the NE $(\mathbf{y}^d_*, \mathbf{y}^a_*)$ can be obtained as $(\mathbf{z}^d \cdot \frac{1}{\mathbf{1}^T \mathbf{z}^d}, \mathbf{z}^a \cdot \frac{1}{\mathbf{1}^T \mathbf{z}^a})$, where $\mathbf{y}^d_* = \mathbf{z}^d \cdot \frac{1}{\mathbf{1}^T \mathbf{z}^d}$ provides the solution of the CP design problem. The complexity of the algorithm is at most $O(M \cdot N)$, where M and N are the respective numbers of vertices of the polytopes defined by (12) and (14).

5 Simulation Results

In order to validate the proposed game theoretic approach for resilient CP design, we perform simulations on the SprintNET shown in Fig. 3 [24]. In the game, we assume that the designer has two strategies and the attacker has three strategies. The designer's strategies are:

- s^d_1: the algorithm from [24], which places controllers at nodes with the highest degree,
- s^d_2: the genetic algorithm from [6], which adopts the placement scheme that aims at minimizing the number of control links.

In both strategies, the shortest physical paths are used for control channels. The attacker's strategy is always to cut n links deemed most critical, i.e., whose cutting maximizes P_{ij}. However, the link criticality assessment is based on three different assumptions:

- s^a_1: the physical topology only (no CP considerations),
- s^a_2: the CP realized according to strategy s^d_1,
- s^a_3: the CP realized according to strategy s^d_2.

The coefficients α and β in the utility functions are set to ensure $P_{ij} \gg D_i/A_{ij}$, so that the attacker has the incentive to launch attacks and the designer to defend against them.

We first set the number of controllers and link cuts to $|U| = 2$ and $n = 2$, respectively. The resulting controller placement for the designer's strategies s^d_1 and s^d_2, as well as the results of link cuts under the attacker's strategies s^a_1, s^a_2 and s^a_3, are depicted in Fig. 3. For example, when the attacker adopts s^a_2, links 7-8 and 10-11 are cut, as the links deemed most critical under the assumption of strategy s^d_1 applied for CP design. Based on this, Table 2 elaborates on the utilities of the two players under different strategy profiles, whose rationality can be analyzed as follows. As can be seen in the table, the designer always

Table 2: Game in strategic form with $n = 2$

	s_1^a	s_2^a	s_3^a
s_1^d	(-84.1, 71.1)	(-92.8, 77.8)	(-83.1, 70.1)
s_2^d	(-102.6, 88.6)	(-95.6, 79.6)	(-116.5, 102.5)

has higher utility when the attacker's utility is lower, regardless of the adopted strategies. For instance, if the designer's strategy is fixed to s_1^d, the attacker gains the maximum utility when it selects strategy s_2^a. This is because in s_2^a, the attacker detects the most critical links based on the CP implementation determined by s_1^d, which verifies that the attacker can maximize utility under the correct assumption of the designer's strategy. Under this strategy profile, i.e., (s_1^d, s_2^a), the designer has the minimum utility of -92.8, which represents the largest loss on the CP resilience. Compared to the other two strategy profiles (i.e., (s_1^d, s_1^a) and (s_1^d, s_3^a)), the utility of the attacker for (s_1^d, s_1^a) is higher than that for (s_1^d, s_3^a). This bears an important implication for the attacker – if the information about the CP implementation is not available, launching attacks based on criticality of links evaluated for the physical topology may be more favorable than that based on a CP implementation guess. Observations similar to above hold for the designer's strategy s_2^d as well.

If the attacker's strategy is fixed, e.g., to s_2^a, the designer's utility under strategy s_2^d is lower than under s_1^d. This may seem counterintuitive as s_2^a is based precisely on the correct assumption of the CP implemented using s_1^d, yet s_1^d yields higher robustness than s_2^d. However, as indicated by the utilities for the other two attacker's strategy profiles, the CP implemented with s_2^d is more vulnerable than that implemented with s_1^d. If the designer chooses s_2^d, link cuts can be more damaging even when the attacker bases the link criticality assessment on the wrong assumption of the CP design strategy. Consequently, by analyzing the game, the designer tends to prioritize s_1^d for a more resilient CP, which is reflected in the resulting NE.

By solving the game in Table 2, we obtain an NE ($\mathbf{y}_*^d$, $\mathbf{y}_*^a$) as $((0.746, 0.254)^T$, $(0.0, 0.0, 1.0)^T)$, where the designer selects strategy s_1^d with the probability of 0.746 and strategy s_2^d with the probability of 0.254, while the attacker uses strategy s_3^a in all cases. Namely, in the NE, when the attacker uses s_3^a for their own benefit, the designer defends by selecting s_2^d with a comparatively lower

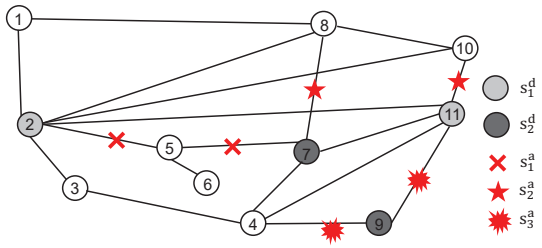


Fig. 3: SprintNET Topology.

Table 3: NEs of Games with Different n

n	$\mathbf{y}_*^d$	$\mathbf{y}_*^a$
1	(0.493, 0.507)	(1.0, 0.0, 0.0)
2	(0.746, 0.254)	(0.0, 0.0, 1.0)
3	(0.625, 0.375)	(0.0, 0.0, 1.0)
4	(0.670, 0.330)	(0.0, 0.0, 1.0)
5	(0.563, 0.437)	(0.0, 0.0, 1.0)

Table 4: Game in strategic form with $n = 1$

	s_1^a	s_2^a	s_3^a
s_1^d	(-81.2, 69.2)	(-86.5, 74.5)	(-78.4, 66.4)
s_2^d	(-93.5, 80.5)	(-88.4, 75.4)	(-94.4, 81.4)

probability. Hence, by following the NE, the designer can avoid large damages to the CP.

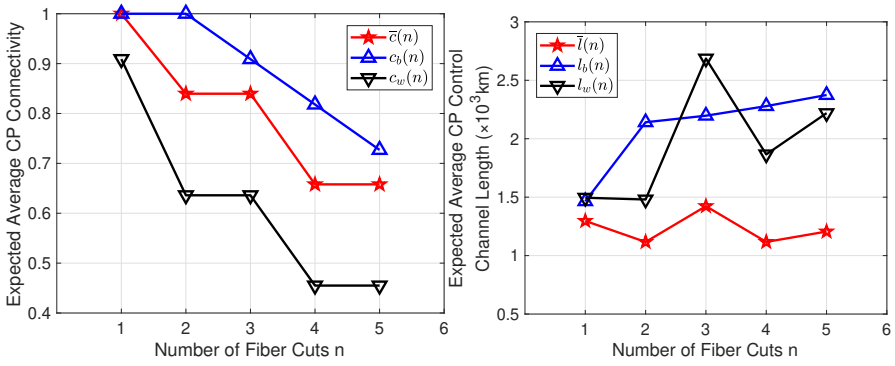
We assess the game when the number of fiber cuts n changes within $[1, 5]$. The NEs of the games are listed in Table 3. For example, when $n = 1$, the game is shown in Table 4, whose rationality can be analyzed similarly as the one in Table 2. In this game, the NE suggests that the designer should select s_1^d and s_2^d with probabilities of 0.493 and 0.507, respectively, to defend against the attack performed with s_1^a. When n changes from 2 to 5, the probability of selecting s_1^d by the designer is always higher than s_2^d, while the attacker would never use s_2^a otherwise the designer would suffer from the largest CP robustness loss, which violates the NE.

To gain insight into the CP solutions resulting from the NEs, we use two metrics to measure their properties in terms of the expected average CP connectivity $\overline{c}(n)$ and the expected average CP transmission distance $\overline{l}(n)$. These are calculated as:

$$\overline{c}(n) = (\mathbf{y}_*^d)^T \cdot \mathbf{C} \cdot \mathbf{y}_*^a, \qquad \overline{l}(n) = (\mathbf{y}_*^d)^T \cdot \mathbf{L} \cdot \mathbf{y}_*^a, . \tag{15}$$

where both $\mathbf{C}$ and $\mathbf{L}$ are $|S^d| \times |S^a|$ matrices, each element of $\mathbf{C}$ is the average CP connectivity $c(n)$ and each element of $\mathbf{L}$ is the average control channel transmission distance $l(n)$ under the corresponding pure strategy profile. The pure strategy profile refers to the one in which both players select one strategy from their own strategy space deterministically. Figs. 4 and 5 show the respective results of $\overline{c}(n)$ and $\overline{l}(n)$ under the NE. For comparison, we also provide the results under the best and the worst scenarios resulting from the pure strategy profiles, denoted with $c_b(n)$ and $c_w(n)$, respectively. Naturally, in Fig. 4(a), the average CP connectivity $\overline{c}(n)$ exhibits a downward trend when n increases.

As shown in Fig. 4(a), $\overline{c}(n)$ is higher than $c_w(n)$, while Fig. 4(b) shows the advantage of $\overline{l}(n)$ over $l_w(n)$. This verifies that, guided by the NEs, the designer can mitigate the effectiveness of attacks, and thus improve the CP robustness. However, $\overline{c}(n)$ cannot reach $c_b(n)$, which is inevitable for the existence of an



(a) Average CP connectivity $\bar{c}(n)$ (b) Average control channel length $\bar{l}(n)$

Fig. 4: The expected average CP connectivity and control channel length for different number of cut links.

intelligent attacker. Note that, in Fig. 4(b), the (expected) average transmission distance of control channels can increase or decrease with n. The reason for the increase is that the control channels have to traverse longer paths, while the decrease occurs when the connectivity between some switch-controller pairs is lost and, thus, the control channels disappear.

6 Conclusion

This paper considered an SDON under the threat from targeted fiber cut attacks and studied the problem of resilient CP design. To solve it, we proposed a game theoretic approach where the problem was modeled as a non-cooperative game between the CP designer and the attacker, and defined the game strategies and the utility functions for both players. In the game, the goal of the designer was to minimize the CP connectivity and latency degradation caused by targeted fiber cuts, while the attacker aimed at maximizing the CP disruption by cutting the most critical links. Theoretical analysis were conducted to obtain the Nash Equilibrium (NE) as the solution. Extensive simulation results suggested that following the NE enabled the designer to avoid the worst-case scenario where the CP suffers the largest losses, which confirmed the effectiveness of the proposed game-theoretic approach in improving the CP resilience to targeted fiber cuts.

References

1. Chen, X., et al.: Leveraging master-slave openflow controller arrangement to improve control plane resiliency in SD-EONs. Opt. Express **23**, 7550–7558 (Mar 2015)
2. Ciftcioglu, E., et al.: Topology design games and dynamics in adversarial environments. IEEE J. Sel. Areas Commun. **35**, 628–642 (Mar 2017)
3. Heller, B., et al.: The controller placement problem. In: Prof. of HotSDN 2012. pp. 7–12 (Aug 2012)

4. Hock, D., et al.: Pareto-optimal resilient controller placement in SDN-based core networks. In: Proc. of ITC 2013. pp. 1–9 (Sept 2013)
5. Hu, Y., et al.: On reliability-optimized controller placement for software-defined networks. China Commun. **11**, 38–54 (Feb 2014)
6. Hu, Y., et al.: The energy-aware controller placement problem in software defined networks. IEEE Commun. Lett. **21**, 741–744 (Apr 2017)
7. Huang, H., et al.: Realizing highly-available, scalable and protocol-independent vSDN slicing with a distributed network hypervisor system. IEEE Access **6**, 13513–13522 (2018)
8. Iyer, S., et al.: Attack robustness and centrality of complex networks. PLoS ONE **8**, 1–17 (Apr 2013)
9. Li, H., et al.: Byzantine-resilient secure software-defined networks with multiple controllers in cloud. IEEE Trans. Cloud Comput. **2**, 436–447 (Oct 2014)
10. Li, S., et al.: Protocol oblivious forwarding (POF): Software-defined networking with enhanced programmability. IEEE Netw. **31**, 58–66 (Mar 2017)
11. Lu, P., et al.: Highly-efficient data migration and backup for Big Data applications in elastic optical inter-datacenter networks. IEEE Netw. **29**, 36–42 (Sept/Oct 2015)
12. McKeown, N., et al.: OpenFlow: Enabling innovation in campus networks. Comput. Commun. Rev. **38**, 69–74 (Mar 2008)
13. Mohan, P., et al.: Primary-backup controller mapping for Byzantine fault tolerance in software defined networks. In: Proc. of GLOBECOM 2017. pp. 1–7 (Dec 2017)
14. Nahir, A., et al.: Topology design of communication networks: A game-theoretic perspective. IEEE/ACM Trans. Netw. **22**, 405–414 (Apr 2014)
15. Natalino, C., et al.: Content accessibility in optical cloud networks under targeted link cuts. In: Proc. of ONDM 2017. pp. 1–6 (May 2017)
16. Nisan, N.: Algorithmic Game Theory. Cambridge University Press (2007)
17. Rueda, D., et al.: Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements. J. Netw. Syst. Manag. **25**, 269–289 (Apr 2017)
18. Shen, Y., et al.: On the discovery of critical links and nodes for assessing network vulnerability. IEEE/ACM Trans. Netw. **21**, 963–973 (Jun 2013)
19. Skorin-Kapov, N., et al.: Physical-layer security in evolving optical networks. IEEE Commun. Mag. **54**, 110–117 (Aug 2016)
20. Thyagaturu, A., et al.: Software defined optical networks (SDONs): A comprehensive survey. IEEE Commun. Surveys Tut. **18**, 2738–2786 (Fourth Quarter 2016)
21. Yang, Z., et al.: An efficient algorithm for constructing controller trees in SDN. In: Proc. of GLOBECOM 2017. pp. 1–6 (Dec 2017)
22. Zhang, Y., et al.: On resilience of split-architecture networks. In: Proc. of GLOBECOM 2011. pp. 1–6 (Dec 2011)
23. Zhao, B., et al.: Survivable control plane establishment with live control service backup and migration in SD-EONs. J. Opt. Commun. Netw. **8**, 371–381 (Jun 2016)
24. Zhu, J., et al.: Control plane robustness in software-defined optical networks under targeted fiber cuts. In: Proc. of ONDM 2018. pp. 118–123 (May 2018)
25. Zhu, Z., et al.: Demonstration of cooperative resource allocation in an openflow-controlled multidomain and multinational SD-EON testbed. J. Lightw. Technol. **33**, 1508–1514 (Apr 2015)
26. Zhu, Z., et al.: Build to tenants' requirements: On-demand application-driven vSD-EON slicing. J. Opt. Commun. Netw. **10**, A206–A215 (Feb 2018)