Optimization Model for Designing Multiple Virtualized Campus Area Networks Coordinating With Wide Area Networks

Takashi Kurimoto, *Member, IEEE*, Shigeo Urushidani, *Member, IEEE*, and Eiji Oki, *Fellow, IEEE*

***Abstract*—We propose an optimization model for designing multiple network functions virtualization (NFV)-based campus area networks (CANs). Organizations, such as universities and research institutions have their own campus information and communication technology equipment, but many would like to move this equipment to NFV and cloud data centers for improving reliability and resiliency. However, NFV-based CAN is not affordable for them, because costs are higher with a cloud. One solution is for multiple organizations to procure NFV and cloud data center resources together. By doing so, their individual costs of using these resources will be reduced. To make progress on this approach, there are planning issues to resolve when choosing optimal NFV and cloud data center locations. The proposed model minimizes the total network costs incurred by the organizations, including the wide area network cost and data synchronization costs for recovery from faults at data centers and the various subcampus network configurations of legacy CANs. The model is formulated and analyzed by using mixed integer linear programming. The effect of cost minimization is evaluated in a ladder network and an actual network, SINET5, and it is found that the costs can be reduced by up to 63%. The calculation times of this model under practical conditions are short and the model will be useful in practice. It is also shown that the cost of fault recovery can be suppressed. These results will encourage organizations to deploy NFV-based CANs.**

***Index Terms*—Network function virtulization, cloud, migration, campus area network.**

I. Introduction

THERE are many universities and academic institutions for which information communication technology (ICT) services are essential for their students, faculties, and researchers. For example, E-learning services are invaluable for students and teachers, while ultra-high-bandwidth data transmissions are needed by researchers for carrying out cutting-edge experimental studies. In Japan, the campus area networks (CANs) of many universities and academic institutions are connected to SINET5 (Science Information NETwork 5) [1]–[3]. SINET5 is a wide area network (WAN) that provides data communication service between CANs and between CANs and the Internet.

Information technology (IT) infrastructures, such as application servers, are usually deployed on campus premises. The servers are accessed from not only campus but also the homes of students and faculty members. Thus, application servers on CANs must be able to be accessed via the Internet. To do so, security devices, such as firewalls and intrusion detection systems (IDSs), are indispensable, as they protect computing resources from malicious cyber activities in CANs. Moreover, researchers transfer their data from shared experimental facilities to CANs. The volume of such data has become very large, and their security requirements have become stringent. For example, it is expected that the volume of gene data sent over networks will reach 10 [TB/s] [4] in the near future, and such personal data will have to be treated securely. For these reasons, CANs are connected through virtual private networks (VPNs) provided over WANs. VPNs enable firewall devices to be shortcut, improving data throughput.

With the emergence of virtualization technologies such as cloud computing [5] and network functions virtualization (NFV) [6]–[8], we expect that ICT infrastructures, such as compute servers, storage devices, and network equipment, can be economically moved from campuses to data centers (DCs). Some organizations have begun to move their ICT infrastructures from their own premises to outside DCs in order to improve security, stability, and reliability [9], [10]. Against this background, the authors previously proposed a multi-campus ICT equipment virtualization architecture [11]. This architecture can encourage organizations to migrate their own ICT systems located on their premises to virtualized cloud environments with NFV technologies.

There have been many resource allocation studies [12]. However, from an economical point of view, not much progress has been made on network planning methods for NFV-based CANs. At present, NFV-based CANs are not affordable. In particular, the data transmission costs increase when moving to a cloud, because the data traffic over them is larger than that for only application servers, such as Web servers. Moreover, as organizations evaluate the merits of an NFV-based CAN individually, they usually do not find enough merit in their migrating their CANs.

This paper proposes an optimization model for designing multiple NFV-based CANs in consideration of WAN costs. In

Manuscript received March 31, 2018; revised August 11, 2018 and September 28, 2018; accepted September 30, 2018. Date of publication October 3, 2018; date of current version December 10, 2018. Parts of this paper were partially presented at IEEE International Conference on Communications (ICC 2018) [13]. The associate editor coordinating the review of this paper and approving it for publication was G. Schembra. *(Corresponding author: Takashi Kurimoto.)*

T. Kurimoto and S. Urushidani are with the Information System Architecture Science Research Division, National Institute of Informatics, Tokyo 101-8430, Japan (e-mail: tkurimoto@nii.ac.jp).

E. Oki is with the Department of Communication and Computer Engineering, Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan.

Digital Object Identifier 10.1109/TNSM.2018.2873831

1932-4537 © 2018 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

particular, we describe a design for migrating multiple CANs to NFV-based ones. The aim is to migrate ICT infrastructures on campus premises to NFV and cloud data centers (NFV-DC) for improving reliability and resiliency. To reduce the cost of introducing NFV-based CANs, one possible solution is for multiple organizations to procure NFV and cloud resources together. That is, by co-procuring resources for NFV-based CANs and sharing them, individual organizations can reduce their costs. To make progress on this approach, we need to address a number of planning issues when choosing optimal NFV-DC sites. In particular, in the model we propose, the total network cost consists of those of CANs, WANs, and NFV data centers. We take into account the two configurations of legacy CANs that have multiple sites on campus. We also introduce a prohibited pair condition to keep the transmission latency between campuses and NFV-DCs within a certain range of values. We present optimization problems that take failures at data centers into consideration for a business continuity plan (BCP) for campuses. For this, the proposed model includes data synchronization to recover from failures. We formulate these optimization problems as mixed integer linear programming (MILP) problems. We evaluated the effect of cost minimization in a ladder network to observe the basic characteristics of the proposed model; we compared different network configurations of legacy CANs with the capability to recover from faults. We also evaluated the cost reduction of NFV-based CANs with the proposed model under more practical conditions and found that the costs can be reduced by up to 63% on the SINET network. We also evaluated the computation time of the proposed model and found that it is practical. Thus, these results indicate that the costs of NFV-based CANs can be reduced, which will encourage organizations to deploy NFV-based CANs.

This paper is an extended version of the work presented in [13]. We give details on the background of networks in terms of the SINET network architecture by referring to various related work. We discuss the various network configurations of multiple sub-campuses that use legacy CANs. We added a capability to recover from faults to the proposed model. Moreover, we extensively evaluated the performance of the proposed model in various traffic and network conditions, including a practical network based on SINET.

II. Background and Related Work

SINET5, shown in Fig. 1, is a Japanese academic backbone network for about 900 research institutes and universities and provides network services to about 3 million academic users. It plays an important role in supporting a wide range of research that need high-performance connectivity, such as high-energy physics, nuclear fusion research, astronomy, geodesy, seismology, and computer science. SINET5 provides points of presence, called “SINET data centers” (SINET-DCs), and one or more SINET-DCs are located in each prefecture in Japan. Universities can connect their own access lines to a router on SINET-DC and communicate with other universities also via the Internet. All IP routers are connected by a 100-Gbps-based path; universities can be connected to SINET with 100-Gbps access lines. End users can transmit data to other end users with a 100-Gbps throughput. An IP router is directly connected to the other routers by a logical circuit, which is routed with the shortest optical fiber length. Thus, the transmission latency between a pair of routers is very low [3].

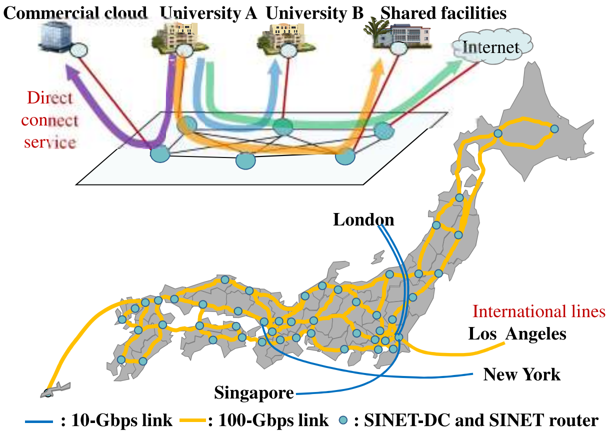


Fig. 1. SINET5 topology.

SINET also provides a direct cloud connection service. With this service, commercial cloud providers directly connect their data centers to SINET5 with high-speed links such as 10-Gbps links. Academic users can thus access cloud computing resources with very high bandwidth and low latency via SINET5 and can receive high-performance computer communications between campuses and cloud computing resources. As of July 2018, 23 cloud service providers are directly connected to SINET5, and more than 129 universities use cloud resources directly via SINET5.

Cloud services were first used to replace some of the services offered through application servers, such as Web servers or e-mail servers. Currently, cloud services are considered in universities’ BCPs as a way of dealing with the threat of natural disaster and cyber-attacks. Here, universities need to strengthen their own buildings to resist earthquakes, floods, power failures, and optical fiber cuts. The security of their buildings also have to be strengthened, for example, with biometric authentication systems to manage the entry of people. The costs of renovating buildings with ICT systems is substantial. Here, cloud service providers can provide a cloud service with strengthened buildings to move ICT equipment, including application servers as well as routers, firewalls and other network equipment, to cloud data centers.

There are two approaches to moving network functions to a data center: (i) deploying vendor-specific network devices on a data center and (ii) installing the virtual network function (VNF) on a computing resource which can be shared with other applications. Generally speaking, the latter approach allows the network configuration to be managed more flexibly. However, it can not handle large amounts of traffic at a lower cost than the former approach. Thus, it is expected to reduce the service costs of NFV which can offer flexible network management with cloud services.

There are two types of cloud service: public clouds and private clouds. In a public cloud, computing resources are shared by many different people. The price of the service depends on the amount of cloud resources used. A public cloud has merit for a user of unpredictable demand or small-demand applications whose data are not so security-sensitive. On the other hand, in a private cloud, physical resources such as compute, storage and network equipments are dedicated to an owner. Physical resource separation is preferable to achieve robust information assurance according to the defense-in-depth strategy [14]. A private cloud has merit for a user who has security-sensitive data [15]. The service expenses are fixed and depend on the amount of dedicated cloud resources.

A private cloud is preferable from a security point of view for the academic segment. However, the higher costs of private clouds are an obstacle for organizations that have only small- or medium-demand applications. In this paper, we focus on a joint procurement of a private cloud for universities. This idea overcomes the cost problem of a private cloud. For example, we have reduced costs by a joint procurement of data links which connect universities to SINET-DC [16]. Required resources for the data link such as network devices, spare devices, network management systems, and operators are shared by universities and a merit of scale can be achieved.

Currently, universities individually negotiate and make contracts with cloud providers. The procedure to purchase cloud resources, which includes describing service specifications and negotiating over costs, is a hard task for a single university that has small- to middle-demand applications. On the other hand, if universities cooperated with each other, their negotiation power would be increased, because their overall cloud resources such as compute and storage would be large and merit of cost can be archived. Joint procurement of private cloud includes not only equipment but also additional works and facilities, which include logical design, physical design, control function configuration, operation system construction, system monitoring, troubleshooting, hardware maintenance, space, and power etc. These additional expenses can be shared among participated universities. Therefore, the cost of cloud services and the burden of the procurement procedure could be reduced. A jointly co-procured private cloud service offsets the higher charges of a private cloud. Note that the resources of the private cloud would be deployed to the cooperating universities; they would not be shared with other unspecified users. Thus, the security is higher than in a public cloud.

To share the computing resources with multiple universities, several NFV and cloud platforms are provided [17], [18]. With this platform, a separate and dedicated sliced network is provided to each university. Traffic incoming from and outgoing to each university is isolated from traffic of the other universities by using a sliced network. Virtual machines (VMs) are created and dedicated to a university and connected to each sliced network. Applications and VNFs are independently executed by the university. Data are handled within the sliced network and the VMs dedicated to the university. Thus, the data of each university can be separated securely. In addition, a redundant NFV-DCs can be used to recover from faults at the data center [11]. With this redundant NFV-DCs, important data in active storage is backed up using storage at another site. When an active storage fault occurs, applications can use data in backup storage. Therefore, VM environment ensures data integrity. With these technologies, multiple universities can operate virtualized ICT equipment in shared computing resources. Also we deployed NFV testbed on SINET5 and this testbed has been opened to universities since April 2017. Currently 11 organizations (seven national universities, one municipal university, two private universities, one research institution) are evaluating NFV features, which include reliability, performance, feasibility and manageability through this testbed [19]. For example, a university evaluates the virtual router functions for connecting CANs to a public cloud via a virtual router. A university evaluates the virtual router functions which can be migrated into another DC against DC failure. On the other hand, no study has addressed network planning for NFV-based CANs. Thus, we decided to determine how to select or set up data centers that are most suitable for multiple organizations to share.

There are several resource allocation studies [8], [12], [20] on designing virtual networks embedded in physical networks for providing NFV services. Several virtual networks and virtual network resources are allocated over physical network resources. One study [21] presented a network function placement and chaining problem was formulated as an integer linear programming (ILP) model. The solution to the ILP problem is an optimal VNFs allocation under resource capacity constraints. Another study [22] presented a heuristic algorithm for on-demand VNF placement to solve a resource allocation problem in an electrical/optical hybrid data center. Moreover, in [23], a genetic algorithm was used to reduce the calculation time needed to solve a similar problem for an on-demand service. The optimization problems considered in these studies put restrictions on the resource capacity as given conditions. This paper aims to find suitable data center locations and resource allocations for a private cloud jointly procured by different universities.

III. Design of Multiple NFV-Based CANs

A. *Multiple NFV-Based CANs*

Figure 2 shows legacy CANs used by multiple universities. Three universities are depicted. Universities 1 and 3 have two and one sub-campuses, respectively. In a legacy CAN, universities are connected via WAN which is dedicated network for universities. Intra-university communications are exchanged via WAN. Traffic form the Internet to a university arrives at the Internet gateway of the WAN, which is connected to an Internet Service Provider (ISP). This traffic is delivered to a main campus via WAN. In the main campus, traffic is checked by a firewall, which is located on the main campus. After that, the traffic allowed through the firewall is delivered to sub-campuses. Application servers are also located on the main campus and can be accessed via the Internet from student homes. Because sub-campus traffic goes through the main campus, we call this type of legacy CAN a "main campus hub type." There is another type of legacy CAN whose sub-campus traffic is directly exchanged over the Internet directly. We call this type of legacy CAN a "direct access type." This type of legacy CAN is discussed in Section III-A4.

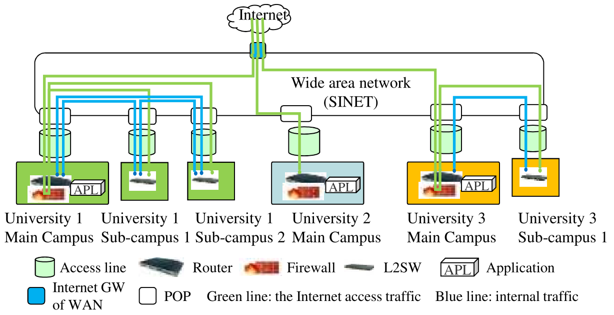


Fig. 2. Legacy CAN configuration (main campus hub type).

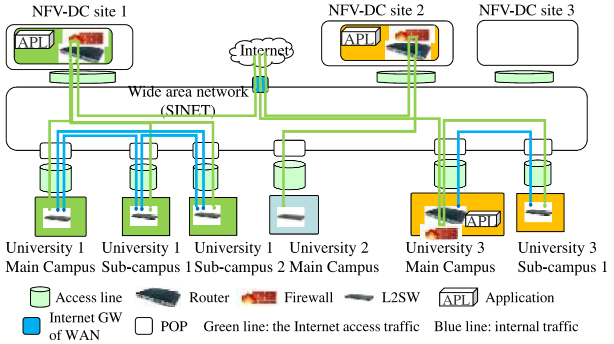
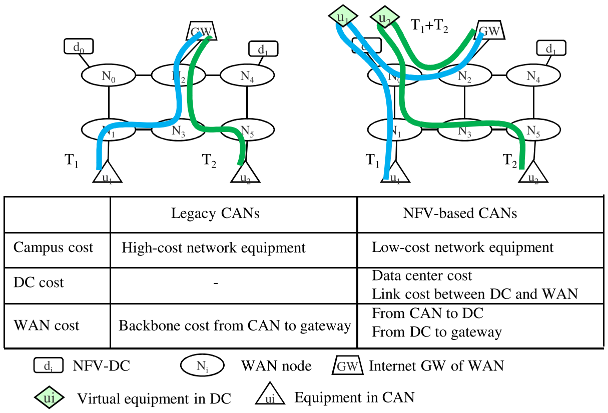


Fig. 3. NFV-based CAN configuration.



	Legacy CANs	NFV-based CANs
Campus cost	High-cost network equipment	Low-cost network equipment
DC cost	-	Data center cost Link cost between DC and WAN
WAN cost	Backbone cost from CAN to gateway	From CAN to DC From DC to gateway

Fig. 4. Cost evaluation outline.

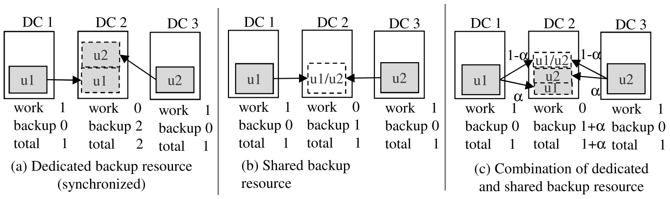
Figure 3 illustrates NFV-based CANs. There are three NFV-DCs, and universities 1 and 3 choose NFV-based CANs, while university 2 does not migrate its data. In an NFV-based CAN, ICT applications are moved from the campus premises to an external NFV-DC. In addition, network functions, such as security devices and routers, are moved to the NFV-DC. Thus, only simple network functions, such as layer-2 switches, remain on premises. In this network, Internet access traffic is delivered to the NFV-DC and checked by a virtual firewall in the form of a virtual network function (VNF) on the NFV-DC. After that, the traffic allowed through the virtual firewall is delivered to the premises through a virtual router in the form of a VNF. Here, traffic from the NFV-DCs to each campus is delivered securely via a VPN provided by a WAN.

Figure 4 shows the pros and cons of legacy CANs and NFV-based CANs. For example, in a legacy CAN, each university has its own expensive network equipment and computing resources. In an NFV-based CAN, multiple universities can share computing resources for VNF and application servers. However, an NFV-based CAN requires additional fees for renting data centers and accessing the links to the center. Thus, we decided to clarify the pros and cons of legacy and NFV-based CANs. The first point is the additional cost of an NFV-DC. The second is the additional transmission latency and WAN costs incurred by taking a deviating route via the NFV-DC. We assume that the WAN is a dedicated network for the university. Therefore, the WAN costs are evaluated when planning the dedicated network.

1) Additional Costs of NFV-Based CAN: When a cloud is used as an NFV-DC, the amount of data exchanged through VNFs, such as routers and firewalls, is larger than the amount of data sent to and from a Web server. This large amount of data burdens universities with higher expenses. Instead, universities could procure together and share cloud resources, as mentioned in Section II. For such joint procurement, we have to decide which data center(s) are best and which universities share them. Thus, a planning method for deciding combinations of universities and NFV-DCs is required.

2) Additional Data Transmission Latency and WAN Cost: Here, we consider the additional WAN costs incurred by the longer NFV-based CAN routes than legacy CAN routes, as illustrated in Fig. 4. In an NFV-based CAN, the Internet traffic goes to the NFV-DC and then goes to the campus. In a legacy CAN, the Internet traffic goes to the campus directly. The longer route increases the WAN costs. Thus, we need to take into account these additional costs. The longer route of the NFV-based CAN also causes an additional data transmission latency in excess of that of a legacy CAN. The network transmission latency consists of two factors. One is the queuing delay in buffers on routers, and the other is the physical signal transmission latency. The queuing delay depends on the link utilization. If we simply assume the $M/M/1$ queuing system [24], the queuing delay can be expressed as $\frac{1}{\lambda}\frac{\rho}{1-\rho}$, where λ means the packet arrival rate per unit time and ρ is the link utilization. ρ is expressed as $\rho = \frac{\lambda}{\mu}$, where μ is the packet service rate per unit time. Note that the value of $\frac{1}{\lambda}\frac{\rho}{1-\rho}$ is less than 1.5 per unit time for moderate utilizations, $\rho < 0.6$, and increases significantly for high utilization, $\rho \geq 0.8$. In normal WAN network operations, the link utilization is controlled to be at a moderate or low level. There are two reasons for this: to reserve backup bandwidth against link failures and to suppress the queuing delay. In particular, the queuing delay should able to be ignored in normal network operations. Thus, we will only take account into the transmission latency due to the physical fiber length in the NFV-based CAN. Along 100 km of fiber, transmission latency (one way) is approximately 0.5 ms.

3) Considering Fault Recovery: Japan is a country that has experienced many large disasters. Thus, BCPs are especially important for academic institutions and universities in the country. Moreover, ICT systems are expected to have fault recovery capabilities. Working ICT systems that have suffered a disaster will not be accessible. By moving the



(a) Dedicated backup resource (synchronized)

(b) Shared backup resource

(c) Combination of dedicated and shared backup resource

Fig. 5. Backup resource allocation for fault recovery.

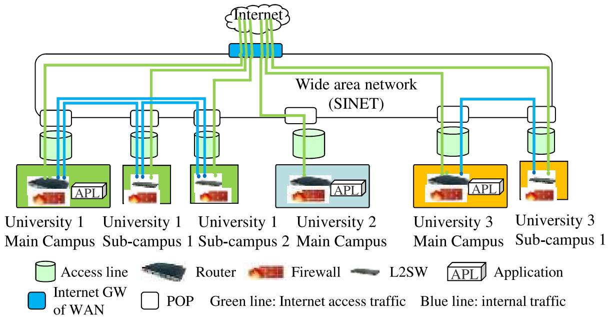


Fig. 6. Legacy CAN configuration (direct access type).

systems to another DC, ICT services can be provided to faculties and students even just after the occurrence of a disaster. To recover ICT services, backup ICT resources should be reserved. Additional costs are incurred for keeping the backup resources ready. Using multiple NFV-based CANs is one way to reduce the additional costs of keeping reserve resources between universities. This means we have to design both working and backup resources simultaneously.

Figure 5 shows the types of backup resource allocation for NFV-based CANs. The first type is a dedicated backup resource. With this option, working and backup ICT systems are synchronized, and the same amount of ICT resources is used for both in a dedicated manner. Figure 5 (a) shows a dedicated backup resource. The working and backup resources of university 1, u_1, are allocated to DC 1 and DC 2, respectively, and those of university 2, u_2, are allocated to DC 3 and DC 2. Consider, for example, a data-base backup application. Figure 5 (b) shows the shared backup resource. Here, the working ICT systems can be re-constructed in the backup resource after a disaster. Thus, the backup resources are shared with u_1 and u_2, whose working resources are allocated to different DCs (DC 1 and DC 3). Consider, for example, a front-end Web server. Figure 5(c) shows a combination of dedicated and shared backup resources. The university uses both shared and dedicated backup applications. Some of the working resources are treated as dedicated backup resources. Note that α ($0 \leq \alpha \leq 1$) is the ratio of dedicated backup resources to working resources. The rest of the working resources are treated as shared backup resources.

4) Direct Access of Sub-Campus in Legacy CANs: Figure 6 illustrates direct access from sub-campuses to the Internet in a legacy CAN. Here, sub-campuses are independent from the main campus, and each sub-campus sends and receives data to and from the WAN directly, while, in Fig. 2, the sub-campus traffic is delivered through the main campus.

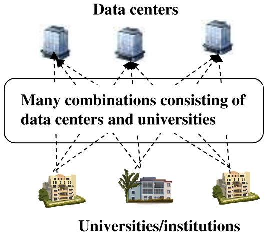

Data centers
Many combinations consisting of data centers and universities
Universities/institutions

Fig. 7. Combination of data centers and universities.

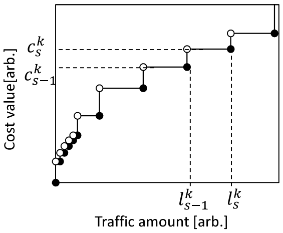


Fig. 8. Cost function example (non-decreasing step function).

B. Problem Statement

To reduce the costs of procuring a DC, we would like to find the lowest-cost data center to which to allocate ICT resources. Figure 7 shows an ICT resource allocation. There are many combinations consisting of DCs and universities. The number of combinations is $K_{\mathrm{D}}^{K_{\mathrm{U}}}$. Here, K_{D} is the number of DCs, and K_{U} is the number of universities. We have to evaluate the costs for each combination and find the combination with the lowest cost. The calculation load increases exponentially depending on K_{U}. Also, taking the backup resource design into consideration, the number of combinations increases, i.e., $K_{\mathrm{D}}^{K_{\mathrm{U}}} \times (K_{\mathrm{D}} - 1)^{K_{\mathrm{U}}}$. For example, by using the brute-force search, we have to calculate the costs of 144 combination patterns in $K_{\mathrm{U}} = 2$ and $K_{\mathrm{D}} = 4$. On the other hand, we have to calculate the costs of 6.19×10^{10} combination patterns in $K_{\mathrm{U}} = 10$ and $K_{\mathrm{D}} = 4$. Thus, we need to find the lowest-cost combination in a practical manner.

C. Network Modeling

1) Assumptions: We define four types of cost functions, each of which is a function of the traffic amount *t*. $f^1(t)$ is the usage cost at a campus site that uses links and layer-2 switches. $f^2(t)$ is the usage cost at a campus site that uses links, layer-2 switches, routers, and applications. $f^3(t)$ is the usage cost at a campus site that uses firewalls. $f^4(t)$ is the usage cost at a data center site that uses links, layer-2 switches, routers, firewalls, and applications.

We assume that $f^k(t)$, where $k \in [1, 4]$, is a non-decreasing step function. S_k denotes a set of cost classes of cost function $f^k(t)$. In the definition of $f^k(t)$, if *t* is less than or equal to l_s^k, where $k \in [1, 4]$ and $s \in S_k$, the cost is c_s^k. If $s_1 < s_2$, we have $l_{s_1}^k < l_{s_2}^k$ and $c_{s_1}^k < c_{s_2}^k$. We set the minimum value of l_s^k over $s \in S_k$ to zero for all $k \in [1, 4]$. Figure 8 shows an example of the cost function $f^k(t)$. Generally speaking, more chances of discount can be expected as larger resources are purchased. The cost per unit speed of a higher speed interface is lower than that of a lower speed interface. Thus, the proposed model assumes non-linear non-decreasing cost functions.

2) Cost of Legacy CAN (Main Campus Hub Type): Here, we discuss the cost of a legacy CAN, as shown in Fig. 2. U denotes a set of users or institutions. $u \in U$ has a main campus and n_u sub-campuses. Z_u denotes a set of campuses in $u \in U$. $i = 0 \in Z_u$ indicates the main campus in $u \in U$, and $i(\neq 0) \in Z_u$ indicates sub-campus *i*, where $|Z_u| = n_u+1$. Traffic from campus $i \in Z_u$ to campus $j(\neq i) \in Z_u$ is denoted by t^u_{ij}, and traffic in the opposite direction is denoted by t^u_{ji}. Traffic from the Internet to campus $i \in Z_u$ is denoted by $t^u_{\mathrm{e}i}$, and that in the opposite direction is denoted by $t^u_{i\mathrm{e}}$.

The access link traffic from a main campus, where $i = 0 \in Z_u$ and $u \in U$, to a WAN is denoted by H^u_0, which is given by

$$H^u_0 = \max\Big(H^u_{0,\mathrm{up}}, H^u_{0,\mathrm{down}}\Big). \tag{1}$$

$H^u_{0,\mathrm{up}}$ and $H^u_{0,\mathrm{down}}$ are the up-link traffic and down-link traffic from the main campus, where $i = 0 \in Z_u$, to the WAN, respectively. $H^u_{0,\mathrm{up}}$ and $H^u_{0,\mathrm{down}}$ are given by

$$H^u_{0,\mathrm{up}} = \sum_{i\in Z_u} t^u_{i\mathrm{e}} + \sum_{i\in Z_u\setminus\{0\}} t^u_{0i} \tag{2}$$

$$H^u_{0,\mathrm{down}} = \sum_{i\in Z_u} t^u_{\mathrm{e}i} + \sum_{i\in Z_u\setminus\{0\}} t^u_{i0}. \tag{3}$$

The access link traffic from sub-campus $i(\neq 0) \in Z_u$ to the WAN is denoted by T^u_i, which is given by

$$T^u_i = \max\Big(T^u_{i,\mathrm{up}}, T^u_{i,\mathrm{down}}\Big). \tag{4}$$

$T^u_{i,\mathrm{up}}$ and $T^u_{i,\mathrm{down}}$ are the up-link traffic and down-link traffic from sub-campus $i(\neq 0) \in Z_u$ to the WAN, respectively. $T^u_{i,\mathrm{up}}$ and $T^u_{i,\mathrm{down}}$ are given by

$$T^u_{i,\mathrm{up}} = \sum_{j\in Z_u\setminus\{i\}} t^u_{ij} + t^u_{i\mathrm{e}} \tag{5}$$

$$T^u_{i,\mathrm{down}} = \sum_{j\in Z_u\setminus\{i\}} t^u_{ji} + t^u_{\mathrm{e}i}. \tag{6}$$

The traffic from/to a main campus, where $i = 0 \in Z_u$ and $u \in U$, to/from the Internet is denoted by P^u_0, which is given by

$$P^u_{0\mathrm{e}} = \sum_{i\in Z_u} (t^u_{i\mathrm{e}} + t^u_{\mathrm{e}i}). \tag{7}$$

C^{L} denotes the costs of a legacy network. C^{L} is given by

$$C^{\mathrm{L}} = \sum_{u\in U}\left\{f^2(H^u_0) + f^3(P^u_{0\mathrm{e}}) + \sum_{i\in Z_u\setminus\{0\}} f^1(T^u_i)\right\}. \tag{8}$$

3) Cost of NFV-Based CAN Network: Here, let us discuss the costs of the NFV-based CAN network shown in Fig. 3.

C^{P} denotes the costs of the proposed network. The access link traffic for $u \in U$ from the data center to the WAN is denoted by T^u_{d}, which is given by

$$T^u_{\mathrm{d}} = \sum_{i\in Z_u} (t^u_{i\mathrm{e}} + t^u_{\mathrm{e}i}). \tag{9}$$

C^{P} is given by

$$C^{\mathrm{P}} = \sum_{u\in U}\sum_{i\in Z_u} f^1(T^u_i) + f^4\left(\sum_{u\in U} T^u_{\mathrm{d}}\right). \tag{10}$$

4) Optimization Problems Integrating NFV-Based and Legacy CANs: Here, we show how to combine an NFV-based CAN network with a legacy network in order to minimize network costs. The optimization problem determines which network each university $u \in U$ adopts, and, if a university adopts an NFV-based CAN, which data center the university uses. For example, in Fig. 3, universities 1 and 3 use data centers, while university 2 does not choose data center migration.

Let us introduce a prohibited pair condition to keep the transmission latency between campuses and NFV-DCs under a certain value. *G* is a set of prohibited pairs (*u*, *d*), $u \in U$, $d \in D$, where *D* is a set of data centers and university $u \in U$ is not allowed to move the data center $d \in D$. For example, suppose that the transmission latencies between university u_1 and data centers d_1 and d_2 are 9 ms and 15 ms, respectively. University u_1 allows ICT resources to be moved to a data center, if the transmission latency is within 10 ms; accordingly, resources can be moved data center d_1, but not to d_2. In this case, the pair (u_1, d_2) is prohibited. In addition, we assume that the traffic $u \in U$ can be allocated to at most one data center without splitting it.

Let x_{ud} be a binary decision variable that is set to one if the traffic of $u \in U$ is allocated to $d \in D$ and is set zero otherwise. Let y_u be a binary decision variable that is set to one if $u \in U$ adopts a legacy network and is set to zero otherwise.

Let z^1_{sui} be a binary decision variable that is set to one if T^u_i, where $i \in Z_u$ and $u \in U$, belongs to cost class $s \in S_1$ and is set to zero otherwise. Let z^2_{su} be a binary decision variable that is set to one if H^u_0 or T^u_0, where $u \in U$, belongs to cost class $s \in S_2$ and is set to zero otherwise. Let z^3_{sui} be a binary decision variable that is set to one if $P^u_{0\mathrm{e}}$, where $i = 0 \in Z_u$ and $u \in U$ or $Q^u_{0\mathrm{e}}$, where $i \in Z_u$ and $u \in U$ belong to cost class $s \in S_3$, and are set to zero otherwise. Let z^4_{sd} be a binary decision variable that is set to one if the sum of traffic allocated to $d \in D$, and T^u_d belongs to cost class $s \in S_4$ and is set to zero otherwise.

We can formulate an optimization problem to minimize the total costs of combining NFV-based and legacy CANs as follows.

Objective

$$\min\sum_{u\in i}\left\{\sum_{i\in Z_u}\sum_{s\in S_1} c^1_s z^1_{sui} + \sum_{s\in S_2} c^2_s z^2_{su} + \sum_{s\in S_3} c^3_s z^3_{su0}\right\} + \sum_{d\in D}\sum_{s\in S_4} c^4_s z^4_{sd} \tag{11a}$$

Subject to

$$T^u_i \sum_{d\in D} x_{ud} \leq \sum_{s\in S_1} z^1_{sui} l^1_s, \forall u \in U, i \in Z_u \tag{11b}$$

$$\sum_{u\in U} T^u_{\mathrm{d}} x_{ud} \leq \sum_{s\in S_4} z^4_{sd} l^4_s, \forall d \in D \tag{11c}$$

$$H_0^u y_u \leq \sum_{s\in S_2} z_{su}^2 l_s^2, \forall u \in U \tag{11d}$$

$$T_i^u y_u \leq \sum_{s\in S_1} z_{sui}^1 l_s^1, \forall u \in U, i \in Z_u \backslash \{0\} \tag{11e}$$

$$P_{0\mathrm{e}}^u y_u \leq \sum_{s\in S_3} z_{su0}^3 l_s^3, \forall u \in U \tag{11f}$$

$$\sum_{d\in D} x_{ud} + y_u = 1, \forall u \in U \tag{11g}$$

$$\sum_{s\in S_1} z_{sui}^1 = 1, \forall u \in U, i \in Z_u \tag{11h}$$

$$\sum_{s\in S_2} z_{su}^2 = 1, \forall u \in U \tag{11i}$$

$$\sum_{s\in S_3} z_{su0}^3 = 1, \forall u \in U \tag{11j}$$

$$\sum_{s\in S_4} z_{sd}^4 = 1, \forall d \in D \tag{11k}$$

$$x_{ud} = 0, \forall (u, d) \in G \tag{11l}$$

$$x_{ud} \in \{0, 1\}, \forall u \in U, d \in D \tag{11m}$$

$$y_u \in \{0, 1\}, \forall u \in U \tag{11n}$$

$$z_{sui}^1 \in \{0, 1\}, \forall s \in S_1, u \in U, i \in Z_u \tag{11o}$$

$$z_{su}^2 \in \{0, 1\}, \forall s \in S_2, d \in D \tag{11p}$$

$$z_{su0}^3 \in \{0, 1\}, \forall s \in S_3, u \in U \tag{11q}$$

$$z_{sd}^4 \in \{0, 1\}, \forall s \in S_4, d \in D \tag{11r}$$

Equation (11a) minimizes the total costs. Equation (11b) indicates that, when $u \in U$ adopts the proposed network model, traffic, T_i^u, belonging to cost class $s \in S_1$ must not exceed l_s^1. Equation (11c) indicates that the sum of traffic allocated to data center $d \in D$, T_{d}^u, belonging to cost class $s \in S_4$, must not exceed l_s^4. Equation (11d) indicates that, when $u \in U$ adopts a legacy network, traffic H_0^u, belonging to cost class $s \in S_2$, must not exceed l_s^2. Equation (11e) indicates that, when $u \in U$ adopts a legacy CAN, T_i^u, belonging to cost class $s \in S_1$, must not exceed l_s^1. Equation (11f) indicates that, when $u \in U$ adopts a legacy CAN, traffic $P_{0\mathrm{e}}^u$, belonging to cost class $s \in S_3$, must not exceed l_s^3. Equation (11g) indicates that the traffic of $u \in U$ can be allocated to at most one data center without splitting it, and, otherwise, $u \in U$ adopts a legacy CAN. Equation (11h) ensures that T_i^u for each $u \in U, i \in Z_u$ belongs to one cost class. If $\sum_{d\in D} x_{ud} = 0$ in (11b), the cost class whose cost value is zero is selected by (11a); (11i)-(11k) are treated similarly. Equation (11i) ensures that H_0^u for each $u \in U$ belongs to one cost class. Equation (11k) ensures that the sum of traffic allocated to $d \in D$, and T_{d}^u belongs to one cost class. Equation (11l) expresses prohibited pairs (*u, d*), where T_{d}^u is not allowed to be allocated to *d*. Equations (11m)-(11r) indicate that x_{ud}, y_u, z_{sui}^1, z_{su}^2, z_{su0}^3, and z_{sd}^4 are binary decision variables, respectively.

5) Optimization Problems Considering WAN Cost: We add the WAN costs to the objective functions of (11a) of the optimization problems described in Section III-C4. We assume that the WAN costs are the sum of the traffic amounts passing through a WAN multiplied by the weight between the two sites. The weight between the two sites is determined by considering the distance between them and administrative factors. Let w_{id}^u, w_{ij}^u, $w_{i\mathrm{e}}^u$, and $w_{d\mathrm{e}}$ denote the weights between campus *i* and data center *d*, between campuses *i* and *j* ($\neq$ *i*), between campus *i* and the Internet gateway of WAN e, and between data center *d* and the Internet gateway of WAN e.

We define the WAN costs of the NFV-based CAN between campus *i* of university *u* and data center *d*, which is denoted by g_{id}^u, as

$$g_{id}^u = (t_{i\mathrm{e}}^u + t_{\mathrm{e}i}^u) w_{id}^u x_{ud}, \forall i \in Z_u, u \in U, d \in D. \tag{12}$$

The WAN cost between *d* and Internet gateway e, which is denoted by $g_{d\mathrm{e}}$, is given by

$$g_{d\mathrm{e}} = \sum_{u\in U} T_{\mathrm{d}}^u w_{d\mathrm{e}} x_{ud}, \forall d \in D. \tag{13}$$

The WAN cost between campus *i* and campus *j* ($\neq$ *i*), which is denoted by g_{ij}^u, is given by

$$g_{ij}^u = \left(t_{ij}^u + t_{ji}^u\right) w_{ij}^u, \forall i, j (\neq i) \in Z_u, u \in U. \tag{14}$$

The sum of the WAN cost of the legacy CAN between the Internet gateway of the WAN e and the main campus of *u* and the WAN cost of the legacy CAN between the main campus and the sub-campuses, which is denoted by $h_{0\mathrm{e}}^u$, is given by

$$\begin{aligned} h_{0\mathrm{e}}^u = & \sum_{i\in Z_u} (t_{i\mathrm{e}}^u + t_{\mathrm{e}i}^u) w_{0\mathrm{e}}^u y_u \\ & + \sum_{j\in Z_u\backslash\{0\}} \left(t_{j\mathrm{e}}^u + t_{\mathrm{e}j}^u\right) w_{0j}^u y_u, \forall u \in U. \end{aligned} \tag{15}$$

Note that there is no traffic between sub-campuses $j (\neq 0) \in Z_u$ of $u \in U$ and the Internet gateway of the WAN e.

By using (12), (13), (14), and (15), the WAN costs for the combination of the NFV-based and legacy CANs, which is denoted by g_1, is given by

$$\begin{aligned} g_1 = & \sum_{u\in U} \left\{ \sum_{i\in Z_u} \left\{ \sum_{d\in D} g_{id}^u + \sum_{j\in Z_u\backslash\{i\}} g_{ij}^u \right\} + h_{0\mathrm{e}}^u \right\} \\ & + \sum_{d\in D} g_{d\mathrm{e}}. \end{aligned} \tag{16}$$

Note that an ISP peering cost must be paid in order to connect a WAN to the Internet. However, because the peering costs of the NFV-based CAN and legacy CAN are the same, as their amounts of Internet access traffic are the same, we will not include peering costs in the proposed model.

We formulate the optimization problem for minimizing the total costs in consideration of the WAN costs as follows.

$$\begin{aligned} & \text{Objective} \\ & \min \sum_{u\in i} \left\{ \sum_{i\in Z_u} \sum_{s\in S_1} c_s^1 z_{sui}^1 + \sum_{s\in S_2} c_s^2 z_{su}^2 + \sum_{s\in S_3} c_s^3 z_{su0}^3 \right\} \\ & \quad + \sum_{d\in D} \sum_{s\in S_4} c_s^4 z_{sd}^4 + g_1 \\ & \text{Subject to (11b)}-\text{(11r) and (12)}-\text{(16)}, \end{aligned} \tag{17a}$$

where g_{id}^u, g_{ij}^u, $h_{0\mathrm{e}}^u$, $g_{d\mathrm{e}}$, and g_1 are decision real-number variables.

6) Optimization Problems Considering Data Center Failures: A failure at a data center must not cause trouble for users allocated to it [25], [26]. To minimize the trouble from a failure, we prepare backup resources so that each user allocated to the failed data center can be protected by one of the other available data centers, which we call a "backup data center." For purposes of synchronization, a portion α_u ($0 \leq \alpha_u \leq 1$), which is a given parameter, of T_{d}^u must be reserved in a dedicated manner at the backup data center whether or not a failure occurs. We assume that multiple data centers will not fail at the same time.

Consider the optimization problems in Section III-C4. Let $b_{dd'}^u$ be a binary decision variable that is set to one in the case of $x_{ud'} = 1$, if $u \in U$ allocated to a failed data center $d' \in D$ is protected by an available data center $d \in D \backslash \{d'\}$, and zero otherwise. In the case of $x_{ud'} = 0$, $b_{dd'}^u$ is not considered.

The usage cost at the data center site, whose cost function is $f^4(t)$, includes the costs for the working and backup resources. Equation (11c) is replaced with the following constraints.

$$\sum_{u \in U} T_{\mathrm{d}}^u \left(x_{ud} + \sum_{d' \in D \backslash \{d\}} \alpha_u b_{dd'}^u \right) + B_d \leq \sum_{s \in S_4} z_{sd}^4 l_s^4, \forall d \in D \tag{18a}$$

$$\sum_{u \in U} (1 - \alpha_u) T_{\mathrm{d}}^u b_{dd'}^u \leq B_d, \forall d \in D, d' \in D \backslash \{d\} \tag{18b}$$

$$\sum_{d \in D \backslash \{d'\}} b_{dd'}^u \geq x_{ud'}, \forall u \in U, d' \in D \tag{18c}$$

$$b_{dd'}^u \in \{0, 1\}, \forall u \in U, d \in D, d' \in D \backslash \{d\} \tag{18d}$$

Equation (18a) indicates that the sum of working, dedicated backup, and shared backup resources [27], [28] belonging to cost class $s \in S_4$ must not exceed l_s^4, where $\sum_{u \in U} T_{\mathrm{d}}^u x_{ud}$ expresses the working resources for $u \in U$ allocated to $d \in D$, $\sum_{u \in U} T_{\mathrm{d}}^u \sum_{d' \in D \backslash \{d\}} \alpha_u b_{dd'}$ expresses the synchronized backup resources protected by $d \in D$ that are allocated to $d' \in D \backslash \{d\}$, and B_d expresses the shared backup resources protected by $d \in D$. Equation (18b) indicates that B_d is the maximum value of $\sum_{u \in U} T_{\mathrm{d}}^u b_{dd'}^u$ over $d' \in D \backslash \{d\}$. Equation (18c) guarantees that $u \in U$ allocated to failed data center $d' \in D$ is protected by one of the available data centers.

7) Direct Access Type of Legacy CAN: Consider a model that integrates NFV-based CANs and legacy CANs whose subcampuses access the Internet directly. In what follows, we will formulate an optimization problem to minimize the total cost of combining the NFV-based CANs and legacy CANs of the direct access type. The cost function $f^5(t)$ is the usage cost at the campus site that uses links, layer-2 switches, and routers. We assume that $f^5(t)$ is a non-decreasing step function, the same as $f^k(t)$, where $k \in [1, 4]$ is defined as in Section III-C1.

Objective

$$\min \sum_{u \in i} \sum_{i \in Z_u} \left(\sum_{s \in S_1} c_s^1 z_{sui}^1 + \sum_{s \in S_5} c_s^5 z_{sui}^5 + \sum_{s \in S_3} c_s^3 z_{sui}^3 \right) + \sum_{u \in i} \sum_{s \in S_2} c_s^2 z_{su}^2 + \sum_{d \in D} \sum_{s \in S_4} c_s^4 z_{sd}^4 \tag{19a}$$

Subject to (19b)

$$T_i^u \sum_{d \in D} x_{ud} \leq \sum_{s \in S_1} z_{sui}^1 l_s^1, \forall u \in U, i \in Z_u \tag{19c}$$

$$\sum_{u \in U} T_{\mathrm{d}}^u x_{ud} \leq \sum_{s \in S_4} z_{sd}^4 l_s^4, \forall d \in D \tag{19d}$$

$$T_0^u y_u \leq \sum_{s \in S_2} z_{su}^2 l_s^2, \forall u \in U \tag{19e}$$

$$T_i^u y_u \leq \sum_{s \in S_5} z_{sui}^5 l_s^5, \forall u \in U, i \in Z_u \backslash \{0\} \tag{19f}$$

$$Q_i^u y_u \leq \sum_{s \in S_3} z_{sui}^3 l_s^3, \forall u \in U, i \in Z_u \tag{19g}$$

$$\sum_{d \in D} x_{ud} + y_u = 1, \forall u \in U \tag{19h}$$

$$\sum_{s \in S_1} z_{sui}^1 = 1, \forall u \in U, i \in Z_u \tag{19i}$$

$$\sum_{s \in S_5} z_{sui}^5 = 1, \forall u \in U, i \in Z_u \tag{19j}$$

$$\sum_{s \in S_2} z_{su}^2 = 1, \forall u \in U \tag{19k}$$

$$\sum_{s \in S_3} z_{sui}^3 = 1, \forall u \in U, i \in Z_u \tag{19l}$$

$$\sum_{s \in S_4} z_{sd}^4 = 1, \forall d \in D \tag{19m}$$

$$x_{ud} = 0, \forall (u, d) \in G \tag{19n}$$

$$x_{ud} \in \{0, 1\}, \forall u \in U, d \in D \tag{19o}$$

$$y_u \in \{0, 1\}, \forall u \in U \tag{19p}$$

$$z_{sui}^1 \in \{0, 1\}, \forall s \in S_1, u \in U, i \in Z_u \tag{19q}$$

$$z_{su}^2 \in \{0, 1\}, \forall s \in S_2, d \in D \tag{19r}$$

$$z_{sui}^3 \in \{0, 1\}, \forall s \in S_3, u \in U, i \in Z_u \tag{19s}$$

$$z_{sd}^4 \in \{0, 1\}, \forall s \in S_4, d \in D \tag{19t}$$

$$z_{sui}^5 \in \{0, 1\}, \forall s \in S_5, d \in D \tag{19u}$$

Equation (19a) minimizes the total costs. Equation (19c) indicates that, when $u \in U$ adopts the proposed architecture, the traffic T_i^u, belonging to cost class $s \in S_1$, must not exceed l_s^1. Equation (19d) indicates that the sum of traffic allocated to data center $d \in D$, T_{d}^u, belonging to cost class $s \in S_4$, must not exceed l_s^4. Equation (19e) indicates that, when $u \in U$ adopts a direct sub-campus access CAN, T_0^u, belonging to cost class $s \in S_2$, must not exceed l_s^2. Equation (19f) indicates that, when $u \in U$ adopts a direct sub-campus access CAN, T_i^u, belonging to cost class $s \in S_5$, must not exceed l_s^5. Equation (19g) indicates that, when $u \in U$ adopts a direct sub-campus access CAN, the

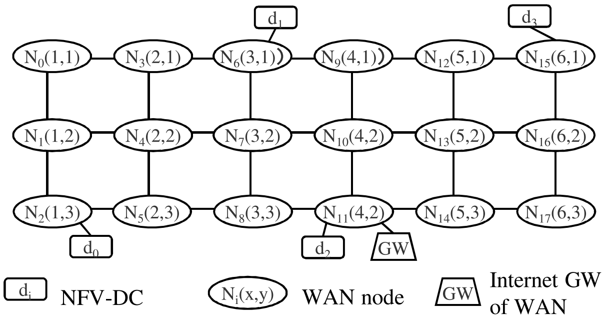


Fig. 9. 18-node ladder network.

traffic Q_i^u, belonging to cost class $s \in S_3$, must not exceed l_s^3. Equation (19h) indicates that the traffic of $u \in U$ can be allocated to at most one data center without splitting, and, otherwise, $u \in U$ adopts a direct sub-campus access CAN. Equation (19i) ensures that T_i^u for each $u \in U, i \in Z_u$ belongs to one cost class. If $\sum_{d \in D} x_{ud} = 0$ in (19c), the cost class whose cost value is zero is selected by (19a); similar explanations apply to (19j)-(19m). Equation (19j) ensures that T_i^u for each $u \in U, i \in Z_u$ belongs to one cost class. Equation (19k) ensures that H_0^u for each $u \in U$ belongs to one cost class. Equation (19l) ensures that Q_i^u for each $u \in U, i \in Z_u$ belongs to one cost class. Equation (19m) ensures that the sum of traffic allocated to $d \in D$, T_{d}^u belongs to one cost class. Equation (19n) expresses the prohibited pairs (*u, d*), where T_{d}^u is not allowed to be allocated to *d*. Equations (19o)-(19t) indicate that x_{ud}, y_u, z_{sui}^1, z_{su}^2, z_{sui}^3, and z_{sd}^4 are binary decision variables, respectively.

The parameters and decision variables used in this paper are summarized in Table I.

TABLE I
SUMMARY OF PARAMETERS AND DECISION VARIABLES

Parameters	Description
K_{D}	Number of DCs
K_{U}	Number of universities
t	Traffic amount
$f^k(t)$	Non-decreasing step function of k^{th} resources costs
S_k	Set of costs l_s^k, c_s^k
l_s^k	Traffic amount of sth step
c_s^k	Cost of sth step
U	Set of users or institutions
$u \in U$	Main campus
$n_u \in U$	Sub-campuses.
Z_u	Set of campuses in $u \in U$
t_{ij}^u	Traffic from campus $i \in Z_u$ to campus $j(\neq i) \in Z_u$
$t_{\mathrm{e}i}^u$($t_{i\mathrm{e}}^u$)	Traffic from the Internet to campus $i \in Z_u$(the opposite direction)
H_0^u	Access link traffic from a main campus to a WAN
T_i^u	Access link traffic from sub-campus to a WAN
$T_{i,\mathrm{up}}^u$	Traffic from sub-campus to a WAN
$T_{i,\mathrm{down}}^u$	Traffic from WAN to sub-campus
P_0^u	Traffic from/to a main campus to/from the Internet
C^{L}	Costs of a legacy network
C^{P}	Costs of the proposed network
T_{d}^u	Access link traffic from a data center to a WAN
D	Set of data centers
G	Set of prohibited pairs (u, d), university u is not moved to DC d
w_{id}^u	Weights between campus i and DC d
w_{ij}^u	Weights between campuses i and $j(\neq i)$
$w_{i\mathrm{e}}^u$	Weights between campus i and the Internet gateway of WAN e
$w_{d\mathrm{e}}$	Weights between data center d and the Internet gateway of WAN e.
$h_{0\mathrm{e}}^u$	The Internet communication WAN costs of legacy-based CAN between the main campus of u and GW e plus between the main campus and sub-campuses,
g_{id}^u	The Internet communication WAN costs of NFV-based CAN between i and d selected by u.
g_{ij}^u	Intra-campus communication WAN costs between i and j of u
$g_{d\mathrm{e}}$	WAN costs between d and e
g_1	WAN costs for the combination of the NFV-based and legacy CANs
α_u	Portion of synchronization
Variables	Description
x_{ud}	Binary decision variable, set to 1 when u is allocated to d
y_u	Binary decision variable, set to 1 u adopts a legacy network
z_{sui}^1	Binary decision variable, if T_i^u belongs to s
z_{su}^2	Binary decision variable, if H_0^u or T_0^u belongs to s
z_{sui}^3	Binary decision variable, if $P_{0\mathrm{e}}^u$ belongs to s
z_{sd}^4	Binary decision variable, if the sum of traffic allocated to d belongs to s
$b_{dd'}^u$	Binary decision variable, if u allocated to a failed data center $d'D$ is protected by available data center d

IV. EVALUATION WITH LADDER NETWORK

This section evaluates the cost reduction effect of the proposed optimization model, by focusing a simplified network to observe the trend of the results. We investigate two points: (i) the parameter dependency of the proposed model and (ii) the calculation time needed to solve an optimization problem.

A. Networks and Parameter Settings

1) Ladder Networks: To examine the parameter dependency, we will use a simple 18-node (3 × 6) ladder network, as shown in Fig. 9. This network represents a central part of SINET from Tokyo to Osaka. There are three different routes from Tokyo to Osaka and intermediate nodes are connected as ladder network. To investigate the calculation time to solve the optimization problem with proposed model, we will consider ladder networks with 36 (3 × 12) and 48 (4 × 12) nodes. Network sizes are decided while referring several networks for academia, including ESnet [29], GÉANT [30], Internet2 [31], and SINET [3]. This backbone networks have 21, 41, 44, and 50 nodes, respectively.

2) Parameter Settings: The proposed optimization model has four major parameters: (i) the topology of the university network, (ii) traffic amount, (iii) restriction on transmission latency, and (iv) cost functions of the resources and WAN.

The 18-ladder network consists of eighteen nodes ($N_0 - N_{17}$), as shown in Fig. 9. It has four data centers ($d_0 - d_3$) and one gateway (GW). Here, $N_i(x, y)$ indicates that node N_i is at position (*x, y*), and all fiber lengths between nodes are assumed to be of unit length. Each university, u_i, is accommodated in an N_i, and the total number of universities is thus 18. Each university has two sub-campuses, and each sub-campus is randomly located at a node adjacent to the one of the main campus. Traffic is set to $t_{ie} = 2T, t_{ei} =$

$t_{ij} = T, \forall i, j (\neq i)$. Here, T is measured in traffic amount units ranged from 1 to 100.

We introduce the prohibited pair condition to maintain the transmission latency between campuses and NFV-DCs within a certain value. The transmission latency mainly depends on physical fiber length along a route, as mentioned in Section III-A2. The prohibited pair are determined by the physical fiber length along the route, as follows. If the fiber length along a normal route (= the shortest route) between campus u and data center d is longer than a constant value, the pair is a prohibited. For example, suppose that the transmission latency caused by the fiber length = 5 [units] is not allowed; the CAN of u_0, which is accommodated in node N_0, is not migrated to the NFV-DC d_2 and d_3. This is because the fiber lengths between u_0 and d_2 and between u_0 and d_3 are each 5 [units].

The cost functions of the resources are non-decreasing step functions, $f^k(t)$, where $k \in [1, 4]$. We assume that $f^k(t)$ is obtained by using a continuous function, $w_k \times t^n$, where t is the traffic amount, w_k is the weight parameter, $k \in [1, 4]$, and n is a real number $(0 \leq n \leq 1)$. When n is close to one, we get little scale merit. On the other hand, when n is a small value, we get a large scale merit. The cost at the sth step, c_s^k, is $w_k \times (l_s^k)^n, s \in S_k$. The cost classes S_k are set to $\{0, 1, \ldots, 19\}$, $l_s^k = \{0, 10, 20, 30, 40, 50, 100, 200, 300, 400, 500, 1000, 2000, 3000, 4000, 5000, 10000, 20000, 30000\}$, where $s \in S_k$, and $k \in [1, 4]$. Weight parameters are set to w_1:w_2:w_3:w_4 = 3:8:10:18.

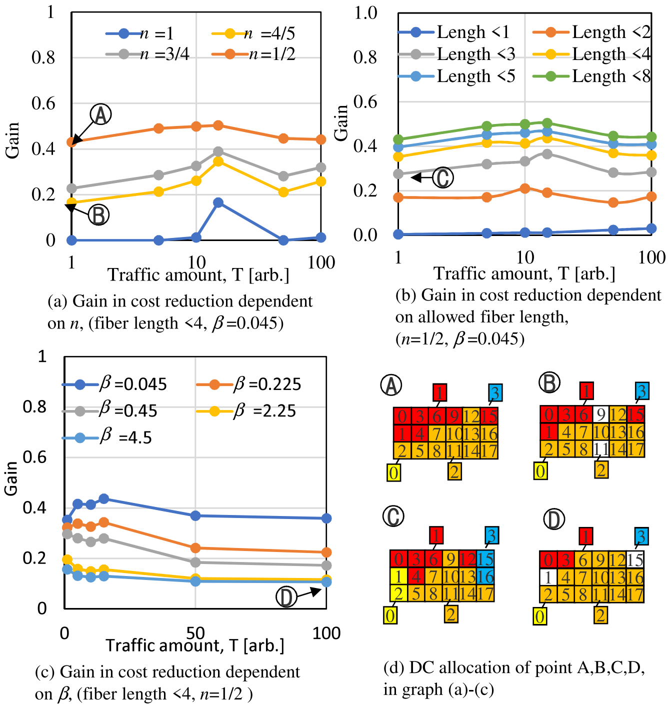
We assume that the weights of the parameters for the WAN costs, i.e., w_{id}^u, w_{ij}^u, and w_{ie}^u, and w_{de}, are proportional to the total fiber length of the route. The WAN costs are calculated using (12)-(14). Each weight is assumed to be $\beta \times$ $L(N_i(x_i, y_i), N_j(x_j, y_j))$. Here, $L(N_i(x_i, y_i), N_j(x_j, y_j))$ expresses the total fiber length of the route from a node $N_i(x_i, y_i)$ to a node $N_j(x_j, y_j)$. In the case of the ladder network, $L(N_i(x_i, y_i), N_j(x_j, y_j))$ is represented by $(|x_i - x_j| + |y_i - y_j|)$. If β is large, the WAN costs are relatively larger than the equipment costs. When β is small, the WAN costs are relatively smaller than equipment costs.

B. Parameter Dependency

Figure 10 shows the cost reduction effect of the proposed optimization model. We will analyze the total network costs represented as (17a) by using MILP. The gain (i.e., cost reduction) with the NFV-based CAN is defined by

$$Gain = 1 - \frac{\text{Total costs with NFV-based CAN}}{\text{Total costs with only legacy CAN}}.$$

Figure 10 shows (a) the dependency on n, which is a parameter of the equipment cost function, (b) effect of the transmission latency restriction with prohibited pairs, which is determined by the fiber length, and (c) β, which, as described in Section IV-A2, is used for evaluating the WAN and equipment costs. Figure 10(a) shows gain for n = 1, 4/5, 2/3, and 1/2. In smaller n is, larger gain becomes, reaching about 40-50% for n = 1/2, because the scale cost merit is larger at smaller n.



(a) Gain in cost reduction dependent on n, (fiber length <4, β=0.045)

(b) Gain in cost reduction dependent on allowed fiber length, (n=1/2, β=0.045)

(c) Gain in cost reduction dependent on β, (fiber length <4, n=1/2)

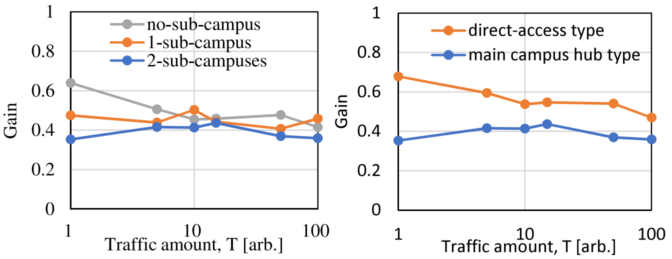
(d) DC allocation of point A,B,C,D, in graph (a)-(c)

Fig. 10. Cost reduction depending on amount of traffic.

Figure 10(b) shows the transmission latency restriction dependency. When the restriction is strong, for example, fiber length < 1, a university can move its ICT equipments only to a data center connected to the same node. In this case, universities do not move to a data center and the gain becomes small. When the restriction is weak, for example, fiber length < 8, universities can select a DC regardless of latency and concentrated there resources into one data center. Accordingly, gain becomes high.

Figure 10(c) shows the dependency of the WAN costs relative to the equipment costs for various values of β. As β increases, the gain decreases. At large β, the ratio of WAN costs to equipment costs becomes large and the gain of NFV-based CAN is reduced by the additional WAN cost. When β is small, the WAN costs are relatively smaller than the equipment costs. In this case, the gain of NFV-based CAN becomes high.

Figure 10(d) shows the DC allocations of each CAN connected to each node at points A, B, C, and D in Figs. 10(a–c). Each rectangle indicates a university, and the color of the rectangle is the corresponding data center that the university migrates to. The colors of d_0, d_1, d_2, and d_3 are yellow, red, orange, and light blue, respectively. No color indicates that the university does not migrate to a data center. At point A, all universities adopt the NFV-based CAN and migrate to two DCs, d_1 and d_2. At point B, the scale merit of the equipment costs is lower and u_9 and u_{11} do not move their equipments to a data center. This is because the cost increases as a step-function. If u_9 and u_{11} move to a data center, total costs go up one higher step. In this case, a few universities remain on their legacy CAN. At point C, universities are distributed to four data centers, because the transmission latency restriction is strong. In this case, the scale merit and gain are lower. At



(a) Gain in cost reduction comparison with number of sub-campus, fiber length<4

(b) Gain in cost reduction comparison direct access type to main campus hub type, 2 sub-campuses, fiber length <4

Fig. 11. Cost reduction depending on number of sub-campuses and legacy CAN types.

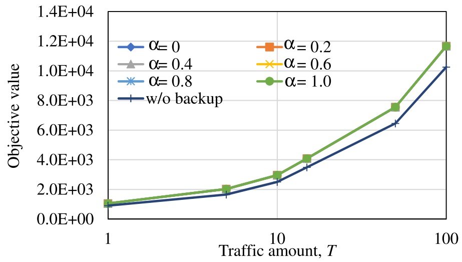


Fig. 12. Increasing cost depending on fault recovery.

TABLE II
CALCULATION TIME

Network	Mean [sec]	Deviation [sec]
18 nodes/18 universities	0.023	0.0025
36 nodes/36 universities	0.127	0.1088
48 nodes/48 universities	0.218	0.3169

point D, the WAN costs are relatively higher than the equipment costs. In this case, the higher WAN costs surpass the cost reduction effect of the NFV-DC. Note that two data centers are selected and most of the universities move their equipments to the data centers. However u_1 and u_{15} do not adopt the NFV-based CAN. These universities have a longer WAN route to the data centers and their WAN costs are relatively high. Thus, u_1 and u_{15} do not move to a data center.

C. Dependence of Cost on Number of Sub-Campuses

Figure 11(a) shows the gain depending on the number of sub-campuses. Here, the traffic T varies from 1 to 100, β is 0.045, and the number of sub-campuses varies from zero to two. Here each sub-campus is randomly located on a node adjacent to the main campus. The gain with sub-campuses is slightly lower than that with no sub-campus. As the number of sub-campuses increases, the traffic amount increases. Moreover, as the traffic amount increases, the WAN cost increases while that of the CANs and DCs remains low. Thus, the gain of NFV-based CANs becomes slightly lowered relatively.

D. Direct Access Type of Legacy CAN

Figure 11(b) shows the gain with the direct access type of legacy CANs relative to the main campus hub type of legacy CAN. Here, T ranges from 1 to 100, and β for the WAN cost parameter is 0.045. In this case, the gain from the direct access type is larger than that from the main campus hub type because the equipment costs of a sub-campus increase when sub-campuses access the Internet via their own firewall directly. Thus, the gain of a direct access sub-campus legacy CAN is larger than that with a dependent access sub-campus legacy CAN.

E. Increasing Cost With Fault Recovery Capability

Figure 12 shows the calculated objective values with/without the fault recovery capability depending on the traffic amount. Here, the ratio of dedicated backup and shared backup resources, α, ranges from 0 to 1, and T ranges from 1 to 100. β is 0.045. The objective values in the case of the fault recovery capability are slightly larger than those without the capability. The objective values are the same whenever the α values are different. The reason is given next. The cost of the data center increases depending on the amount of traffic with a non-linear step function. As the amount of traffic increases, the width of the step increases. Thus, the data centers' costs become the same even when there are different amounts of backup resource for different α values. From this result, we can say that the fault recovery capability for $\alpha = 1$ will be sufficient for evaluating the cost gain because the amount of backup resources is largest for $\alpha = 1$.

F. Calculation Time

We evaluated time needed to solve the optimization problem for 36 (3 × 12) and 48 (4 × 12) -node ladder networks. In particular, we evaluated the calculation time with MILP, IBM, ILOG, CPLEX, and Interactive Optimizer 12.7.1.0. The evaluation was performed on a virtual machine (OS: Centos, release version 7.4.1708) [32]. The virtual machine was run on a computer with a 2.4-GHz Intel Core i7-5500U, and the host OS was Windows 10. The calculation times were evaluated for six combinations in a ladder network. The six combinations were two traffic amounts and three fiber lengths for the prohibited pair condition. The two traffic amounts, T, were set to 1 and 50. The three fiber lengths were set to be 1, 4, and 8, with $\beta = 0.025$ for each T.

Table II shows the mean and standard deviation of the calculation times for the six combinations. This result indicates that the proposed model yields a solution in a practical time in the examined networks.

V. SINET-BASED EVALUATION

We evaluated the effect of the proposed optimization model in a more practical setting based on SINET.

A. Example of Procurement Process and Use Case of the Proposed Model

Consider that there are six steps in a joint procurement. (i) Universities are invited to a joint procurement. (ii) Information about the traffic amount, CAN costs, and the transmission latency restrictions of each university is gathered.

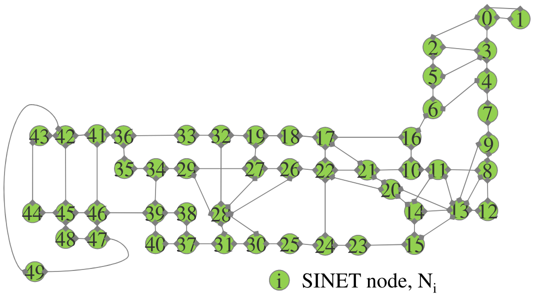


Fig. 13. SINET logical topology.

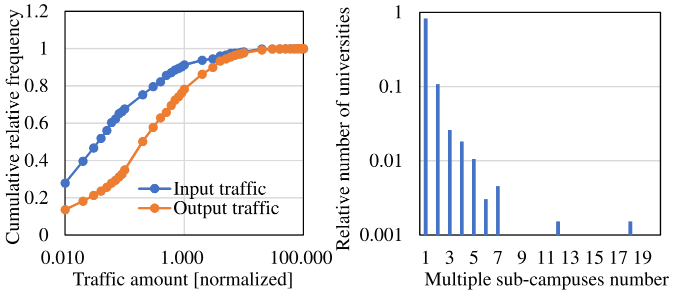
(iii) Cloud providers are sent requests for information (RFI) regarding DC costs depending on traffic. (iv) Cost functions (CAN costs, DC costs) are estimated from the gathered information. (v) The proposed model is used to find an optimal combination of DCs and universities. If a gain is expected from using NFV-based CAN, the number of DCs, the location of each DC, and the traffic amount of each DC are determined. Finally, (vi) requests for proposal (RFP) to provide a private cloud has the optimal the number, location, and traffic amount of DCs are sent.

B. Network and Parameter Settings

1) Current SINET Network Topology: Here, we evaluated the proposed model on subset (50 nodes; $N_0 - N_{49}$) of SINET as shown in Fig. 13. The access links of the universities are accommodated by these 50 SINET nodes. The Internet Gateway (GW) of SINET is located on the Tokyo node. The distance between nodes is determined by the total physical length of fiber between them.

2) Conditions of Universities: There are 660 universities that have their own dedicated access links connected to SINET (see There are some universities that connect to SINET via a commercial shared network service.). The total number of dedicated access links is 880. The traffic amounts through each of these access links were measured, and the amounts were used for the evaluation with the proposed model. Figure 14(a) shows the cumulative relative frequency of the measured access link traffic. The horizontal axis represents the access link traffic divided by the mean of the measured traffic amounts of the 880 access links. The vertical axis represents the cumulative relative frequency. It indicates that the relative number of universities whose traffic amounts are smaller than or equal to the value of the horizontal axis. The traffic amount, measured from August 1 to August 22, 2017, was used for the evaluation. Several universities have multiple sub-campuses. Figure 14(b) shows the relative histogram of universities correlated with the sub-campus number. The horizontal axis represents the number of sub-campuses, a, and the vertical axis represents the ratio of universities that have a sub-campuses to all universities. This indicates that over 10% universities have multiple sub-campuses.

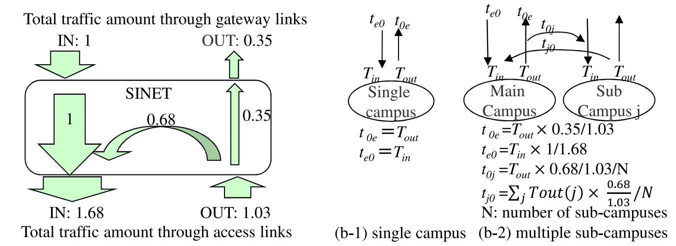
3) Parameter Estimation: Suppose that a certain number of universities apply for a joint procurement, and we can get information about the input/output traffic amount of each university (see Figure 14(a)). We need to know the amount of intra sub-campus traffic. The intra sub-campus traffic of the universities that have multiple sub-campuses is estimated as follows. We measure the input and output traffic of each access link. Some of the traffic is Internet access traffic, and the rest is intra sub-campus traffic. To estimate the amount of intra sub-campus traffic, we use the traffic exchange ratio of SINET shown in Fig. 15(a). On the basis of this exchange ratio, the intra sub-campus traffic is calculated as shown in Fig. 15(b). We set the parameters, t_{ie}, t_{ei}, and t_{ij}, in accordance with the measured traffic amount.



(a) Cumulative relative frequency of the measured access link traffic

(b) Relative histogram of universities correlated with the sub-campus number

Fig. 14. Cumulative relative frequency of measured access link traffic of universities and relative histogram of universities correlated with the sub-campus number.


Total traffic amount through gateway links
IN: 1
OUT: 0.35
SINET
1
0.68
0.35
IN: 1.68
OUT: 1.03
Total traffic amount through access links
t_{e0}
t_{0e}
T_{in}
T_{out}
Single campus
$t_{0e} = T_{out}$
$t_{e0} = T_{in}$
t_{0j}
t_{j0}
Main Campus
Sub Campus j
$t_{0e} = T_{out} \times 0.35/1.03$
$t_{e0} = T_{in} \times 1/1.68$
$t_{0j} = T_{out} \times 0.68/1.03/N$
$t_{j0} = \sum_j Tout(j) \times \frac{0.68}{1.03}/N$
N: number of sub-campuses
(b-1) single campus
(b-2) multiple sub-campuses

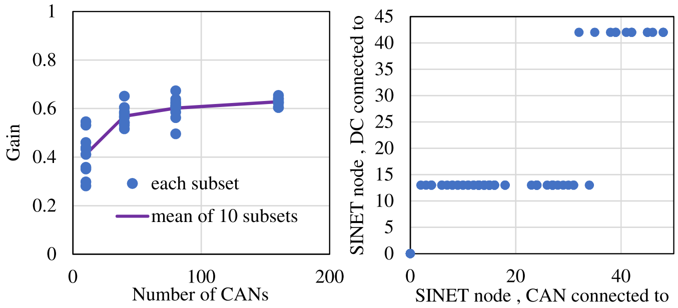
(a) Traffic exchange over SINET Traffic amount is normalized by IN traffic of gateway links

(b) Amount of intra-campus traffic exchange in a multiple sub-campuses university

Fig. 15. Intra sub-campus traffic assumption.

The CAN and DC costs are estimated as follows. We request information about the costs of the elements of the CAN and DC, i.e., the access link cost, C_t^l, router cost, C_t^r, layer-2 switch cost, C_t^s, firewall cost, C_t^f, and application cost, C_t^a. Note that the costs depend on the traffic amount, $t \in T_{\text{sample}}$, where T_{sample} is a set of traffic amounts. We assume that a cost function, $f^k(t)$, is obtained by using a continuous function, $w_k \times t^{n_k}$, where $k \in [1, 4]$, t is the traffic amount, w_k is the weight parameter of each element, and n_k is a real number ($0 \leq n_k \leq 1$). For example, the usage costs at a campus site that uses links and layer-2 switches, $f^1(t)$, is obtained by using $w_1 \times t^{n_1}$. We can get w_1 and n_1 by fitting the data set, (t, $C_t^l + C_t^s$), $t \in T_{\text{sample}}$ to the function, $w_1 \times t^{n_1}$. After that, the step function cost c_s^1 is set to $w_1 \times (l_s^1)^{n_1}$. Here, the sets of cost classes are such as l_s^1, $s \in S_k$. The other functions, $f^k(t)$, where $k = 2$, 3, and 4, are treated similarly.

The prohibited pairs are determined as follows. In the case that a university requests that the transmission latency be under 5 ms (one way), a pair of NFV-DC and the university, whose distance is longer than the 1000 km is a prohibited pair. The distance between the DC and the university is the total optical



(a) Gain dependence on number of universities

(b) Selected data center corresponding to each university

Fig. 16. Cost reduction comparison with two legacy CANs.

fiber length along a physical route from the university to the DC. Note that if other university and DC combinations are prohibited for other reasons, they can be added to the prohibited pair condition.

It is assumed that the WAN costs are proportional to the traffic amount t and the length of actual real optical fiber, $L(N_i, N_j)$. Therefore the WAN cost is represented as $\beta \times L(N_i, N_j) \times t$. For example, suppose that a WAN cost of 10 [unit] is charged to carry 1 [unit] traffic amount per 100 km of fiber. In this case, β is 10/1/100=0.001.

Currently, 21 cloud providers connect their data centers to SINET. Thus, these data centers are candidate for NFV-cloud DCs. In addition, the data centers on which the SINET nodes are deployed are candidates.

C. Cost Reduction Depending on Number of Universities

Figure 16(a) shows the gain with the proposed model for the main campus hub type shown in Fig. 2 without fault recovery capability. We analyzed the total network costs represented as (17a) by using MILP. $\beta = 0.001$ and cost functions are the same as those described in Section IV-A2 with n=1/2. The transmission latency is restricted to be within 5 ms. There are 11 candidate DCs that connect to nodes $N_0, N_{10}, N_{11}, N_{13}, N_{15} N_{19}, N_{21}, N_{28}, N_{29}, N_{42}$, and N_{43}. These locations are the same as the data centers where current cloud providers connect to. We evaluate the gains defined in Section IV-B for various numbers of universities, where we set K_{U} to 10, 40, 80, and 160. We set subsets of the sampled universities, which consist of K_{U} universities randomly extracted from the 660 universities. We evaluate the gains ten times with ten different subsets of each K_{U}; the gain strongly depends on the combination of universities. In Fig. 16(a), each dot represents the gain for each subset, and the line represents the mean of the ten gains with ten different subsets of the same K_{U}. The mean and standard deviation of 10 gains with different subsets of the same K_{U} are as follows; K_{U}, the average of gains, the stranded deviation of gains) = (10, 0.41, 0.085), (40, 0.57, 0.038), (80, 0.60, 0,045), (160, 0.63, 0.015). The larger K_{U} is, the greater the gain becomes. In addition, the variance decreases as the number of universities increase. This is because, in the case of many universities, the gain statistically converges. Figure 16(b) shows the selected DC corresponding to each university in the subset of $K_{\mathrm{U}} = 80$. The horizontal axis represents the SINET node to which that university is connected, and the vertical axis represents the SINET node to which that university is moved. Dot (*p*, *q*) represents that a university connected SINET node *p* (horizontal axis) moves to a DC connected SINET node *q* (vertical axis). This result shows three DCs (N_0, N_{13}, N_{48}) are selected and each university is accommodated in one of three DCs. Therefore, we can procure three DCs for 80 universities.

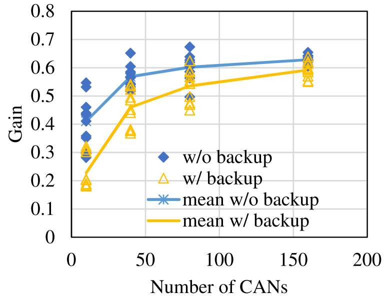


Fig. 17. Increasing cost depending on fault recovery.

D. Cost Reduction for Fault Recovery

We evaluated the gain of the NFV-based CAN in comparison with the legacy CANs of the main campus hub type with the fault recovery capability. Figure 17 shows the gain depending on the number of sampled universities, K_{U}. We selected ten different subsets, the same as in the previous sections, and assumed the condition described in Section V-C. The gain with fault recovery is slightly lower than that without fault recovery. That is, the gain does not deteriorate much. Thus, we can expect that allocating backup resources will be effective for fault recovery with NFV-based CANs.

VI. Conclusion

We proposed an optimization model for designing multiple NFV-based CANs. Organizations, such as universities and research institutions, have their own campus ICT equipment, and many would like to move this equipment to an NFV-DC for the sake of improving reliability and resiliency. However, NFV is not affordable because data transmission costs are higher with a cloud. One solution is for multiple organizations to procure NFV-DC resources together. This reduces the costs they have to pay individually for the resources of the NFV and cloud. There are planning issues when choosing optimal NFV-DC locations. The proposed model minimizes the total network costs of multiple organizations, including the WAN costs. The model was formulated using MILP. The effect of cost minimization was evaluated in a ladder network and a practical SINET based network. The gains of the proposed model were up to 55% in a ladder network. The mean and standard deviation were as follows: (number of nodes, mean calculation time, standard deviation of calculation time) (18, 0.023, 0.0025), (0.127, 0.108), and (0.218, 0.317). The results indicate that the calculation time is short enough and the proposed model is useful in practical cases. In particular the model can reduce the costs in the SINET based network by up to 63%. The mean and standard deviation of 10 gains with different subsets of the same $K_{\rm U}$ were as follows: ($K_{\rm U}$, the average of gains, the stranded deviation of gains) = (10, 0.41, 0.085), (40, 0.57, 0.038), (80, 0.60, 0,045), (160, 0.63, 0.015). Gain increases as $K_{\rm U}$ increases. Also, the more universities there are, the smaller the variance becomes. The gain converges with a sufficient number of universities. We also showed that additional costs for fault recovery can be suppressed. These results should encourage organizations to deploy NFV-based CANs.

Acknowledgment

The authors thank all members of the Organization of Science Network Operations and Coordination for their support of SINET. They are also grateful to all members of NII's SINET team for their continuous cooperation.

References

[1] S. Urushidani *et al.*, "Design of versatile academic infrastructure for multilayer network services," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 3, pp. 253–267, Apr. 2009.

[2] S. Urushidani *et al.*, "New directions for a Japanese academic backbone network," *IEICE Trans. Inf. Syst.*, vol. 98, no. 3, pp. 546–556, 2015.

[3] T. Kurimoto *et al.*, "SINET5: A low-latency and high-bandwidth backbone network for SDN/NFV era," in *Proc. IEEE Int. Conf. Commun.*, 2017, pp. 1–7.

[4] Z. D. Stephens *et al.*, "Big data: Astronomical or genomical?" *PLoS Biol.*, vol. 13, no. 7, Jul. 2015, Art. no. e1002195. [Online]. Available: http://journals.plos.org/plosbiology/article/file?id=10.1371/journal.pbio.1002195&type=printable, doi: 10.1371/journal.pbio.1002195.

[5] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, document SP 800-145, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Sep. 2011.

[6] "Network functions virtualization," Sophia Antipolis, France, ETSI, White Paper, Oct. 2014. [Online]. Available: https://portal.etsi.org/NFV/NFV_White_Paper.pdf

[7] Q. Duan, N. Ansari, and M. Toy, "Software-defined network virtualization: An architectural framework for integrating SDN and NFV for service provisioning in future networks," *IEEE Netw.*, vol. 30, no. 5, pp. 10–16, Sep./Oct. 2016.

[8] R. Mijumbi *et al.*, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.

[9] S. Togawa and K. Kanenishi, "Live migration destination selecting method for disaster recovery on e-learning environment," in *Proc. Int. Conf. Big Data Smart Comput. (BigComp)*, 2016, pp. 149–156.

[10] M. Pokharel, S. Lee, and J. S. Park, "Disaster recovery for system architecture using cloud computing," in *Proc. IEEE/IPSJ 10th Int. Symp. Appl. Internet (SAINT)*, Seoul, South Korea, 2010, pp. 304–307.

[11] T. Kurimoto *et al.*, "Multi-campus ICT equipment virtualization architecture for cloud and NFV integrated service," in *Proc. IEEE CoDit*, Apr. 2017, pp. 0615–0620.

[12] J. G. Herrera and J. F. Botero, "Resource allocation in NFV: A comprehensive survey," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 3, pp. 518–532, Sep. 2016.

[13] T. Kurimoto, H. Yamada, U. Shigeo, and E. Oki, "Optimization model for designing multiple virtualized campus area networks coordinating with wide area network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[14] *National Security Agency, Central Security Service*. Accessed: Sep. 28, 2018. [Online]. Available: http://www.nsa.gov/

[15] G. Suciu, E. G. Ularu, and R. Craciunescu, "Public versus private cloud adoption—A case study based on open source cloud platforms," in *Proc. 20th Telecommun. Forum (TELFOR)*, 2012, pp. 494–497.

[16] H. Matsumura, "SINET5 launch," in *Proc. 42nd Asia–Pac. Adv. Netw. Meetings Netw. Eng. Workshop*, Aug. 2016. [Online]. Available: http://www.jp.apan.net/meetings/1608-HK/index.html

[17] *Openstack*. Accessed: Sep. 28, 2018. [Online]. Available: https://www.openstack.org/

[18] *Open Source MANO, ETSI*. Accessed: Sep. 28, 2018. [Online]. Available: https://osm.etsi.org/images/OSM-Whitepaper-TechContent-ReleaseONE-FINAL.pdf

[19] T. Kurimoto, "SINET5, R&E network for Japan, and NFV service trial," in *Proc. 46th Asia–Pac. Adv. Netw. Meetings Cloud Working Group*, Aug. 2018. [Online]. Available: https://apan.net/meetings/apan46/activity.php?id=11#sn1

[20] M. Veeraraghavan *et al.*, " Network function virtualization: A Survey," *IEICE Trans. Commun.*, vol. E100-B, no. 11, pp. 1978–1991, Nov. 2017.

[21] M. C. Luizelli, L. R. Bays, L. S. Buriol, M. P. Barcellos, and L. P. Gaspary, "Piecing together the NFV provisioning puzzle: Efficient placement and chaining of virtual network functions," in *Proc. IEEE IM*, Ottawa, ON, Canada, 2015, pp. 98–106.

[22] M. Xia, M. Shirazipour, Y. Zhang, H. Green, and A. Takacs, "Network function placement for NFV chaining in packet/optical datacenters," *J. Lightw. Techol.*, vol. 33, no. 8, pp. 1565–1570, Apr. 15, 2015.

[23] W. Rankothge, J. Ma, F. Le, A. Russo, and J. Lobo, "Towards making network function virtualization a cloud computing service," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, 2015, pp. 89–97.

[24] L. Kleinrock, *Queuing Systems Volume I: Theory*. New York, NY, USA: Wiley, 1975, pp. 94–99.

[25] M. T. Gardner *et al.*, "Creating network resilience against disasters using service level agreements," in *Proc. 12th Int. Conf. Design Rel. Commun. Netw. (DRCN)*, Mar. 2016, pp. 62–70.

[26] M. Johnston, H.-W. Lee, and E. Modiano, "A robust optimization approach to backup network design with random failures," *IEEE/ACM Trans. Netw.*, vol. 23, no. 4, pp. 1216–1228, Aug. 2015.

[27] W. D. Grover, *Mesh-Based Survivable Transport Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[28] L. Guo, H. Yu, and L. Li, "Segment shared protection for survivable meshed WDM optical networks," *Opt. Commun.*, vol. 251, nos. 4–6, pp. 328–338, 2005.

[29] *ESnet*. Accessed: Sep. 28, 2018. [Online]. Available: http://es.net/about/

[30] *GÉANT*. Accessed: Sep. 28, 2018. [Online]. Available: https://www.geant.org/

[31] *Internet2*. Accessed: Sep. 28, 2018. [Online]. Available: http://www.internet2.edu/

[32] (Mar. 2018). *CPLEX Optimizer*. [Online] http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/

Takashi Kurimoto is an Associate Professor with the National Institute of Informatics, Japan. He worked for NTT from 1996 to 2014, where he was engaged in both network planning and research and development of next generation network. He is currently involved in the design and implementation of national research and educational network. He has been engaged in researching the switching technology for high-speed computer networks and the next generation network.

Shigeo Urushidani is currently a Deputy Director General and a Professor with the National Institute of Informatics (NII), Japan. He worked for NTT from 1985 to 2006, where he was engaged in the research and development of ATM, AIN, IP/MPLS, and optical switching systems. He moved to NII in 2006 and is currently involved in the design and implementation of the science information network, as well as in the research and development on future network architectures.

Eiji Oki is a Professor with the Graduate School of Informatics, Kyoto University, Kyoto, Japan. He was with Nippon Telegraph and Telephone Corporation Laboratories, Tokyo, from 1993 to 2008, and the University of Electro-Communications, Tokyo, from 2008 to 2017. His research interests include routing, switching, protocols, optimization, and traffic engineering in communication and information networks.