IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 31, 2019, accepted April 22, 2019, date of publication May 8, 2019, date of current version May 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2915374

Resource-Efficiently Survivable IoT Services Provisioning via Virtual Network Embedding in Fiber-Wireless Access Network

YEJUN LIU[1], PENGCHAO HAN[2], JIAN HOU[2], AND JIANBO ZHENG[3]

[1]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2]School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
[3]Guangdong Provincial Key Laboratory of Computer Vision and Virtual Reality Technology, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China

Corresponding author: Jianbo Zheng (jb.zheng@siat.ac.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61775033, Grant 61501104, Grant 61801063, and Grant 61771120, in part by the Fundamental Research Funds for the Central Universities under Grant N161608001, in part by the National Natural Science Foundation of China, CAS Key Technology Talent Program, through the Shenzhen Technology Project, under Grant JSGG20170413171746130 and Grant JCYJ20180507182610734, and in part by the Shenzhen Engineering Laboratory for 3D Content Generating Technologies under Grant [2017]476.

ABSTRACT Fiber-Wireless (FiWi) access network is a promising network architecture to provide the constantly available connections for the collaboration of objects in the Internet of Things (IoT). The network virtualization is dominating the evolution of FiWi, i.e., virtualized FiWi access network, which shields the difference between wireless and optical subnetworks and enables the customized transmission of different types of the IoT services in a common substrate network. However, the differences between optical and wireless subnetworks pose severe obstacle on their interoperability of resource allocation. In this paper, we focus on the survivable virtual network embedding (SVNE) in the FiWi access network for the purpose of the robust IoT service provisioning even in the scenario of network component failure. Each type of the IoT service is carried on one virtual network (VN), which is characterized by not only computing the resource and bandwidth resource demands but also the connection availability requirement. A connection availability model is proposed as an indicator of the network survivability and the IoT service robustness. We aim to allocate the resource for each VN with the resource cost minimized. The optimization problem of resource allocation is formulated in the integer linear programming (ILP) model that is solved for the optimal solution in a small-scale network. A heuristic algorithm is further put forward to facilitate the use of the proposed SVNE mechanism in a large-scale network. The simulation results verify that the proposed SVNE mechanism gains significant advantages in lower resource redundancy and higher acceptance ratio of VNs.

INDEX TERMS Internet of Things, fiber-wireless access network, network virtualization, virtual network embedding, connection availability.

I. INTRODUCTION

The Internet of Things (IoT) has been gaining ever-increasing attentions from both academic and industrial communities and is expected to be one of the dominating traffic in future Internet. It is anticipated that the number of IoT devices will reach up to 18 billion in 2020. The massive IoT scale will promote the collaboration among different objects and thus involve huge traffic data [1], which imposes severe challenges on the fronthaul/backhaul transmission techniques. Fiber-Wireless (FiWi) access network, which perfectly combines the advantages of wireless access network at front-end and optical access network at backend [2]–[5], is regarded as one of the most promising candidates for next generation fronthaul/backhaul networks. Specifically, FiWi access network can not only achieve flexible network access with high reliability for IoT services, but also improve network survivability due to the feasibility of resource rescheduling, such as wireless rerouting [6]. A typical architecture of FiWi access network is shown in Fig. 1. The optical back-end,

The associate editor coordinating the review of this manuscript and approving it for publication was Chunsheng Zhu.

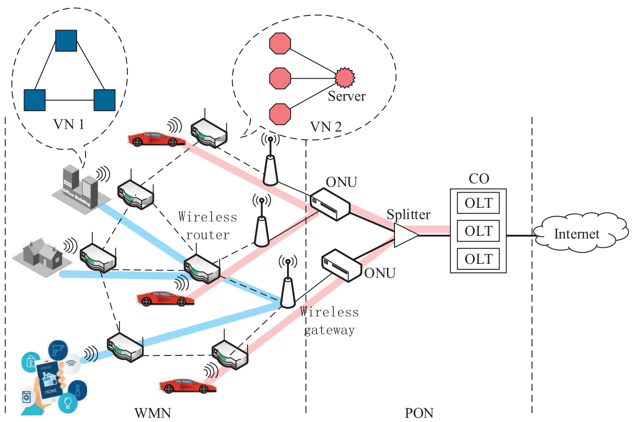


FIGURE 1. IoT services in virtualized FiWi access network.

which is a tree-like topology including Optical Line Terminal (OLT) locating in Central Office (CO), splitter and Optical Network Units (ONUs), is responsible for the high-rate and long-distance signal transmission from/to backbone network. The Wireless Mesh Network (WMN) at the front-end is composed of flat-deployed wireless routers, each of which is equipped with a single or multiple radio interfaces such that the IoT service can be provided for end users anytime and anywhere. Although FiWi access network can achieve the advantageous complementation of optical and wireless subnetworks, the seamless integration of both subnetworks is difficult to realize for the reason that there are great differences in their independent protocols, leading to extra time for data format transformation and unnecessary complexity for network management and control. Moreover, since different computation-demanding IoT services have different Quality of Service (QoS) requirements, FiWi access network is turning out to be ossified [7], making it hard to support differentiated IoT services.

Network virtualization is an effective solution for the problem of network ossification and global resource optimization in FiWi [8]–[13] due to the separated Infrastructure Provider (InP) and Service Provider (SP). Specifically, by abstracting the substrate network and providing the customized services to SPs, the physical details of Substrate Network (SN) are transparent to SPs. Thus, the virtualization of FiWi access network can shield the differences between wireless and optical subnetworks, while simplifying the network control and management and guaranteeing security through resource isolation. Moreover, multiple SPs, that are responsible for different IoT services, can coexist on a shared SN and each SP is able to deploy Virtual Networks (VNs) according to its specified service level agreement privately and independently. Therefore, the virtualized FiWi access network becomes more flexible and suitable for IoT service provisioning.

Despite the advantages of virtualized FiWi access network for IoT, there are still challenges for the implementation of network virtualization in FiWi. The problems of QoS guarantee and energy-efficient network design can be tackled easily due to the centralized service scheduling in network virtualization, while the survivable planning of FiWi is still an open issue, particularly the survivability against link failure. Because link failure occurs more frequently than node failure and most of the node failure cases can be transformed into link failure. The survivability issue in FiWi access network focuses mostly on the scenario of link failure. There have been many works for the survivability of FiWi access network [14], [15] leveraging the wireless rerouting. However, the Survivable Virtual Network Embedding (SVNE), which aims to construct survivable VNs by making efficient use of underlying resources while satisfying constraints of VNs [8] remains less mentioned in virtualized FiWi access network. As for the SVNE problem itself, related works focused mostly on the virtualization of backbone network and considered less about the hybrid architecture of wireless and optical access networks [16]–[18].

The challenges of SVNE in virtualized FiWi access network mainly include the complexity of failures in heterogeneous links and the need for high resource efficiency. First, traditional fault recovery strategy is no longer suitable for virtualized FiWi. The main idea for the problem of survivable resource allocation is to reserve a backup link (or path) for each working link (or path) during resource reservation stage. When the working path is interrupted, traffic will be switched to the reserved backup path immediately. However, there is a high probability of simultaneous failures on multiple physical links in FiWi access network due to the internal and external factors such as co-channel interference and time-varying channel condition in wireless subnetwork. It is unpractical to set one link as the backup of another since they may breakdown at the same time. Moreover, from the perspective of virtualization, due to the limitation of SPs in controlling physical resources, it is hard for SP to construct backup paths dynamically for interrupted services by using limited resources or requiring new resources from InP. Thus, the traditional 1+1 protection [16], [19] and dynamic recovery strategy [20] become less efficient in virtualized FiWi. The survivability of VNs is mainly limited by the availability of virtual links, which is dependent on the connection availability of embedded physical path, especially the wireless multi-hop path [21], [22]. Hence, a connection availability model is needed to quantify the demand of VN operator in survivability and serves as a guideline for the embedding of survivable VNs.

In our earlier work [23], we have studied the SVNE problem based on connection availability and verified the effectiveness of connection availability in reducing resource redundancy. However, there are still some challenging issues in terms of resource underutilization unsolved. To be specific, although the reservation of backup virtual resource can recover the interrupted traffic instantly, it suffers from the underutilization of resource because the backup virtual resource remains idle before a interruption occurs. Generalized strategy for improving resource utilization is the resource sharing between different backup virtual links (or paths) [16]–[18]. As long as the working virtual paths are geographically disjoint, their backup virtual paths can share the network resource with each other. However, the above resource sharing mechanism is not suitable for virtualized FiWi access network, because two geographically disjoint wireless links possibly break down at the same time due to the poor availability of wireless links. Therefore, a customized resource sharing mechanism should be invented for the survivable embedding of VNs in FiWi access network. Owing to the flexibility of resource scheduling in virtualized FiWi access network including bandwidth resource and wireless channels, there is an opportunity to improve resource utilization by introducing a more fine-grained resource sharing in terms of wireless channels.

In this paper, we address the SVNE problem in FiWi access network for the purpose of robust collaboration of IoT services. The survivability of each VN is guaranteed by reserving backup virtual path with connection availability requirement satisfied for each working virtual link. Unlike previous works, for each virtual link, backup virtual path does not have to be strictly disjoint from working virtual path as long as their combined connection availability meets the connection availability requirement. Therefore, the cost of virtual network embedding can be effectively reduced by utilizing substrate network resource more efficiently. In order to further reduce the redundancy of backup resource, we introduce resource sharing into wireless domain and put forward a wireless channel sharing mechanism. To the best of our knowledge, this paper is the first work regarding the SVNE problem in FiWi access network supporting IoT service with the consideration of connection availability. Our main contributions are summarized as follows:

1) We propose a novel connection availability model to qualify the survivability demands of IoT VNs in order to provide the customized IoT service in FiWi access network with robust collaboration of objects.
2) Utilizing the collision domain of wireless subnetwork, we put forward an effective channel sharing mechanism and thus refine substrate resource allocation for the embedding of survivable IoT VNs.
3) We formulate the survivable virtual link embedding problem in FiWi access network using Integer Linear Programming (ILP) with the objective of minimizing resource cost while guaranteeing the availability requirements of IoT VNs.
4) We put forward an efficient heuristic algorithm to generate approximately optimal solution to the SVNE problem of IoT service in polynomial time.

The remainder of this paper is organized as follows. In Section II, related work is presented. In Section III, we introduce the preliminaries and network models for SVNE in FiWi access network. ILP formulation of the survivable virtual link embedding problem is described in Section IV, and then a heuristic algorithm is proposed in Section V. We verify the effectiveness of proposed algorithm and evaluate its performance in Section VI. Finally, we conclude our works.

II. RELATED WORK

The IoT has been utilized to help machines sense the real world through various sensors. The computing-driven applications in IoT are able to complete complex tasks and achieve artificial intelligence [1]. It is important to achieve IoT service provisioning with high robustness and reliability. An architecture of 5G IoT was proposed in [24] to realize effective utilization of channels and QoS improvement. The mobile edge computing was applied in [25] to reduce latency brought by unstable wireless networks and computation failures caused by constrained resource. The heterogeneity of IoT devices was addressed in [26]. A service based approach called IoT Testing as a Service (IoT-TaaS) was proposed to resolve the constraints regarding coordination, cost and scalability issues of traditional software testing. In order to deal with the massive data generated by IoT applications, it was proposed in [27] to exploit geo-distributed Data Centers (DCs) for data analysis. Virtual network embedding was applied to achieve more flexible and efficient resource allocation for uncertain and heterogeneous traffic from massive computation-demanding applications. However, the survivability of VNE for IoT service provisioning has not been addressed previously, which is important to ensure the robustness of IoT services in virtualized FiWi access network.

Some protection and recovery methods have been investigated for different failure scenarios in network virtualization. In order to save the cost of InP, a virtual network embedding approach which enables the resilience to attacks and the efficient resource utilization was put forward in [20]. A reactive strategy was designed to reallocate the capacity affected by an underlying DoS attack for single facility failure. Despite the recovery strategy, most works focused on survivable network design based on protection policies. For single facility failure, an enhanced virtual network with one more virtual node was designed to achieve virtual node protection in [28]. In [29], location-constrained SVNE (LC-SVNE) approaches were proposed to jointly embed the working and backup paths. Resource sharing among working and backup facilities and bandwidth conservation were achieved in node embedding and link embedding, respectively. For single link failure, backup resource was allocated to the working paths with the least resource cost in [18]. In [30], [31], the Service Level Agreement (SLA) of customers was considered in the embedding process to prioritize the restoration of the virtual links that failed with the objective of minimizing the overall impact of failures and maximizing the economic profit of InP. A hybrid policy based on a fast rerouting strategy was proposed to find the backup paths for physical links where InP can control the percentage of resource dedicated for backup and the number of paths allowed for primary and detour flows. Therefore, InP has a great flexibility in determining the optimal allocation based on current failure patterns. In [32], the SVNE is achieved using both physical and logical protections aiming at either single facility failure or single link failure. The classical p-cycle method was utilized in physical protection to find backup resource for embedding the physical paths, while the survival VNs were constructed before they were embedded in the logical protection.

The co-channel interference and time-varying channel condition in wireless network leads to a high possibility of multiple link failures in FiWi access network. Specifically, large-scale network failures may occur because of natural disaster such as tsunami. Reserving backup resource for each virtual link independently causes the unpredictable network fault because multiple physical links may break down simultaneously. Service disruption occurs when multiple virtual links share the same backup physical resource or when the link failure hits on both the working and backup paths of a virtual link. The connection availability is an efficient metric to represent network survivability. Some methods regarding availability analysis were described in [33] and [34].

Researches have been investigated for VNE against multiple node/link failures on the basis of availability. In [19], the availability requirements of services were considered in the embedding by exactly finding a backup node at a reasonable network distance for each node to achieve overall network protection. In [35], authors formulated an ILP model for the SVNE problem, trying to satisfy the availability requirement of each virtual component (i.e., a virtual link or a virtual node) in a VN. Two node mapping strategies based on sequential selection of availability and graph theory, i.e., the maximum-weight maximum clique, were proposed. Simulation indicates the proposed algorithms perform better in terms of blocking probability, availability gap and penalty. However, backup resource always bring high resource consumption, which unavoidably undermines the network resource efficiency. One viable way to addressing this issue is resource sharing.

Many resource sharing strategies have been put forward for survivable network design. The resource sharing between working link and backup link for each VN was applied in [36] against the single network component failure. Moreover, the resource sharing among the backup links of VNs was also used to tolerate the single network component failure because only one VN breaks down at a time [18]. However, the failure of one network component may influence multiple VNs that are embedded on and multiple wireless links may break down at the same time due to the open-air nature of wireless channels. Resource sharing between working and backup links should take into account the collision domains of wireless channels and resource sharing among backup links is not available any more due to unpredictable link failures.

III. PRELIMINARIES AND NETWORK MODELS

A. CONNECTION AVAILABILITY

The availability is initially defined to reflect the ability of repairable systems in which there are two transferable states, working and fault [37], [38]. The system availability A is mainly dependent on its average working time $MTTF$ and average repair time $MTTR$ as (1).

$$A = \frac{MTTF}{MTTF + MTTR}. \tag{1}$$

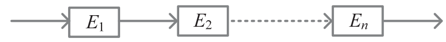


FIGURE 2. Schematic of serial system.

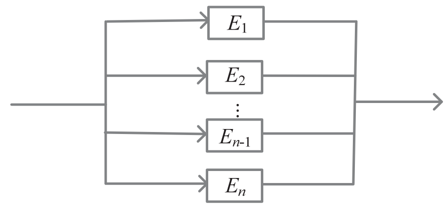


FIGURE 3. Schematic of parallel system.

The formulation of the availability of a system relies on the way it is organized in. A general system can be constructed by two fundamental systems, serial system and parallel system. A typical serial system including n elements is shown in Fig. 2 with E_i denoting the ith independent element. Generally, the availability of a serial system A_s can be expressed as (2), where A_i denotes the availability of the ith individual component. It is worth of noting that the failure of any component in a serial system can lead the entire system to be fault.

$$A_s = \prod_{i=1}^{n} A_i. \tag{2}$$

If a failure occurs only when all n components in a system fall into fault state simultaneously, the system is regarded as an n-order parallel system, as shown in Fig. 3. The availability of n-order parallel system is formulated as (3).

$$A_s = 1 - \prod_{i=1}^{n} (1 - A_i). \tag{3}$$

Based on the fact that communication system is a typical repairable system, we exploit availability to represent the survivable FiWi access network by introducing the probability that a substrate link can work normally. Moreover, in network virtualization, each virtual link is embedded onto a physical path with one or multiple hops and the availability of an embedded path is represented by the product of the availability of all substrate links included. Therefore, the end-to-end connection in virtualized FiWi is a serial system, where as long as any one of the network components along the connection fails, the connection would be interrupted. In addition, it is obvious that parallel system features a higher availability compared with serial system since parallel system enters failure state only when the faults occur in every branch of the system. Therefore, there is an opportunity to improve availability by allocating backup path to each end-to-end working connection and constructing all embedded resource to be parallel system.

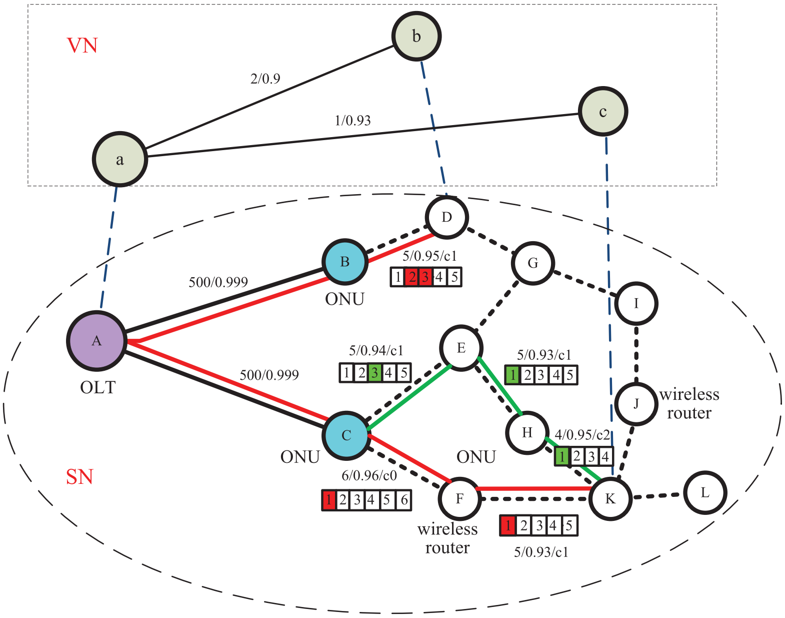


FIGURE 4. Survivable virtual network embedding.

B. SUBSTRATE NETWORK

The substrate FiWi access network can be modeled as an undirected graph $G^S = (N^S, L^S)$ where N^S indicates the set of substrate nodes including OLT, ONUs and wireless routers, and L^S indicates the set of substrate links including fiber links and wireless links as shown in Fig. 4. The substrate node indexed by i is characterized by a CPU capacity CPU_i^S and a location LOC_i^S. The substrate link between nodes i and j, $l_{ij}^S \in L^S$, has a bandwidth capacity of BW_{ij}^S, and a connection availability of A_{ij}^S which is equal to the probability that the link does not break down. The connection availability of a link depends on both the link type and the channel condition. Generally, optical link experiences higher availability than wireless link due to less interference. As shown in Fig. 4, the wireless links and optical links in SN are designated in the forms of $BW_{ij}^S/A_{ij}^S/CH_{ij}^S$ and BW_{ij}^S/A_{ij}^S, respectively.

C. VIRTUAL NETWORK REQUEST

Each type of IoT application is carried on a single VN. The VN request indexed by n is modeled as an undirected graph $G_n^S = (N_n^V, L_n^V)$ where N_n^V and L_n^V denote the sets of virtual nodes and links respectively. The virtual node indexed by u is related to CPU demand CPU_{nu}^V, desired location LOC_{nu}^V and maximum location offset DIS_{nu}^V. The virtual link between u and v, $e_{nuv}^V \in L_n^V$, is characterized by bandwidth demand BW_{nuv}^V and availability demand A_{nuv}^V. Virtual links are shown in the form of BW_{nuv}^V/A_{nuv}^V in Fig. 4.

D. SVNE BASED ON CONNECTION AVAILABILITY

In virtualized FiWi access network, whenever a VN request arrives, InP should implement the embedding procedure according to the requirements of the VN for CPU resource, bandwidth resource, availability and location. Strategies on the embedding of virtual nodes have been studied widely in [39]–[42]. Thus, we focus on the embedding of virtual links in this paper. Different from the general VNE problem, in the SVNE problem the availability of the embedded physical path of each virtual link should be checked once the embedding is finished. If the availability of the embedded physical path meets the availability requirement of the virtual link, the embedding can be finalized. Otherwise, it is required to reserve backup paths to guarantee the availability of the embedded physical path.

In order to improve availability, it is feasible to transform the construction of embedded paths from serial system to parallel system by configuring backup paths. As a result, the embedded path for each virtual link is a combination of serial system and parallel system. We let P_{nuv}^W and P_{nuv}^B denote the embedded working path and backup path of the virtual link e_{nuv}^V, respectively. Thus, the availability of the virtual link e_{nuv}^V after it is embedded, $\bar{A}_{nuv}^V$, is formulated as follows.

$$\bar{A}_{nuv}^V = \left[1-\left(1-\prod_{l_{ij}^S\in P_{nuv}^W, l_{ij}^S\notin P_{nuv}^B} A_{ij}^S\right)\left(1-\prod_{l_{ij}^S\notin P_{nuv}^W, l_{ij}^S\in P_{nuv}^B} A_{ij}^S\right)\right] \cdot \prod_{l_{ij}^S\in P_{nuv}^W\cap P_{nuv}^B} A_{ij}^S, \quad \forall n,\ e_{nuv}^V, \tag{4}$$

where the first term on the right side of Eq. (4) is the probability of disjoint working and backup links, which can be regarded as a parallel serial system. The second term is the probability of overlapped working and backup links, which is a serial system combining the former disjoint part as a whole.

Figure 4 shows an illustrative SVNE example where the virtual nodes a, b and c are mapped to the substrate nodes A, D and K, respectively. The virtual links e^V_{ab} and e^V_{ac} are mapped to the physical paths $A \rightarrow B \rightarrow D$ and $A \rightarrow C \rightarrow F \rightarrow K$, respectively. According to (2), the connection availability of the path $A \rightarrow B \rightarrow D$ is 0.949 (i.e., 0.999 × 0.95), which satisfies the availability demand of e^V_{ab}. Therefore, no backup path is needed. However, the availability of path $A \rightarrow C \rightarrow F \rightarrow K$ is 0.883 (i.e., 0.999 × 0.96 × 0.93), which cannot satisfy the availability demand of e^V_{ac}. Therefore, the backup path $A \rightarrow C \rightarrow E \rightarrow H \rightarrow K$ is allocated for e^V_{ac} and the joint availability of working and backup paths is 0.9808, i.e., $0.999 \times [1-(1-0.94\times 0.93\times 0.95)\times(1-0.96\times 0.93)]$ according to (4), which satisfies the availability demand of e^V_{ac}. It should be noted that availability of wireless to wireless connection can also be enhanced in the aid of optical links through OLT due to the shielded heterogeneity through virtualization.

E. WIRELESS CHANNEL SHARING STRATEGY

While backup resource are allocated to make sure the availability requirements of VNs satisfied, lower resource utilization is resulted as a cost. However, the flexibility of resource scheduling in wireless subnetwork provides opportunities to make the most use of resource by allowing the resource sharing between working and backup links. In the virtualized FiWi access network, each of the wireless channels is shared among different wireless links via time division multiplexing. The idle time slots of one link can be reallocated to other links such that they can share the wireless channels. Specifically, while one of substrate links along the working path fails, data traffic would be switched into the backup path, which leads the bandwidth resource (in terms of time slot) of the invalid link to be idle. Therefore, the backup links that uses the same channel as the invalid link are able to reuse the idle bandwidth resource while generating no interference. If the idle bandwidth resource is enough, no extra bandwidth resource is needed for the backup links. Figure 4 illustrates an example of wireless channel sharing where the blocks with numbers denote the bandwidth resource of the allocated channel and the colored blocks represent the resource that are being taken up currently. If the working path $A \rightarrow C \rightarrow F \rightarrow K$ is interrupted, the link l^S_{FK} cannot carry any more traffic. Thus, the time slot 1 of channel $c1$ becomes idle. Since the backup link l^S_{EH} also occupies the same channel $c1$ as l^S_{FK}, the idle time slot 1 can be reused by l^S_{EH} to recover service. Although l^S_{CE} also occupies channel $c1$, extra time slots have to be allocated because there is no idle bandwidth resource of channel $c1$ released by the working path. Therefore, the channel sharing strategy is effective in reducing resource cost for embedding virtual links.

IV. PROBLEM FORMULATION AND ANALYSIS

A. PROBLEM FORMULATION

In this section, we formulate the problem of virtual link embedding in SVNE based on connection availability as an ILP model. We introduce the following notation to facilitate the problem formulation.

- x^u_i: Binary variable, taking 1 if the virtual node u is embedded into the substrate node i, and 0 otherwise.
- α^{nuv}_{ij}: Binary variable, taking 1 if the embedded working path of virtual link e^V_{nuv} passes the substrate link l^S_{ij}, and 0 otherwise.
- b^{nuv}_{ij}: Binary variable, taking 1 if the embedded backup path of virtual link e^V_{nuv} passes the substrate link l^S_{ij}, and 0 otherwise.
- β^{nuv}_{ijk}: Binary variable, taking 1 if the embedded backup path of virtual link e^V_{nuv} passes the substrate link l^S_{ij} and l^S_{ij} needs to provide extra backup bandwidth resource to e^V_{nuv}, which indicates that no channel sharing is available for l^S_{ij}, and 0 otherwise.
- k: index of channel.
- COL^S_{ij}: collision domain of l^S_{ij}, which indicates the set of wireless links that use the same channel as l^S_{ij}.

- minimize:

$$\sum_{n} \sum_{e^V_{nuv}\in L^V_n} \sum_{l^S_{ij}\in L^S} \alpha^{nuv}_{ij} \cdot BW^V_{nuv} + \beta^{nuv}_{ij} \cdot BW^V_{nuv}. \tag{5}$$

The former in (5) is to minimize the resource cost of working paths, and the latter is to minimize the resource cost of backup paths for all VNs. It is worth mentioning that not all backup links consume resource while we allow channel sharing between working and backup links.

The constraints in (6)-(8) describe the relationship between the working resource and the backup resource:

- subject to:

$$\beta^{nuv}_{ij} \leq b^{nuv}_{ij}, \quad \forall l^S_{ij}, e^V_{nuv}. \tag{6}$$

$$\sum_{l^S_{pq}\in L^S\cap COL^S_{ij}} (b^{nuv}_{pq} - \beta^{nuv}_{pq}) \leq \sum_{l^S_{pq}\in L^S\cap COL^S_{ij}} \alpha^{nuv}_{pq}, \quad \forall e^V_{nuv},\ l^S_{ij}. \tag{7}$$

$$\sum_{n} \sum_{e^V_{nuv}} (\alpha^{nuv}_{ij} + \beta^{nuv}_{ij}) \cdot BW^V_{nuv} \leq BW^S_{ij}, \quad \forall l^S_{ij}. \tag{8}$$

The Equation(6) indicates that the amount of resource shared by backup links should be no more than the amount of idle resource released by invalid working links. It is specified in (7) that channel sharing between the working and the backup links of the same VN is possible only when the links are within the collision domains of each other. Moreover, whether a backup link requires extra bandwidth resource depends not only on the availability of channel sharing but also on if the released resource are enough, Thus, the saved backup resource should be no more than the consumed working resource in each collision domain for each virtual link, as shown in (7). Equation (8) indicates that the resource consumed by working and backup links is no more than the bandwidth capacity of substrate links.

In order to ensure the continuity of embedded physical paths, we introduce flow conservation constraints in (9) and (10):

$$\sum_{l_{ij}^S \in L^S} \alpha_{ij}^{nuv} - \sum_{l_{ji}^S \in L^S} \alpha_{ji}^{nuv} = \begin{cases} 1, & if\ x_i^u = 1, \\ -1, & if\ x_i^v = 1, \\ 0, & \text{otherwise}, \end{cases} \quad \forall e_{nuv}^V. \tag{9}$$

$$\sum_{l_{ij}^S \in L^S} b_{ij}^{nuv} - \sum_{l_{ji}^S \in L^S} b_{ji}^{nuv} = \begin{cases} 1, & if\ x_i^u = 1, \\ -1, & if\ x_i^v = 1, \\ 0, & \text{otherwise}. \end{cases} \quad \forall e_{nuv}^V. \tag{10}$$

The availability constraint specifies that the joint availability of embedded working and backup paths should satisfy the availability requirements of VNs as shown in (11):

$$\bar{A}_{nuv}^V \geq A_{nuv}^V, \quad \forall e_{nuv}^V. \tag{11}$$

B. PROBLEM LINEARIZATION

Since (11) is a nonlinear constraint, we transform it into a linear one using the approximate equation of (12).

$$\prod_{l_{ij}^S} A_{ij}^S \approx 1 - \sum_{l_{ij}^S} (1 - A_{ij}^S). \tag{12}$$

Combining (11) and (12) gives a nonlinear constraint (13). Thus, we introduce an auxiliary variable c_{ij}^{nuv} as defined in (14)-(16) to transform (13) into a linear constraint (17).

$$\begin{aligned} 1 - &\sum_{l_{ij}^S \in L^S} \alpha_{ij}^{nuv} \cdot (1 - A_{ij}^S) + 1 - \sum_{l_{ij}^S \in L^S} b_{ij}^{nuv} \cdot (1 - A_{ij}^S) \\ &- 1 + \sum_{l_{ij}^S \in L^S} (\alpha_{ij}^{nuv} + b_{ij}^{nuv} - \alpha_{ij}^{nuv} \cdot b_{ij}^{nuv})(1 - A_{ij}^S) \\ &\geq A_{nuv}^V, \quad \forall e_{nuv}^V. \end{aligned} \tag{13}$$

$$c_{ij}^{nuv} \leq \alpha_{ij}^{nuv}, \quad \forall l_{ij}^S,\ e_{nuv}^V. \tag{14}$$

$$c_{ij}^{nuv} \leq b_{ij}^{nuv}, \quad \forall l_{ij}^S,\ e_{nuv}^V. \tag{15}$$

$$c_{ij}^{nuv} \geq \alpha_{ij}^{nuv} + b_{ij}^{nuv} - 1, \quad \forall l_{ij}^S,\ e_{nuv}^V. \tag{16}$$

$$\begin{aligned} 1 - &\sum_{l_{ij}^S \in L^S} \alpha_{ij}^{nuv} \cdot (1 - A_{ij}^S) + 1 - \sum_{L_{ij}^S \in L^S} b_{ij}^{nuv} \cdot (1 - A_{ij}^S) \\ &- 1 + \sum_{l_{ij}^S \in L^S} (\alpha_{ij}^{nuv} + b_{ij}^{nuv} - c_{ij}^{nuv})(1 - A_{ij}^S) \geq A_{nuv}^V, \quad \forall e_{nuv}^V. \end{aligned} \tag{17}$$

C. PROBLEM ANALYSIS

In this section, we specify that the problem of virtual link embedding in SVNE based on connection availability is NP-hard by reducing it into a polynomial combination of calculating K-shortest paths which has been proved to be NP-hard [43].

Theorem 1: The problem of virtual link embedding in SVNE based on connection availability is NP-hard.

Proof: For each virtual link, we can find the embedded working and backup paths with satisfied connection availability in following steps. First, we calculate the first K-shortest paths between the embedded end nodes of the virtual link. Then, we check if any path meets the connection availability requirement of the virtual link. If we cannot find any single path with connection availability large enough, then, for any pair of paths, we check their joint connection availability and find two paths with the least resource cost. Overall, we can achieve the embedding of each virtual link through a calculation of K-shortest paths plus $K + K * (K - 1)/2$ checking of connection availability. Since the problem of K-shortest paths is NP-hard, the problem of virtual link embedding in SVNE based on connection availability is NP-hard. ■

TABLE 1. Notation for the heuristic algorithms.

Symbol	Definition
p_k	The kth path calculated by the K-Shortest Paths (KSP) algorithm.
$PATH$	The set of calculated paths.
s_t	The tth solution for the virtual link embedding, which consists of a single working path or joint working and backup paths with the availability requirement satisfied, where $s_t = (p_{work}, p_{backup})$.
SOL	The set of s_t,where $SOL = \{s_0, s_1, \cdots\}$.
$c(l_{ij}^S)$	The channel occupied by l_{ij}^S .
$POOL$	The set of link-channel pairs or links that can be shared, where $POOL = (l_{ij}^S, c(l_{ij}^S))$ or $POOL = l_{ij}^S\ \forall l_{ij}^S \in p_{work}$.
$cost$	The bandwidth cost for the embedding of virtual links, including working and backup links.

V. HEURISTIC ALGORITHMS

Since the virtual link embedding in SVNE based on connection availability is NP-hard, even professional optimization tools such as ILOG CPLEX cannot meet the time-efficient need of embedding large-scale VNs in reality. Therefore, heuristic algorithm is necessary to solve the problem while supporting dynamic VN requests. In this section, we propose an heuristic algorithm based resource sharing and connection availability, where two resource sharing schemes, i.e, link sharing and channel sharing are elaborated. For the convenience of algorithm description, we introduce the definition of symbols used in the heuristic algorithm in Table 1.

As in Algorithm 1, when a VN request arrives, we first obtain the results of node embedding from Greedy Node Mapping (GNM) algorithm [38]. Then, for each virtual link, the KSP algorithm [44] is used to get an approximate solution of K paths from the source to the destination (in Line 5). It should be noted that these K paths are not completely disjoint with each other. The working path and backup path will be chosen among these K paths. If a single path satisfying the availability requirement of the virtual link exists, there is no backup path assigned for it (in Line 8). Otherwise, another backup path that can make the joint availability of working path and backup path satisfy the requirement of the virtual link will be selected (in Line 12). By means of the resource sharing in Algorithm 2 (i.e., link sharing) or Algorithm 3 (i.e., channel sharing), the combination of working and backup paths that satisfies the availability requirement with the least resource cost will be selected as the final embedding solution. If there is no feasible solution, the VN request will be rejected (in Line 20).

Algorithm 1 SVNE Based on Resource Sharing and Connection Availability (SSA)

Input: $G_n^V(N_n^V, E_n^V)$, $G_n^S(N_n^S, E_n^S)$
Output: Embedded working path and backup path for each virtual link

1: **while** all virtual nodes **do**
2: Embed them using the GNM algorithm in [19];
3: **end while**
4: **while** $e_{nuv}^V \in E^V$ **do**
5: Use the KSP algorithm to get K shortest paths, $PATH = \{p_0, p_1, p_2, ..., p_{K-1}\}$, and then sort $PATH$ in the increasing order of the bandwidth cost;
6: **while** $p_k \in PATH$ **do**
7: **if** The availability of p_k is no less than A_{nuv}^V **then**
8: Store p_k as a working path in the solution set SOL, then **break**;
9: **else**
10: **while** $p'_k \in PATH$ **do**
11: **if** The joint availability of p_k and p'_k is no less thanA_{nuv}^V **then**
12: Store p_k as a working path and p'_k as a backup path in the solution set SOL;
13: **end if**
14: **end while**
15: **end if**
16: **end while**
17: **if** $SOL \neq \phi$ **then**
18: Select the solution with the least resource cost $s = \min\{SOL\}$ by means of the resource sharing in Algorithm 2 or Algorithm 3;
19: **else**
20: Reject the VN;
21: **end if**
22: **end while**

Algorithm 2 Link Sharing (LS)

Input: $s \in SOL$, BW_{nuv}^V
Output: $cost$.

1: Initialize $cost \leftarrow 0$;
2: **if** $p_{work} \neq null$ **then**
3: **while** $l_{ij}^S \in p_{work}$ **do**
4: $cost \leftarrow cost + BW_{nuv}^V$;
5: Put l_{ij}^S into the set of links $POOL$;
6: **end while**
7: **end if**
8: **if** $p_{backup} \neq null$ **then**
9: **while** $l_{ij}^S \in p_{backup}$ **do**
10: **if** $l_{ij}^S \in POOL$ **then**
11: $POOL \leftarrow POOL - \{l_{ij}^S\}$;
12: **else**
13: $cost \leftarrow cost + BW_{nuv}^V$;
14: **end if**
15: **end while**
16: **end if**

Algorithm 3 Channel Sharing (CS)

Input: $s \in SOL$, BW_{nuv}^V
Output: $cost$.

1: Initialize $cost \leftarrow 0$;
2: **if** $p_{work} \neq null$ **then**
3: **while** $l_{ij}^S \in p_{work}$ **do**
4: $cost \leftarrow cost + BW_{nuv}^V$;
5: Put $(l_{ij}^S, c(l_{ij}^S))$ into the set of link-channel pairs $POOL$;
6: **end while**
7: **end if**
8: **if** $p_{backup} \neq null$ **then**
9: **while** $l_{ij}^S \in p_{backup}$ **do**
10: **if** a link in $POOL$ is in the collision domain of l_{ij}^S with the same channel **then**
11: delete this link from $POOL$;
12: **else**
13: $cost \leftarrow cost + BW_{nuv}^V$;
14: **end if**
15: **end while**
16: **end if**

In the SSA algorithm, two resource sharing mechanisms are used to reduce the resource cost for SVNE by allowing resource sharing between working and backup paths. There are two kinds of resource that can be shared, that is, Link Sharing (LS) and Channel Sharing (CS). The LS mechanism takes advantage of the connection availability to reduce the resource cost since the working and backup paths are not necessarily disjoint. The CS mechanism takes advantage of the ubiquitous nature of wireless resource to increase the probability of resource sharing.

According to the SSA algorithm, the working and backup paths may not be completely disjoint. Therefore, in LS mechanism, the overlapping part of the working and backup paths is allowed to share resource with each other. With the resource shared, the corresponding link should be removed from $POOL$ (in Line 10). The working links as well as the disjoint part of the backup path will cost extra resource.

In the CS mechanism, resource sharing is achieved on channels. Detailed procedure is described in Algorithm 3. Each backup wireless link which is in any collision domains of the links on its working path has the opportunity to share resource with the working links (in Lines $10 - 13$). In order to avoid contention, the amount of shared resource by backup links should be no more than the idle resource on the working path. Otherwise, extra resource should be assigned to backup links.

The illustration of wireless channel sharing is shown in Fig. 5, where the number on each wireless link denotes the occupied channel, and the collision domain of each wireless link is marked with dashed circle. The collision domain of

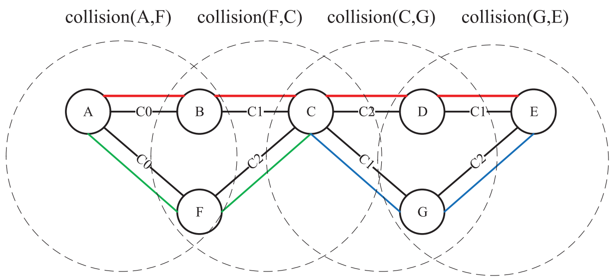


FIGURE 5. Illustration of channel sharing.

a wireless link is defined as the set of wireless links that interfere with the link, which will lead to a high error rate and even cause transmission failure when they transmit data simultaneously. We assume a virtual link whose end nodes have been embedded onto the nodes A and E. When we attempt to embed the virtual link, a physical path should be built between A and E. By using the KSP algorithm, we obtain three paths that are link-disjoint with each other, p_0: $A \rightarrow B \rightarrow C \rightarrow D \rightarrow E$, p_1: $A \rightarrow F \rightarrow C \rightarrow D \rightarrow E$ and p_2: $A \rightarrow B \rightarrow C \rightarrow G \rightarrow E$. As a result, there are six candidate embedding solutions, i.e., $SOL = \{s_0, s_1, s_2, s_3, s_4, s_5\}$, where $s_0 = (p_0, null)$, $s_1 = (p_1, null)$, $s_2 = (p_2, null)$,$s_3 = (p_0, p_1)$,$s_4 = (p_0, p_2)$ and $s_5 = (p_1, p_2)$. We take s_3 and s_4 as an example. The working path p_0 always needs to be allocated the bandwidth resource. For the backup path p_1 in s_1, the links l^S_{AF} and l^S_{EC} can reuse the idle resource released by l^S_{AB} and l^S_{CD}. Therefore, we do not need to allocate additional resource for them. For backup link p_2 in s_2, the idle resource released by l^S_{DE} can be reused by l^S_{CG}. Since the link l^S_{GE} and its conflicting links on the working path occupy different channels, it is required to allocate extra resource to l^S_{GE}. Obviously, embedding solution s_3 is better than s_4 for less extra resource cost.

VI. PERFORMANCE EVALUATIONS

A. SIMULATION SETTINGS

In the simulation, we evaluate a substrate FiWi access network with 1 OLT, 4 ONUs (each ONU is equipped with 2 wireless gateways) and 36 wireless routers. The PON subnetwork is organized in a single tree structure with each ONU connected with OLT in a fixed position. The WMN subnetwork is deployed in a grid structure. Each router is equipped with two Radio Frequency (RF) interfaces. Both the transmission range and collision range of wireless router is set to 100m. Different wireless links within the same collision range share the channel capacity by means of time division multiplexing. The RF interfaces are allocated channels according to IEEE 802.11a, with 11 orthogonal channels of 20MHz bandwidth for outdoor communication. The settings of substrate link capacity and the failure probability are shown in Table 2, where μ denotes the average failure probability of wireless link.

The number of virtual nodes in a VN follows uniform distribution in the range of [2], [5] and node location requests are randomly generated. The link connectivity between any two virtual nodes is 50%. The CPU demands of virtual nodes follow uniform distribution in [1], [2] units and the bandwidth demands of virtual links follow uniform distribution in [1], [2] Mbps. To evaluate the effectiveness of proposed algorithm, we make a performance comparison with previous VNE algorithms [39] with regards to different criteria. Specifications of the benchmark algorithms are shown in Table 4.

TABLE 2. Parameter settings of substrate network [2], [31].

Parameters	Value
Distribution fiber link capacity	1000 Mbps
CPU capacity of ONU	10000 units
CPU capacity of wireless router	100 units
Cable link capacity	100 Mbps
Wireless link capacity	54 Mbps
Fiber link failure probability	0.0001
Cable link failure probability	0.001
Wireless link failure probability	uniformly in $[\mu-0.5, \mu+0.5]$

TABLE 3. Benchmark algorithms.

Algorithm	Specification
Dh	VNE based on the Dijkstra algorithm aiming at the minimum hops [22], [43].
Du	VNE based on the Dijkstra algorithm with the link unavailability as weight [22], [43].
DPP-ILP	ILP model of the SVNE based on dedicated path protection [16].
CSA-ILP	ILP model of the SVNE based on channel sharing and availability.
LSA-ILP	ILP model of the SVNE based on link sharing and availability.
CSA	Proposed heuristic algorithm of SVNE based on channel sharing, link Sharing and availability.
LSA	Proposed heuristic algorithm of SVNE based on link sharing and availability.
DPP	Proposed heuristic algorithm of SVNE based on dedicated path protection [16].

B. SIMULATION RESULTS AND ANALYSIS

In this subsection, we first verify the necessity of considering connection availability during virtual network embedding. Then, we compare the upper bound performance of SVNE algorithms of CSA, LSA and DPP based on the results of their ILP models which are solved with IBM ILOG CPLEX 12.1. Finally, we evaluate and analyze the performance of the heuristic algorithms above in terms of bandwidth cost, resource redundancy and virtual network acceptance rate.

The average availability and worst availability are evaluated among Dh, Du and DDP with different settings of wireless link availability,[0.85, 0.9], [0.9, 0.95] and [0.95, 0.99]. As shown in Figs. 6 and 7, the performance of Dh, where only resource cost but not availability is considered, is the worst. Specifically, the average availability of virtual links is 0.76, 0.84 and 0.94 respectively for different settings, while the worst availability of virtual links is 0.43, 0.6 and 0.82, respectively. Therefore, it is difficult for Dh to meet the availability requests of virtual links. In comparison, Du prefers to select links with high availability during the

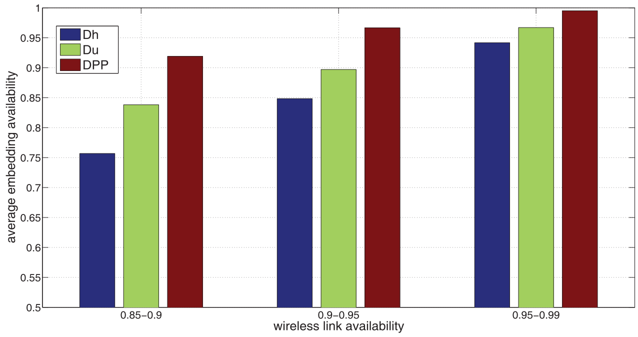


FIGURE 6. Average availability of embedded links for different SVNE algorithms.

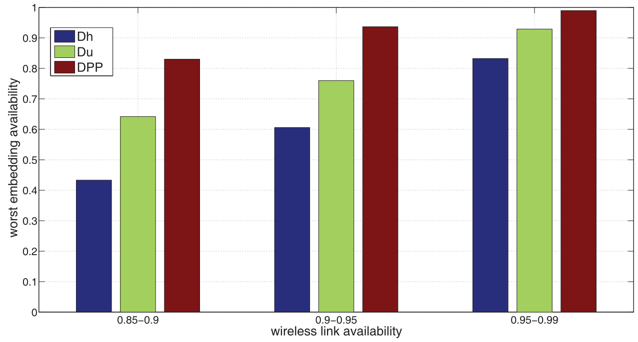


FIGURE 7. Worst availability of embedded links for different SVNE algorithms.

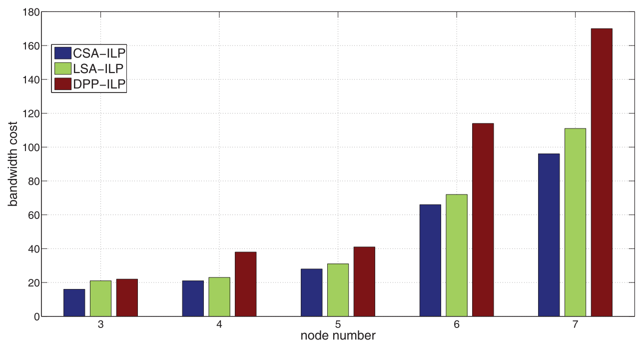


FIGURE 8. Bandwidth cost for different SVNE algorithms.

virtual link embedding. Thus, Du outperforms Dh in terms of resource cost. In addition, DPP provides a completely disjoint backup path for each working path and achieves the average availability of 0.92, 0.96 and 0.99 and the worst availability of 0.83, 0.93 and 0.98, respectively. It can be observed that, as long as the availability of wireless links is not too bad, DPP algorithm can meet the availability requests of most virtual links.

Figure 8 shows the upper bounds of bandwidth cost provided by solving ILP models of different mechanisms. Bandwidth cost is defined as the total amount of bandwidth resource that is used for SVNE. Since DPP provides a completely disjoint backup path for each working path, its

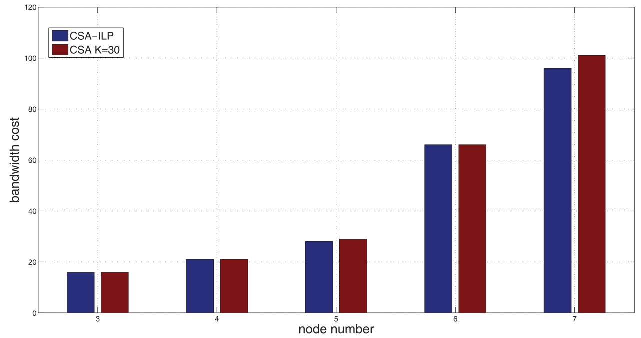


FIGURE 9. Bandwidth cost for heuristic algorithm and ILP.

TABLE 4. Running time of heuristic algorithm and ILP (in seconds).

Node number	Running time of heuristic algorithm(K=30) (s)	Running time of ILP (s)
3	0.27	0.23
4	0.5	0.29
5	0.652	13.87
6	1.54	21.48
7	2.39	7038

bandwidth cost is the largest. Moreover, LSA embeds the working and backup paths for each VN according to its availability demands without the path disjointness constraint, thus the cost of backup resource can be effectively reduced. Finally, CSA can further reduce the cost of backup resource by allowing backup links to reuse the idle radio resource released by working links.

Figure 9 shows the comparison of bandwidth cost between heuristic algorithm ($K = 30$ in KSP) and ILP for CSA with different VN sizes in terms of virtual node number. It can be observed that while the network size is small, the heuristic CSA can achieve the optimal solutions. With the expansion of network size, heuristic CSA is still able to yield the approximate optimal solutions (with the gap of less than 5.21%).

More importantly, heuristic CSA is time-efficient, especially when it comes to large VN sizes. Table 4 shows the comparison of running time between the heuristic algorithm and the ILP. With the network size increasing, the running time of solving ILP model increases dramatically. Specifically, while the number of virtual nodes is 7, the running time of ILP is nearly 3,000 times that of the heuristic algorithm. In this case, the heuristic algorithm is obviously more advantageous than ILP for real-time requests.

With the VN number growing, Fig. 10 and 11 display the comparison of different algorithms in resource redundancy ratio and VN acceptance ratio, respectively. It can be observed that greater K value helps CSA reach closer to the optimal solution. However, the performance of CSA will not increase constantly with the infinite increase of K value due to the finite size of solution space. When the value of K increases above 30 (e.g., $K = 50$), the performance of CSA is almost the same as $K = 30$ as shown in Fig. 11. Therefore, CSA realizes a best compromise between computational

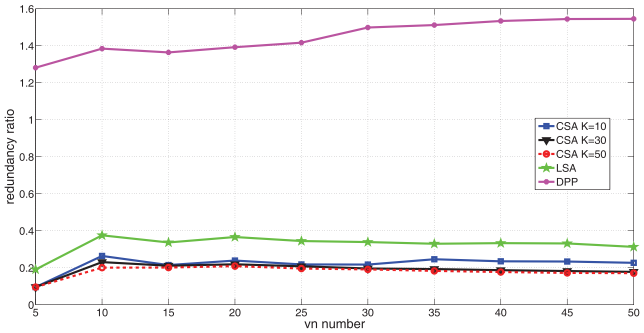


FIGURE 10. Resource redundancy ratio for different SVNE algorithms.

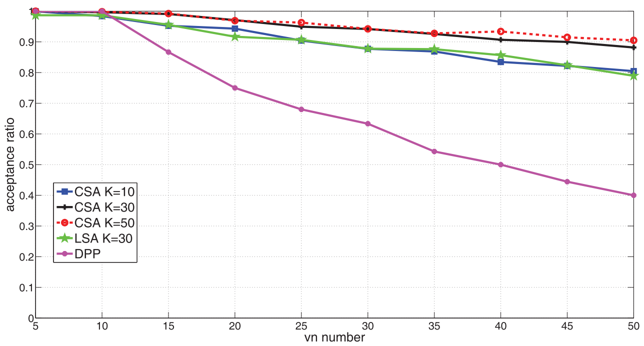


FIGURE 11. Acceptance ratio for different SVNE algorithms.

complexity and performance when $K = 30$. Moreover, CSA is better than LSA, which performs better than DPP. The reason for this result is similar to the analysis aforementioned. Particularly, in CSA, the average resource redundancy is reduced by around 41.3% and 84.2% compared to traditional LSA and DPP algorithms respectively, when the number of VNs reaches to 50. Owing to the superiority in reducing resource redundancy, CSA gains a rise of around 12.5% and 112.4% in VN acceptance ratio over LSA and DPP, respectively.

VII. CONCLUSION

In this paper, we addressed resource-efficiently survivable virtual network embedding in FiWi access network for robust collaboration of objects in IoT service. We first put forward a probabilistic model to quantify the connection availability of virtual links. Then, we proposed a more fine-grained channel sharing mechanism on the basis of link sharing. By taking into account the availability requests of VNs, we formulated the survivable virtual link embedding problem as an ILP model aiming to minimize resource cost. Furthermore, in order to support dynamic VN requests in a real-time pattern, we proposed an efficient heuristic algorithm for the survivable virtual network embedding to generate the approximately optimal solutions in polynomial time. Simulation results verified better performance of proposed algorithm in terms of resource cost, VN acceptance ratio and resource redundancy. In our future research works, we will focus on the impact of QoS requirements of various IoT services on network resource utilization, which remains as an open issue in previous works.

ACKNOWLEDGMENT

This paper was presented at the Asia Communications and Photonics Conference (ACP) 2016.

REFERENCES

[1] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16–22, Feb. 2018.

[2] N. Ghazisaidi, M. Maier, and C. M. Assi, "Fiber-wireless (FiWi) access networks: A survey," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 160–167, Feb. 2009.

[3] Z. Ning, P. Dong, X. X. Wang, and J. Rodrigues, "Deep reinforcement learning for vehicular edge computing: An intelligent offloading system," *ACM Trans. Intell. Syst. Technol.*, vol. 25, p. 1, May 2019. doi: 10.1145/3317572.

[4] M. Chowdhury, E. Steinbach, W. Kellerer, and M. Maier, "Context-aware task migration for HART-centric collaboration over FiWi based tactile Internet infrastructures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 6, pp. 1231–1246, Jun. 2018.

[5] Z. Ning, X. Wang, J. J. Rodrigues, and F. Xia, "Joint computation offloading, power allocation, and channel assignment for 5G-enabled traffic management systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 3058–3067, May 2019.

[6] C. Ranaweera *et al.*, "Optical X-haul options for 5G fixed wireless access: Which one to choose?" in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 1–2.

[7] Q. Dai, G. Shou, Y. Hu, and Z. Guo, "A general model for hybrid fiber-wireless (FiWi) access network virtualization," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2013, pp. 858–862.

[8] X. Wang *et al.*, "Optimizing content dissemination for real-time traffic management in large-scale Internet of Vehicle systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1093–1105, Feb. 2019.

[9] C. Zhu, L. Shu, V. C. M. Leung, S. Guo, Y. Zhang, and L. T. Yang, "Secure multimedia big data in trust-assisted sensor-cloud for smart city," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 24–30, Dec. 2017.

[10] C. Zhu, V. C. M. Leung, J. J. P. C. Rodrigues, L. Shu, L. Wang, and H. Zhou, "Social sensor cloud: Framework, greenness, issues, and outlook," *IEEE Netw.*, vol. 32, no. 5, pp. 100–105, Sep. 2018.

[11] H. Cao, Y. Zhu, G. Zheng, and L. Yang, "A novel optimal mapping algorithm with less computational complexity for virtual network embedding," *IEEE Trans. Netw. Service Manag.*, vol. 15, no. 1, pp. 356–371, Mar. 2018.

[12] X. Wang *et al.*, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, to be published. doi: 10.1109/COMST.2018.2882064.

[13] H. Cao, L. Yang, and H. Zhu, "Novel node-ranking approach and multiple topology attributes-based embedding algorithm for single-domain virtual network embedding," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 108–120, Feb. 2018.

[14] N. Ghazisaidi, M. Scheutzow, and M. Maier, "Survivability analysis of next-generation passive optical networks and fiber-wireless access networks," *IEEE Trans. Rel.*, vol. 60, no. 2, pp. 479–492, Jun. 2011.

[15] X. Wang *et al.*, "A city-wide real-time traffic management system: Enabling crowdsensing in social Internet of Vehicles," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 19–25, Sep. 2018.

[16] S. R. Chowdhury *et al.*, "Dedicated protection for survivable virtual network embedding," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 4, pp. 913–926, Dec. 2016.

[17] M. M. A. Khan, N. Shahriar, R. Ahmed, and R. Boutaba, "Multi-path link embedding for survivability in virtual networks," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 2, pp. 253–266, Jun. 2016.

[18] Q. Chen, Y. Wang, X. Qiu, W. Li, and A. Xiao, "A survivable virtual network embedding scheme based on load balancing and reconfiguration," in *Proc. NOMS*, May 2014, pp. 1–7.

[19] A. Khan, X. An, and S. Iwashina, "Virtual network embedding for telco-grade network protection and service availability," *Comput. Commun.*, vol. 84, pp. 25–38, Jun. 2016.

[20] R. R. Oliveira *et al.*, "No more backups: Toward efficient embedding of survivable virtual networks," in *Proc. IEEE ICC*, Jun. 2013, pp. 2128–2132.

[21] G. Egeland and P. E. Engelstad, "The availability and reliability of wireless multi-hop networks with stochastic link failures," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1132–1146, Sep. 2009.

[22] M. Kiese, E. Georgieva, D. Schupke, B. Mukherjee, and J. Eberspacher, "Availability evaluation of hybrid wireless optical broadband access networks," in *Proc. IEEE ICC*, Jun. 2009, pp. 1–6.

[23] J. Hou, Y. Liu, L. Guo, P. Han, and X. Han, "Survivable virtual network embedding based on connection availability in fiber-wireless access network," in *Proc. ACP*, Nov. 2016, pp. 1–3.

[24] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 87–93, Jun. 2019.

[25] C. Zhu, X. Li, V. C. M. Leung, L. T. Yang, E. C.-H. Ngai, and L. Shu, "Towards pricing for sensor-cloud," *IEEE Trans. Cloud Comput.*, to be published. doi: 10.1109/TCC.2017.2649525.

[26] Z. Ning, J. Huang, X. Wang, J. Rodrigues, and L. Guo, "Mobile edge computing-enabled Internet of Vehicles: Toward energy-efficient scheduling," *IEEE Netw.*, Apr. 2019. doi: 10.1109/MNET.2018.1800309.

[27] W. Wei, H. Gu, K. Wang, X. Yu, and X. Liu, "Improving cloud-based IoT services through virtual network embedding in elastic optical inter-DC networks," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 986–996, Feb. 2019. doi: 10.1109/JIOT.2018.2866504.

[28] Z. Ning, X. Wang, and J. Huang, "Mobile edge computing-enabled 5G vehicular networks: Toward the integration of communication and computing," *IEEE Veh. Technol. Mag.*, vol. 14, no. 1, pp. 54–61, Mar. 2019.

[29] H. Jiang, L. Gong, and Z. W. Zuqing, "Efficient joint approaches for location-constrained survivable virtual network embedding," in *Proc. IEEE GLOBECOM*, Dec. 2014, pp. 1810–1815.

[30] M. R. Rahman and R. Boutaba, "SVNE: Survivable virtual network embedding algorithms for network virtualization," *IEEE Trans. Netw. Service Manag.*, vol. 10, no. 2, pp. 105–118, Jun. 2013.

[31] P. Han, Y. Liu, and L. Guo, "QoS satisfaction aware and network reconfiguration enabled resource allocation for virtual network embedding in Fiber-wireless access network," *Comput. Netw.*, vol. 143, pp. 30–48, Oct. 2018.

[32] Z. Ning, P. Dong, X. Kong, and F. Xia, "A cooperative partial computation offloading scheme for mobile edge computing enabled Internet of things," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2018.2868616.

[33] Y. Liu, Y. Yu, and P. Han, "Joint wireless and optical resources allocation for availability-guaranteed service in survivable fiber-wireless access network," *Photonic Netw. Commun.*, vol. 32, no. 2, pp. 310–319, Oct. 2016.

[34] L. Zhou, M. Held, and U. Sennhauser, "Connection availability analysis of shared backup path-protected mesh networks," *J. Lightw. Technol.*, vol. 25, no. 5, pp. 1111–1119, May 2007.

[35] H. Jiang, Y. Wang, L. Gong, and Z. Zhu, "Availability-aware survivable virtual network embedding in optical datacenter networks," *J. Opt. Commun. Netw.*, vol. 7, pp. 1160–1171, Dec. 2015.

[36] A. S. Gowda, L. G. Kazovsky, K. Wang, and D. Larrabeiti, "Quasi-passive optical infrastructure for future 5G wireless networks: Pros and cons," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 8, no. 12, pp. B111–B123, Dec. 2016.

[37] R. Billinton and R. N. Allan, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. New York, NY, USA: Springer, 1992.

[38] A. Birolini, *Reliability Engineering: Theory and Practice*. Berlin, Germany: Springer-Verlag, 2004.

[39] L. Gong and Z. Zhu, "Virtual optical network embedding (VONE) over elastic optical networks," *J. Lightw. Technol.*, vol. 32, no. 3, pp. 450–460, Feb. 1, 2014.

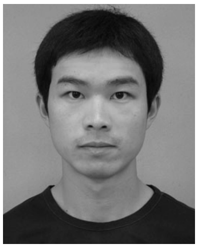
[40] L. Gong, Y. Wen, Z. Zhu, and T. Lee, "Toward profit-seeking virtual network embedding algorithm via global resource capacity," in *Proc. INFOCOM*, Apr. 2014, pp. 1–9.

[41] L. Gong, H. Jiang, Y. Wang, and Z. Zhu, "Novel location-constrained virtual network embedding LC-VNE algorithms towards integrated node and link mapping," *IEEE/ACM Trans. Netw.*, vol. 24, no. 6, pp. 3648–3661, Dec. 2016.

[42] A. Fischer, J. F. Botero, M. T. Beck, H. de Meer, and X. Hesselbach, "Virtual network embedding: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1888–1906, 4th Quarter, 2013.

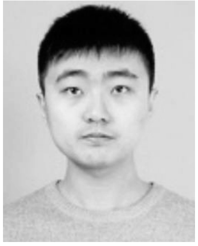
[43] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York, NY, USA: Freeman, 1979.

[44] W. Hou, Z. Ning, L. Guo, and M. S. Obaidat, "Service degradability supported by forecasting system in optical data center networks," *IEEE Syst. J.*, to be published. doi: 10.1109/JSYST.2018.2821714.



YEJUN LIU is currently a Professor with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China. His research interests include converged fiber-wireless access networks and optical communication.

PENGCHAO HAN is currently pursuing the Ph.D. degree with Northeastern University, Shenyang, China. Her research interests include converged fiber-wireless access networks and network virtualization.



JIAN HOU received the master's degree in electronics and communication engineering from the School of Computer Science and Engineering, Northeastern University, Shenyang, China, in 2017. His research interests include converged fiber-wireless access networks and network survivability.

JIANBO ZHENG received the B.S. degree in management from the Shandong University of Science and Technology, China, in 2006, the M.S. degree in software engineering from Southeast University, China, in 2013, and the M.S. degree in computer science from the University of New Brunswick, Canada, in 2014. From 2014 to 2017, he was a Senior Developer of network security and cloud computing with IBM Canada. He is currently an Engineer with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences. His research interests include cloud robotics, human–computer interaction, and data mining.