

带有区分保护的虚拟化 FiWi 网络可靠传输机制

王汝言^{1,2}, 高毅爽^{1,2}, 陈霄^{1,2}

(1. 重庆邮电大学通信与信息工程学院, 重庆 400065; 2. 重庆邮电大学光通信与网络重点实验室, 重庆 400065)

摘要: 针对用户对网络服务的差异化可靠性需求, 提出一种带有区分保护的虚拟化光无线融合网络可靠传输机制。以用户需求的保护质量及所能够支付的费用作为条件, 通过恢复概率进行多等级保护质量的量化, 灵活地分配备份保护资源; 利用等级服务区分算法筛选满足业务保护质量等级的保护路径, 降低业务阻塞以及不受保护的的业务数量, 提高业务保护质量。结果表明所提机制在平均收益开销比和底层网络资源开销等指标上具有较高优势, 在满足用户可靠性需求的同时, 能够为用户提供更灵活的虚拟网络数据传输。

关键词: 光无线融合网络; 网络虚拟化; 可靠性; 区分保护

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-436x.2019069

Reliable transmission mechanism with differentiated protection in virtualized fiber-wireless access network

WANG Ruyan^{1,2}, GAO Yishuang^{1,2}, CHEN Xiao^{1,2}

1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

2. Key Laboratory of Optical Communication and Network, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: In view of the different reliability requirements of network service, a reliable transmission mechanism with differentiated protection was proposed in virtualized fiber-wireless access network. The quality of protection required by users and the fees that can be paid were used as a prerequisite. The backup protection resources were flexibly allocated by quantifying the multi-level protection quality with the probability of recovery. Then, for reducing traffic congestion and the unprotected services, the level service differentiation algorithm was used to choose protection link which was satisfied with the level of protection quality. The results show the proposed mechanism has more advantages in terms of long-term benefit-to-cost ratio and underlying network resource overhead, and provides users with a more flexible virtual network transmission while satisfying users' reliability requirements.

Key words: integrated fiber-wireless access network, network virtualization, reliability, differentiated protection

1 引言

随着用户对高速数据和多媒体业务的需求日益增长, 传统无线接入方式已无法满足用户不断增长的带宽需求, 移动互联网、物联网等业务的迅速普及导致高容量的光纤接入方式无法保障接入的

灵活性^[1]。低成本、高带宽的光网络与高移动性、高灵活性的无线网络的有效结合为下一代接入网提供了合理可行的解决方案^[2]。光无线 (FiWi, fiber-wireless) 融合接入网由前端无线网状网 (WMN, wireless mesh network) 和后端无源光网络 (PON, passive optical network) 组成^[3], 具有 PON

收稿日期: 2018-08-28; 修回日期: 2019-02-22

基金项目: 国家自然科学基金资助项目 (No.61771082); 重庆市高校创新团队建设计划基金资助项目 (No.CXTDX201601020)

Foundation Items: The National Natural Science Foundation of China (No.61771082), Chongqing Funded Project of Chongqing University Innovation Team Construction (No.CXTDX201601020)

的高带宽、低损耗、传输稳定和 WMN 的易部署、支持移动性等优点，能够以更加灵活的方式为用户提供更高质量的接入服务。然而，随着用户规模不断扩大，不同用户的身份背景、使用目的和经济状况不同，用户对网络服务的使用，尤其是服务可靠性保护方面呈现差异化的需求^[4]。

根据文献[5]中对用户需求差异化的定义，可将网络中的用户分为3类。第一类用户对业务的实时性要求较高，需要服务提供商(SP, service provider)提供高质量的服务保护，同时愿意支付相应的报酬作为交换。第二类用户对业务实时性要求相对较低，在保证数据正确传输的情况下，可以接受一定的服务延迟。因此对服务的保护质量(QoP, quality of protection)没有第一类用户高，同时希望降低一定的支付费用。第三类用户由于业务不重要或经济不允许等原因，不想支付保护费用，且愿意忍受服务的数据损坏或中断。对于这3类用户的不同需求，SP如何将其同时映射到融合网络中，并为其分配合理的网络资源来满足不同用户的不同需求，成为FiWi融合接入网络可靠传输的一大研究热点。

网络虚拟化技术将数据传输功能和控制功能解耦合，使多个相互独立的虚拟网络可共存于相同基础设施，因此，利用虚拟化技术可在FiWi网络中将多等级业务映射在不同虚拟网络中，实现有效隔离。同时，利用网络虚拟化高效的资源分配机制，可以在保证服务质量的前提下，实现底层资源的最优化使用。网络虚拟化中虚拟网络映射问题是网络虚拟化技术实现的一个关键步骤^[6]。目前，虚拟网络可靠映射方法通常是基于冗余资源的保护。文献[7]提出了一种全备份保护方法，通过对链路采用全备份保护，使网络可靠性得到了保障。文献[8]提出了一种备份资源池共享机制，通过备份资源共享实现保障网络可靠，同时减少备份资源占用。文献[9]以最小资源消耗为目标提出一种节点和链路迁移与重映射算法。通过将故障节点和链路进行重映射保障网络的可靠性。以上机制在一定程度上提高了业务传输的可靠性，不足之处在于所提方案并未对业务进行区分，没有考虑到实际场景中不同业务间的差异性以及对可靠性的不同要求。从充分利用网络可用资源的角度出发，文献[10]提出了QoP的概念，通过参数形式表示网络故障时业务需要提供的保护资源比例，然而其仅考虑了带宽约束，而虚拟网络映射需要考虑节点和链路双重约束。文献[11]在虚

拟网络基础上提出了区分业务等级的QoP，但只是将业务保护按比例进行区分，并没有对业务进行有效的划分。

目前，FiWi网络中的可靠传输机制主要依赖业务无差别的设备级备份方式，或从服务等级区分的角度考虑业务级的可靠传输，但服务等级区分相对粗糙，造成因备份资源分配不合理而导致的资源浪费问题。因此，FiWi网络中的传统可靠传输机制并不适用于虚拟化FiWi网络中，其主要原因在于，传统可靠传输机制无法利用虚拟化的资源集中管理优势对拓扑路径和节点资源进行最优分配，虽然生存性得到保障，但使备份资源在主链路无故障的情况下长期处于闲置状态，降低了资源利用率。

为解决以上问题，本文提出一种带有区分保护的虚拟化FiWi融合网络可靠传输机制。首先，根据用户需求的QoP及能够支付的费用，设计出基于恢复概率的灵活区分保护的策略。然后，提出一种灵活等级服务区分算法(FLSDA, flexible level service differentiated algorithm)选择满足业务QoP需求的保护路径，所提算法利用广度优先搜索树寻找映射节点。最后，利用带有灵活QoP策略的遗传算法求解链路映射方案，进而完成保护路径映射，最小化网络开销，为用户提供更灵活的虚拟网络故障恢复方案。

2 问题描述与网络模型

2.1 业务保护等级划分

近年来，针对链路故障的共享备份保护方案中，大多是针对全网业务提高资源利用率、网络可靠性的方案，忽略了业务多样性所引发的服务质量需求差异化问题。随着业务种类的增多，业务优先级的划分也成为一种必然的趋势。然而，目前针对业务优先级的划分大多将实时要求较高的语音、视频等业务定义为非弹性服务，设置为较高的优先级，将对时延不敏感的WWW/E-mail等业务定义为弹性服务，设置为较低优先级^[12]，很少从用户角度根据所愿意支付的费用和对保护质量的需求对业务实现有效的区分保护。针对以上问题，本文从用户角度出发，利用网络虚拟化全局视角和资源集中管理的优势，根据业务要求的QoP，灵活地为业务提供不同等级的恢复概率，减小统一备份方案与差异化业务不匹配造成的资源浪费。所提方案中首先利用多路径在WMN中并行传输业务数据，并将业

务数据在光网络单元 (ONU, optical network unit) 处进行汇聚; 其次, 利用光域的高带宽及高可靠性, 在 PON 侧进行单链路传输。WMN 中主路径采用多路径传输, 备份路径在考虑用户需求的 QoP 及所能够支付的费用的前提下, 通过恢复概率进行多等级保护质量的量化, 更加灵活地为其分配备份保护资源。所提策略的 QoP 等级通过传输链路的平均可恢复概率确定, 不同业务的 QoP 方案如下。

1) 优先服务。独享的主传输路径和备用路径, 恢复概率 $p_{s_u} = q_0 = 100\%$ 。

2) 带有 L 级保护的服务。独有的主传输路径和带有恢复概率 $p_{s_u} \geq q_i = M\%$ 的共享备用路径, 其中, $i \in \{1, 2, \dots, |Q| - 3\}$, $Q = \{q_0, q_1, \dots, q_{|Q|-1}\}$ 表示网络提供的 QoP 等级集合, $|Q|$ 为等级集合的数量。与固定 1: N 共享类别相比, 本方案有更多的 QoP 级别。

3) 不需要保护的服务。只有主传输路径不分配保护路径, 恢复概率 $p_{s_u} = q_{|Q|-2} = 0$ 。

4) 可被抢占服务。主传输路径为需要保护级别的备份路径, 恢复概率 $p_{s_u} = q_{|Q|-1} = 0$ 。

通过以上灵活的等级划分, 服务提供商可根据用户需求更加有效地分配保护资源, 达到提高网络资源利用率进而提高收益的目的。

2.2 网络模型

FiWi 网络虚拟化的过程就是将网络中的物理资源抽象成虚拟资源的过程, 通过抽象物理节点和链路 ID、位置、功能属性、非功能属性等资源, 屏蔽 FiWi 网络中光域和无线域拓扑结构、链路带宽等网络性能的差异。图 1 为融合网络虚拟化的整体架构。为了屏蔽光域和无线域网络的异构性, 本节

将虚拟化 FiWi 分为 3 层: 基础设施层 (InF, infrastructure)、虚拟化管理层 (VM, virtual manager) 以及网络服务层 (SP, service provider)。该模型把基础设施层中 PON 和 WMN 的物理资源抽象成虚拟资源, 形成虚拟资源层, 以便虚拟资源管理器 (VRM, virtual resource manager) 将抽象化的资源集中化管理。这些抽象的虚拟资源继承了底层设备的物理属性, 包括带宽、容量、存储空间等资源。在虚拟化管理层, VRM 根据服务提供商的虚拟请求对虚拟资源进行分配。SP 在虚拟网络上为用户提供个性化的网络服务, 用户需求的业务完成后, VRM 释放该 VN 占用的网络资源, 等待 SP 的再一次虚拟资源请求, 进而完成 FiWi 网络的虚拟化。

本文以满足业务不同 QoP 保护需求为目标, 对区分 QoP 的虚拟网络映射问题进行混合规划建模。首先对虚拟网络请求及底层物理网络的模型和文中所用的符号、变量进行说明, 如表 1 所示。

表 1 符号及变量说明

符号及变量	定义
N^S	物理设备集合
E^V	虚拟链路集合
$C(n_i)$	物理节点 i 的处理能力
$c_k(n^v)$	第 k 个虚拟网映射所需处理能力
e_{ij}	i 到 j 的链路
$r(e_{ij})$	可用带宽
$B(e_{ij})$	e_{ij} 总带宽
$b_k(e^v)$	第 k 个虚拟网映射占用带宽
p_u	主路径映射方案
b_u	备份路径映射方案
l	第 l 级 QoP 保护方案

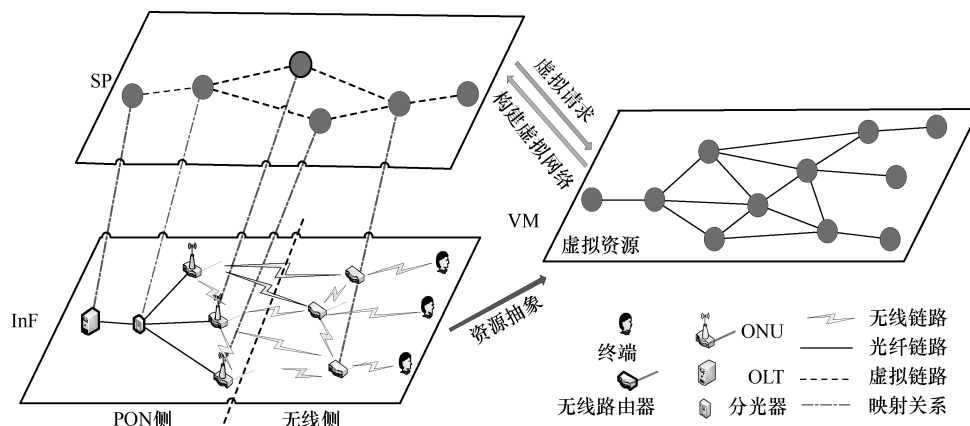


图 1 融合网络虚拟化模型

设备供应商作为基础设施层为虚拟化管理层提供物理资源，并将资源信息以加权无向图 $G^S = (N^S, E^S)$ 的方式同步到虚拟化管理层，其中， N^S 表示所有物理设备的集合，包括 OLT、ONU、分光器、无线路由器等； E^S 表示所有物理链路的集合，包括光纤链路、无线链路。虚拟化管理层将抽象得到的虚拟资源表示为 $G^V = (N^V, E^V)$ ，其中， N^V 表示所有虚拟节点的集合， E^V 表示所有虚拟链路的集合。节点属性包括节点的 CPU 处理能力及位置、价格等信息，链路属性包括链路的总带宽及可用带宽等信息。

令 x_i^m 表示虚拟节点 m 对物理节点 i 的映射情况，当虚拟节点 m 映射到物理节点 i 上时 x_i^m 值为 1，否则 x_i^m 值为 0。即

$$x_i^m = \begin{cases} 1, & \text{虚拟节点 } m \text{ 映射到底层物理节点 } i \text{ 上} \\ 0, & \text{否则} \end{cases} \quad (1)$$

由于虚拟网络共享底层物理网络，不同保护等级的业务对应的虚拟节点映射在同一个物理节点上，因此，物理节点剩余处理能力为该节点总处理能力与已经映射到该节点上的业务占用的处理能力之差，如式(2)所示。

$$r(n_i^s) = C(n_i^s) - \sum_{k=1}^K c_k(n^v) x_i^m \quad (2)$$

其中， $C(n_i)$ 表示物理节点 i 的处理能力， $c_k(n^v)$ 指第 k 个虚拟网络占用节点 i 的处理能力。同样，对于链路映射过程，令 M_{ij}^{mm} 表示链路映射关系，当虚拟链路 (m, n) 映射到物理链路 (i, j) 上时， M_{ij}^{mm} 为 1，否则为 0，即

$$M_{ij}^{mm} = \begin{cases} 1, & \text{虚拟链路 } (m, n) \text{ 映射到物理链路 } (i, j) \text{ 上} \\ 0, & \text{否则} \end{cases} \quad (3)$$

进而，物理链路的可用带宽表示为

$$r(e_{ij}) = B(e_{ij}) - \sum_{k=1}^K b_k(e^v) M_{ij}^{mm} \quad (4)$$

其中， $B(e_{ij})$ 指物理链路 e_{ij} 的总带宽， $b_k(e^v)$ 表示第 k 个虚拟网映射到物理链路 e_{ij} 上所占用带宽。即链路可用带宽为链路总带宽与映射到该链路业务占用该链路带宽之差。

SP 负责接收业务请求，当有业务到达时，SP

根据业务特点及 QoP 需求生成面向虚拟化管理层的虚拟网络资源请求，虚拟网管理层根据虚拟网请求组建虚拟网络，然后将组建好的虚拟网络反馈给 SP。最后，通过开放的编程接口将虚拟网络映射到物理网络进行传输。

3 带有区分保护的传输机制

网络虚拟化的全局视角及屏蔽异构性等优势为融合网络多路径选择过程提供了更加准确的网络状态信息。为了更好地利用虚拟化为用户提供网络服务，同时有效地减轻无线域网络对 FiWi 接入网吞吐量的约束，本文将业务在 WMN 通过 k 条不相交路径进行多路径传输，并在 ONU 处进行汇聚重组，减少多路径引起的数据分组乱序，改善业务 QoS。由于光纤链路能满足单链路传输所需的带宽，且故障链路的数据可通过负载转移机制在相邻光纤传输，因此在 PON 侧采用单路径传输，然后根据用户需求的 QoP 及所能支付的费用，基于链路恢复概率选择相应 QoP 需求等级的备份路径进行区分保护，最后通过启发式灵活服务等级算法进行求解，以提高网络传输可靠性。

3.1 路径 QoP 等级量化

基于恢复概率进行区分保护的 QoP 策略中，链路的 QoP 等级由传输路径的平均可恢复概率，即可被替换的概率 P_{s_u} 确定， P_{s_u} 越大，该路径的 QoP 等级越高，反之越低。 $u = (f, d, l)$ 表示用户请求业务，其中， f 表示源节点， d 表示目的节点， l 表示第 l 级 QoP 保护； $s_u = (p_u, b_u, l)$ 表示虚拟化管理层对请求业务 u 提供的服务方案，其中， p_u 表示主路径映射方案， b_u 表示备份路径映射方案， l 表示为该服务提供的第 l 级 QoP 保护方案。

路径的平均可恢复概率由组成路径的链路恢复概率 $P_{s_u}^{\bar{e}}$ 决定，其中， \bar{e} 表示故障路径。而链路恢复概率与共享保护资源中的业务量 η_{s_u} 有关，故障链路共享备份资源的业务量越少，故障链路可恢复的概率越大，反之越小。 η_{s_u} 为同一时刻业务备份路径上与之共用备份资源的故障业务量，如式(5)所示。

$$\eta_{s_u} = \sum_{s_u \in S - \{s_u\}} \left(F_{p_u} \sum_{B_e \in b_u} \sum_{B_e \in b_u} Z_{c_e}^e \right), \forall e \in p_u, \forall u \in U \quad (5)$$

$$\text{s.t. } F_{p_v} = \begin{cases} 1, \exists p_v \text{ 失败} \\ 0, \text{ 否则} \end{cases} \quad (6)$$

$$Z_{c_e}^c = \begin{cases} 1, B_e = B_e' \\ 0, \text{ 否则} \end{cases}$$

其中, F_{p_v} 为二进制变量, 当业务 u 的传输路径故障的同时存在一个业务 v 的传输链路也故障, 值为 1, 否则为 0; $Z_{c_e}^c$ 为二进制变量, 当业务 u 、业务 v 的备份路径相同时值为 1, 否则为 0; B_e 、 B_e' 分别为业务 u 、业务 v 的备份路径。

本文设定同一 QoP 等级的业务共享备份资源, 即当链路故障时各业务均等概率获得备份资源, 因此业务 u 的传输链路可恢复概率为共享备份路径的故障业务量的倒数, 如式 (7) 所示。

$$p_{s_u}^{\bar{e}} = \frac{1}{1 + \eta_{s_u}} \quad (7)$$

由式(7)可知, 当业务 u 的传输链路故障时, 若其备份保护链路上没有与之共享备份资源的其他业务故障, 则 $\eta_{s_u} = 0$, 业务 u 的传输链路可恢复概率 $p_{s_u}^{\bar{e}} = 1$, 否则, 共享比例越高, 可恢复概率越低。

本文在 WMN 中利用网状拓扑结构进行多路径传输, 因此链路状态互相独立, 由此可知, 业务可恢复概率为各链路可恢复概率的期望值, 如式(8)所示。

$$P_{s_u} = \frac{\sum_{\forall e \in p_u} P_{s_u}^{\bar{e}}}{|p_u|} \quad (8)$$

其中, $|p_u|$ 指业务 u 所经过的链路数量。式(8)即本文用于定义路径故障时划分路径 QoP 级别的标准。虚拟化管理层在寻找业务传输路径时可根据用户业务所要求的 QoP 等级 (如 $M\%$ 的恢复概率) 灵活选择合适路径进行资源分配。

3.2 目标函数

本文目的是满足用户 QoP 保护需求的同时最小化底层网络资源映射开销。为充分利用网络资源并提高服务质量, 对于同一目标 ONU 但较低 QoP 需求的业务, 首先判断其是否能部署到已经建立的具有较高 QoP 等级的剩余节点、链路资源中。如果剩余资源无法满足较低等级 QoP 要求的业务, 则为其分配相应保护等级的节点、链路资源, 因此, 在已知网络拓扑 G^S 、 G^V 和节点、链路代价的情况下,

可利用网络虚拟化全局视角对一组带有 QoP 需求的业务 U 提供解决方案, 其中 $U = \{u_1, u_2, \dots, u_{|u|}\}$ 表示业务请求集合, $|u|$ 表示业务的数量。通过多目标优化, 使得解决方案最大限度地减少被阻止的业务数量 f_1 及未得到备份保护的作业数量 f_2 , 并且使网络开销 f_3 最小。对该问题进行混合规划建模, 具体表达式如式(9)所示。

$$\min f = [f_1, f_2, f_3] \quad (9)$$

其中, f_1, f_2, f_3 分别表示为

$$f_1 = \sum_{u \in U} F_{p_u} \quad (10)$$

$$f_2 = \sum_{u \in U} F_{b_u} \quad (11)$$

$$f_3 = \sum_{u \in U} \sum_{e_{ij} \in E} \sum_{n^s \in V} [c_{n^s} (\sigma_{n^s}^{p_u} + \sigma_{n^s}^{b_u}) + c_{e_{ij}} (\sigma_{e_{ij}}^{p_u} + \sigma_{e_{ij}}^{b_u})] \quad (12)$$

$$F_{p_u} = \begin{cases} 1, p_u \neq \phi \\ 0, p_u = \phi \end{cases} \quad F_{b_u} = \begin{cases} 1, b_u = \phi \\ 0, b_u \neq \phi \end{cases}$$

$$\text{s.t. } \sigma_{n^s}^{p_u} = \begin{cases} 1, n^s \in p_u \\ 0, n^s \notin p_u \end{cases} \quad \sigma_{n^s}^{b_u} = \begin{cases} 1, n^s \in b_u \\ 0, n^s \notin b_u \end{cases}$$

$$\sigma_{e_{ij}}^{p_u} = \begin{cases} 1, e_{ij} \in p_u \\ 0, e_{ij} \notin p_u \end{cases} \quad \sigma_{e_{ij}}^{b_u} = \begin{cases} 1, e_{ij} \in b_u \\ 0, e_{ij} \notin b_u \end{cases} \quad (13)$$

其中, F_{p_u} 为二进制变量, 当业务被拒绝时, F_{p_u} 值为 1, 否则为 0; F_{b_u} 为二进制变量, 当业务 u 的备份路径集为空时说明业务 u 没有收到相应保护, F_{b_u} 值为 1, 否则为 0; c_n 、 c_e 分别表示节点和链路的代价; $\sigma_{n^s}^{p_u}$ 为二进制变量, 表示当业务 u 的传输路径经过节点 n^s 时为 1, 否则为 0; $\sigma_{n^s}^{b_u}$ 为二进制变量, 表示当业务 u 的备份路径经过节点 n^s 时为 1, 否则为 0; $\sigma_{e_{ij}}^{p_u}$ 为二进制变量, 表示当业务 u 的传输路径经过链路 e_{ij} 时为 1, 否则为 0; $\sigma_{e_{ij}}^{b_u}$ 为二进制变量, 表示当业务 u 的备份路径经过链路 e_{ij} 时为 1, 否则为 0。

3.3 基于路径恢复概率的 QoP 策略

对于规模较大的虚拟化 FiWi 网络, 本文提出一种灵活的服务等级区分算法用于业务可靠传输。该算法通过构建广度优先搜索树^[13]寻找映射节点, 通过遗传算法寻找链路映射方案,

给定底层物理网络拓扑和带有 QoS 保护需求的虚拟网络映射。当网络故障发生时，所提策略要能够保障不同用户的 QoS 需求，同时最小化网络开销。

算法首先构建广度优先搜索树 G_V 进行节点分配。选取虚拟网络中节点容量最大的作为根节点，容量最小的作为目的节点，并对每个虚拟节点建立满足条件的映射节点集合，同时以广度优先的方式，根据处理能力将虚拟节点和物理节点进行模糊匹配，映射存在 k 条最小开销路径的物理节点上。在进行链路映射时，文献[14]表明多路径业务传输可提高资源利用率并减少资源冗余备份，然而路径数超过 5 时会导致节点分流、合流开销和时延的明显增大。因此，本文将路径数设置为 $2 \leq k \leq 5$ ，满足条件的路径集合记作 $\{P^2, P^3, P^4, P^5\}$ ，并根据节点和链路代价 c_n 、 c_e 计算其总开销，然后按照开销最小的路径方案 P^m 在无线侧进行链路映射，最后在 ONU 处聚合重组后继续传输。多路径映射策略伪代码如算法 1 所示。

算法 1 多路径映射策略伪代码

```

1) function)  $MpMS(G^S, G^V, \xi_N)$  // 多路径映射函数,  $\xi_N$  为节点映射关系
2) for all  $e^v \in E^V$  do
3)  $\forall k \in \{2, 3, 4, 5\}$ :  $P^k \leftarrow \phi \wedge \text{cost}(P^k) \leftarrow \infty$ 
// 初始化映射链路  $P^k$ 
4) for  $k \in \{2, 3, 4, 5\}$  do
5)  $\mathbb{R}^S \leftarrow E^S$  // 初始化可用链路集合
6) for  $j=1, k$  do
7)  $Q \leftarrow \text{Dijkstra}(N^S, \mathbb{R}^S, \xi_N(e_s^v), \xi_N(e_u^v), \frac{b(e^v)}{k})$  // 寻找满足条件路径
8)  $P^k \leftarrow P^k \cup Q$  // 满足条件路径赋值
9)  $\mathbb{R}^S \leftarrow \mathbb{R}^S - P^k$  // 更新可用链路集合
10) end for
11) end for
12)  $P^* \leftarrow \min(P^2, P^3, P^4, P^5)$  // 将 4 种方案中开销最小的方案作为映射方案
13) if  $\text{cost}(P^*) = \infty$  then

```

```

14) return  $\phi$ 
15) end if
16)  $P_U \leftarrow P^*$  // 将开销最小的方案作为映射方案输出
17) end for
18)  $\forall e^s \in E^S \cap P^*$ : update  $r(e^s)$  // 更新链路可用资源
19) return  $P_U$ 
20) end function

```

由于遗传算法采用种群搜索，可实现信息交互、全局解空间搜索，更符合网络虚拟化的全局化管理方式，并且，遗传算法中只考虑输入输出关系的黑箱式操作可简化虚拟网映射关系复杂度。本文利用遗传算法选择备份路径，提供满足业务 QoS 需求的备份资源，保证业务传输的可靠性。根据遗传算法的执行流程和业务区分保护设计映射的求解要求，本文通过如下步骤来实现算法得出优化方案。

1) 编码模式

编码模式直接影响着目标可行解和遗传形式间的对应关系，而染色通过遗传所得的可行解是否较优则需要通过目标函数来验证^[15]。根据虚拟化 FiWi 网络区分 QoS 需求的设计优化目标，本文将业务请求的映射方案作为染色体 S ，如式(14)所示。

$$S = \{s_{u_1}, s_{u_2}, \dots, s_{u_{|U|}}\} \quad (14)$$

其中， s_u 作为基因，包含传输路径和备份路径的映射方案； $|U|$ 代表整个 FiWi 网络所有带有 QoS 需求的业务总量。

图 2 描述了染色体基因的基本结构。其中， S 为染色体； s_{u_i} 作为第 i 个基因，表示第 i 个业务请求带有 QoS 的备份路径映射方案， a 、 b 、 c 、 y 、 z 表示映射到 FiWi 网络的网状网节点 (MP, mesh point) 和网状网接入点 (MAP, mesh access point)， L_n 为 QoS 等级。

2) 创建初始群体

为在过程开始获得种群基因的多样性，初始群体的个体 S 均随机产生，即移动终端 (STA, station) 和 ONU 间的路径随机选取，形成初始群体 $\Omega_{g=0}$ ，然后初始群体通过遗传操作寻找满足条件的备份路径配备方案。

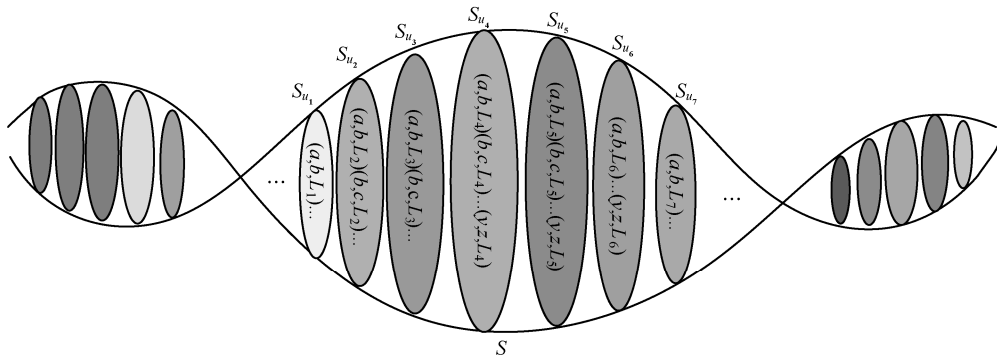


图 2 染色体结构

3) 确定适应值函数

被阻止业务数量 f_1 和未备份保护的... 将它们与网络开销 f_3 一起作为目标函数共同优化...

S_f = [f_1, f_2, f_3] (15)

通过遗传算法的迭代, 产生出使目标函数 S_f 最小的映射方案。

4) 遗传操作

遗传操作的意义是通过遗传法则随机地改变群体中的个体, 进而在可行解得范围中尽快地搜索到问题的最优解[16]。

在选择运算时, 为了保证群体中较优个体不会在遗传过程中丢失, 并且在遗传过程中不断优化个体性能...

分别计算群体中个体的适应值, 即 S_f。其次, 将较优的个体保留, 并判断遗传是否达到截止条件。如果达到截止条件则进行基因突变操作...

然后, 进行交叉运算。交叉运算即利用当前群体中所包含的遗传信息产生出性能更加优良的新个体... 重复该过程 |Omega_g|/2 次以...

最后, 进行变异运算。为了以当前群体为基础

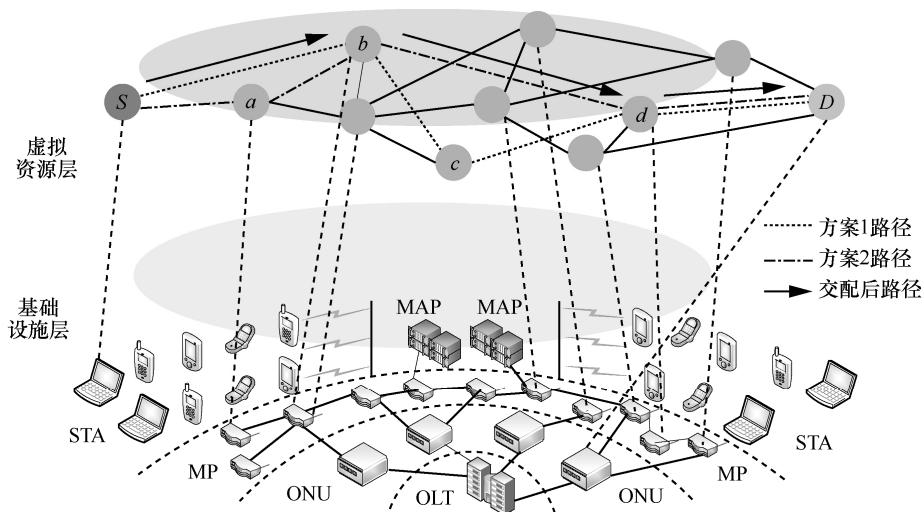


图 3 备份路径选择过程

完成全部可行解的搜索(即全局寻优), 算法还需要进行变异操作。本文采用对群体中的个体以概率 $p(m)$ 被随机生成的另一个新个体替换, 并将变异后的个体 $\Omega_{\text{mutated}_g}$ 与之前较优的个体 $\Omega_{\text{crossed}_g}$ 通过目标函数分别进行比较。如果 $\Omega_{\text{mutated}_g}$ 的目标函数优于 $\Omega_{\text{crossed}_g}$, 则对该个体执行变异, 即 $\Omega_{\text{final}_g} = \Omega_{\text{mutated}_g}$ 。否则仍然维持原来个体不变, 即 $\Omega_{\text{final}_g} = \Omega_{\text{crossed}_g}$ 。个体比较规则定义如下: 分别比较 $\Omega_{\text{mutated}_g}$ 和 $\Omega_{\text{crossed}_g}$ 的目标函数 S_f , 如果变异后的函数 $f_1^* \leq f_1$, 则选取变异方案; 如果 $f_1^* = f_1$, 但 $f_2^* \leq f_2$ 则选取变异方案; 如果 $f_1^* = f_1, f_2^* = f_2$, 但 $f_3^* \leq f_3$ 则选取变异方案; 否则输出原方案 $\Omega_{\text{final}_g} = \Omega_{\text{crossed}_g}$ 。

综上所述, 算法的主要过程如下: 首先构建广度优先搜索树; 其次, 依据处理能力将物理节点与虚拟节点进行模糊匹配, 并对每个虚拟节点建立 FiWi 网络中满足条件的候选映射节点集合; 再次, 计算该节点的候选映射节点与上一个映射成功节点之间的最优路径个数 k , 如果 $k \geq 2$ 则进行映射, 否则继续查找; 最后, 根据上述链路映射策略在 WMN 中进行多路径链路映射, 并对带有区分 QoP 的备份链路进行映射。

本文所提算法 FLSDA 的区分 QoP 的备份链路映射策略的伪代码如算法 2 所示。

算法 2 区分 QoP 备份链路选择策略伪代码

```

1) input:  $U, Q, G^S, G^V, c_n, c_e // U$  业务请求集合,  $Q$  为 QoP 等级集合
2) output:  $B_U$ 
3) initialize initial population  $\Omega_{g=0} //$  初始化种群
4) while stop condition do not meet do
5)    $L = \phi //$  初始化链路集合
6)    $S_f = [f_1, f_2, f_3] = [0, 0, 0] //$  初始化目标函数值
7)   for all  $u \in U$  do
8)     if primary path  $P_U = \phi$  then
9)        $f_1 = f_1 + 1 //$  通过式(6)计算被拒绝的业务量
10)    else
11)       $L = L \cup P_U$ 
12)    if  $B_U \neq \phi$  and  $q_u \neq q_{|Q|}$  then
13)       $L = L \cup B_U //$  备份链路不为空

```

且 QoP 不是最低级说明业务有保护

```

14)    else
15)       $f_2 = f_2 + 1 //$  通过式(7)计算不受保护的
        业务量
16)    end if
17)  end if
18)     $f_3 = \sum_{u \in U} \sum_{e_{ij} \in E} \sum_{n^s \in V} [c_{n^s} (\sigma_{n^s}^{p_u} + \sigma_{n^s}^{b_u}) +$ 
         $c_{e_{ij}} (\sigma_{e_{ij}}^{p_u} + \sigma_{e_{ij}}^{b_u})] //$  通过式(9)计算开销
19)  end for
20)  return  $S_f$ 
21) apply binary tournament to  $\Omega_g$ , obtaining  $\Omega_{\text{selected}_g} //$  通过淘汰制选择优良个体
22) cross  $\Omega_{\text{selected}_g}$ , obtaining  $\Omega_{\text{crossed}_g} //$  杂交优良个体, 获得新一代染色体
23) mutate  $\Omega_{\text{crossed}_g}$ , obtaining  $\Omega_{\text{final}_g} //$  以概率  $p(m)$  随机生成新个体, 完成基因突变
24) for all  $S_f^* \in P_g$  do //  $S_f^*$  指通过变异操作后的方案
25)   if  $f_1^* \leq f_1$  then
26)      $S_f \leftarrow S_f^*$ 
27)   else
28)     if  $f_1^* = f_1$  and  $f_2^* \leq f_2$  then
29)        $S_f \leftarrow S_f^*$ 
30)     else
31)       if  $f_1^* = f_1, f_2^* = f_2$  and  $f_3^* \leq f_3$ 
then
32)          $S_f \leftarrow S_f^*$ 
33)       end if
34)     end if
35)   end if
36) end for
37) update best solution  $S_f$  with  $\Omega_{\text{final}_g} //$  用较优方案作为这一代的最终方案
38)  $g \leftarrow g + 1$ 
39) end while
40)  $B_U \leftarrow L$ 
41) return  $B_U$ 

```

3.4 算法复杂度分析

本文所提灵活等级服务区分算法主要由多路径映射及区分 QoP 备份链路选择算法组成, 下面对

算法复杂度进行具体分析。

在多路径映射过程中，首先，在节点分配过程中使用广度优先搜索算法，其算法时间复杂度为 $O(n+e)$ ，其中， n 为物理节点的数量， e 为节点间链路数量。根据处理能力将虚拟节点和物理节点进行模糊匹配，经典模糊匹配的最优时间复杂度为 $O(nlbn)$ 。因此，节点选择过程的整体时间复杂度为 $O(nlbn+n+e)$ 。其次，在链路映射过程中，使用计算最小开销的方法寻找满足条件的路径集合，经过分析可知，最其整体时间复杂度为 $O(e(nlbn+e))$ 。根据上述分析，可得本文多路径映射算法的整体时间复杂度为 $O((nlbn+n+e)(e(nlbn+e)))$ 。

在区分 QoS 的备份链路选择算法中，首先通过目标函数的约束产生映射方案，完成初始父染色体的建立，即满足约束条件的 STA 到 ONU 之间的可用路径，因此其复杂度为 $O(u)$ ，其中 u 为带有 QoS 请求的业务数量；然后进行父染色体的交叉，其过程为两两交叉，因此该过程的复杂度为 $O\left(\frac{u}{2}\right)$ 。在变异阶段，首先是以概率 $p(m)$ 进行替换，然后与之前较优个体进行比较，因此其复杂度为 $O(up)$ 。根据上述分析可得，区分 QoS 的备份链路选择算法的整体时间复杂度为 $O(u+\frac{u}{2}+up)$ 。

综上所述，本文所提灵活等级服务区分算法复杂度的最高指数形式为常值，即为多项式时间。

4 数值结果分析

本文使用 NS2 (network simulator 2) 仿真平台验证所提满足不同 QoS 需求的灵活服务等级区分算法 FLSDA 的性能，并分别与 2 种典型保护算法进行比较，其中包括文献[17]提出的全备份保护算法 (FBPA, full backup protection algorithm) 和文献[18]提出的比例备份保护算法 (PBPA, proportional backup protection algorithm)。在全备份保护算法 FBPA 中，每条虚拟链路映射到由 Dijkstra 算法得到满足条件的 2 条不相交的底层路径上，2 条路径中较短的一条作为主路径进行传输，另一条作为备份进行保护。而比例备份保护算法 PBPA 采用不完全保护措施，业务需求的保护比例由 q 表示，其中 $q \in [0,1]$ 。当 $q=1$ 时算法与 FBPA 相同；当 $q=0$ 时，则不分配备份资源；当 $0 < q < 1$ 时为共享保护，发生故障时

受影响的虚拟链路尽可能地将其业务转移到备份路径上传输，当共享相同备份路径的多条虚拟链路同时受故障影响时则采用公平共享策略分配备份资源。

网络拓扑由 GT-ITM 工具随机产生^[19]，本文的主要仿真参数如表 2 所示。

表 2 仿真参数设置

参数设定	参数值
OLT 数	1
ONU 数	8
无线路由器数	64
光纤链路带宽/(Gbit·s ⁻¹)	10
无线链路带宽/(Mbit·s ⁻¹)	54
光侧节点处理能力/GHz	50
无线侧节点处理能力/GHz	20
路径拆分开销/ μ s	100
路径合流开销/ μ s	100
物理节点转发开销/ μ s	[20,70]
虚拟节点资源需求/GHz	[5,15]
虚拟链路带宽请求/(Mbit·s ⁻¹)	[5,50]

其中，每个虚拟节点间以等概率设置虚拟链路，即 n 个节点的虚拟网络平均含 $\frac{n(n-1)}{4}$ 条链路。设置虚拟网络请求服从 $\lambda = 0.05$ 的泊松分布，且每一个虚拟网络请求的活跃时间服从均值为 1 000 时间单位的指数分布。

4.1 不同 QoS 等级的网络资源开销

为验证本文所提算法 FLSDA 的性能，首先对 FLSDA 的网络资源开销进行验证。考虑到节点处理能力远远大于虚拟节点请求，且节点失效的概率较小，本文仿真中的网络资源开销以链路带宽资源开销为依据进行验证。在不同网络请求量 U_n 下，网络资源开销与 QoS 等级的关系如图 4 所示。可以看出当 U_n 一定时，随着 QoS 等级的增大，网络资源开销也随之增大。这是因为当 QoS 等级相同时，随着请求数量的增大网络拥塞导致故障的概率也会增大，因此需要更多的备份资源；QoS 等级增大，备份资源的比例随之增大，因此带宽开销随之增大。

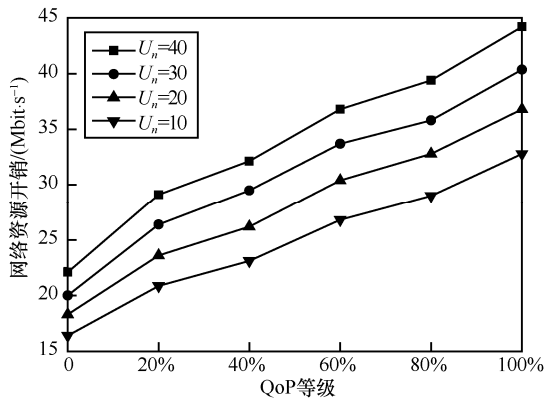


图 4 不同 QoS 等级的网络资源开销

4.2 不同算法的网络资源开销

图 5 为不同算法的网络资源开销。比例备份 PBPA 算法和本文所提 FLSDA 算法会根据业务需求的保护比 q 进行备份资源的调整，因此，保护比例 q 较低时 2 种算法的开销也较低，随着 q 的增大算法开销也增大。在全备份保护算法 FBPA 中，采用 2 条链路进行完全备份作为保护，因此备份产生的开销不受保护比例 q 的影响，且相当于 $q=1$ 时比例备份算法 PBPA 算法的开销。可以看出，FBPA 开销最大，PBPA 次之，FLSDA 在满足用户不同 QoS 需求的同时，相比于前两者需要更少的底层网络资源。在 $q=0.5$ 时，FLSDA 比 FBPA 节省了约 27% 的带宽资源。这是因为 FBPA 在虚拟网络映射时将每条虚拟链路映射到满足条件的 2 条不相交的底层路径上，一条作为主路径进行传输，另一条作为备份进行保护，所以带宽开销最大。虽然 FLSDA 和 PBPA 均采用不完全保护措施，但 FLSDA 采用多路径映射策略，链路失效的几率较小，因此消耗更少的备份带宽。

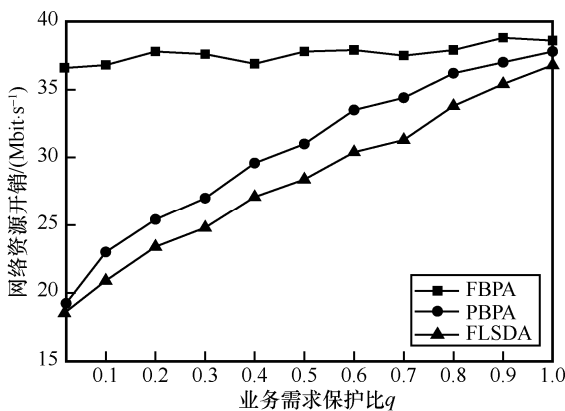


图 5 不同算法的网络资源开销

4.3 虚拟网络故障修复率

图 6 是 3 种算法对虚拟网络故障修复率的影响。可以看出 FBPA 虚拟网络故障修复率最高，几乎为 1；本文的 FLSDA 次之，约为 80%；PBPA 的虚拟网络故障修复率最低，平均为 60%。这是因为全备份保护算法 FBPA 对所有业务均采用与主链路带宽相同的备份链路进行全备份保护，当网络故障时，可以迅速将业务转移到备份路径进行传输，因此，故障修复率较高。比例备份保护算法 PBPA 采用不完全保护措施且主路径是单路径传输，当 q 较小时，备份资源不足以保障主链路上的业务传输，因此网络故障修复率相对最低。而 FLSDA 虽然也属于不完全保护，但其采用多路径传输，底层的一条物理链路失效只会影响到该虚拟链路带宽的失效，备份资源满足该链路上分配的带宽请求的概率较大，因此，其网络故障修复率要高于 PBPA。

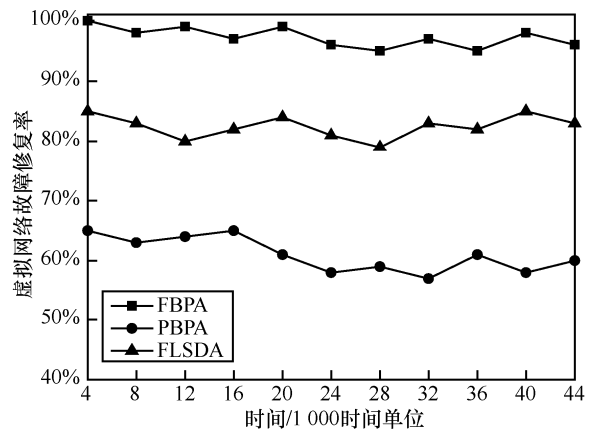


图 6 虚拟网络故障修复率

4.4 虚拟网络请求接受率

采用备份路径构造传输算法能够使虚拟网络获得较高的故障修复率，但由于备份资源占用了大量的网络可用资源，导致用于传输业务的网络资源减少。图 7 是 3 种算法的虚拟网络请求接受率对比。由图可知 FLSDA 的网络请求接受率相比 PBPA 平均高出 7%，相比 FBPA 平均高出 16%。这是因为 FBPA 采用全备份保护，由图 5 的网络资源开销可以看出对于相同的网络请求，FBPA 需要的网络资源最多，因此，其接受率最小。相比于 PBPA，FLSDA 采用多路径传输，能更充分地利用网络可用资源，因此其网络请求接受率最大。

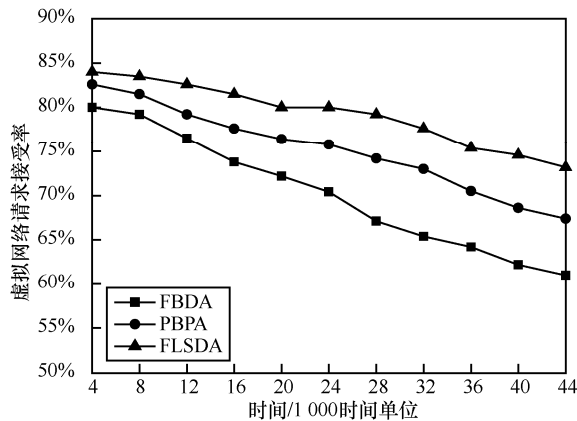


图 7 虚拟网络请求接受率

4.5 平均收益开销比

为了分析算法的网络效益, 本文分别对 3 种算法的收益开销比进行仿真分析, 其中收益指用户所支付的费用, 表示为

$$R(G_v) = \sum_{n_v \in N_v} \alpha s(n_v) + \sum_{e_v \in E_v} \beta b(e_v) \quad (16)$$

其中, α 、 β 分别为单位节点和带宽资源用户所支付的费用, $s(n_v)$ 、 $b(e_v)$ 分别为业务所请求的节点资源、带宽资源。

开销指网络分配给用户网络资源的开销, 表示为

$$C(G_s) = \sum_{n_s \in N_s} s(n_s) + \sum_{e_s \in E_s} b(e_s) \quad (17)$$

其中, $s(n_s)$ 、 $b(e_s)$ 分别网络为用户网络请求分配的节点资源、带宽资源。

仿真过程中设置 α 、 β 均为 1, 仿真结果如图 8 所示。可以看出 FLSDA 的平均收益开销比平均高出 PBPA 的平均收益开销比约 16%, 相比 FBPA 平均高出 43%。主要是因为对于相同的网络资源请求, FBPA 分配给用户的网络资源最多, 因此, 其平均收益开销比最少。而 FLSDA 采用多路径传输,

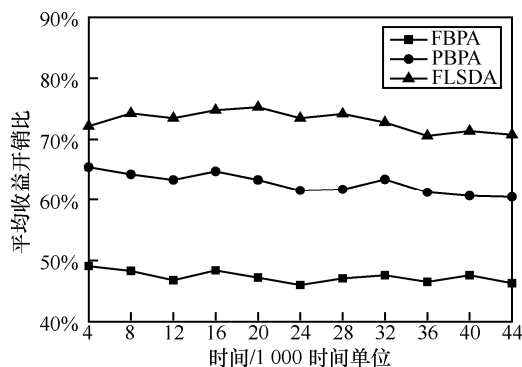


图 8 平均收益开销比

对于相对较低的 QoP 需求, 几乎不用额外分配备份资源, 因此平均所需分配的备份资源较少, 所以其平均收益开销比最高。

5 结束语

本文针对网络用户不同 QoP 需求的网络虚拟化映射问题进行了研究, 提出一种带有区分保护的 FiWi 网络可靠传输机制, 并设计了一种基于恢复概率区分 QoP 的启发式算法对该问题进行求解。算法根据网络的可恢复概率定义链路的 QoP 等级, 然后依据用户需求的 QoP 及所能够支付的费用, 通过遗传算法为其灵活地分配备份保护资源。实验结果表明算法在平均收益开销比和底层网络资源开销等指标上具有较高优势, 从而在满足用户 QoP 需求, 提高网络资源利用率的同时, 为用户提供更灵活的虚拟网络数据传输。

参考文献:

- [1] WU D P, YAN J J, WANG H G. Social attribute aware incentive mechanism for device-to-device video distribution[J]. IEEE Transaction on Multimedia, 2017, 19(8): 1908-1920.
- [2] 王汝言, 周超, 吴大鹏, 等. 自适应延迟感知的光无线混合宽带接入网节能机制[J]. 上海交通大学学报, 2017, 51(1):105-112. WANG R Y, ZHOU C, WU D P, et al. Adaptive energy saving mechanism with delay aware in hybrid optical-wireless broadband access networks[J]. Journal of Shanghai Jiaotong University, 2017, 51(1):105-112.
- [3] BEYRANVAND H, LIM W, MAIER M, et al. Backhaul-aware user association in FiWi enhanced LTE-a heterogeneous networks[J]. IEEE Transactions on Wireless Communications, 2015, 14(6):2992-3003.
- [4] WU D P, ZHANG H P, WANG H G, et al. Quality of protection (QoP)-driven data forwarding for intermittently connected wireless networks[J]. IEEE Wireless Communication, 2015, 22(4): 66-73.
- [5] CHOWDHURY S R, AHMED R, KHAN M M A, et al. Dedicated protection for survivable virtual network embedding[J]. IEEE Transactions on Network & Service Management, 2016, PP(99):1.
- [6] LIU J, GUO H, NISHIYAMA H, et al. New perspectives on future smart FiWi networks: scalability, reliability, and energy efficiency[J]. IEEE Communications Surveys & Tutorials, 2017, 18(2):1045-1072.
- [7] RAHMAN M R, BOUTABA R. SVNE: survivable virtual network embedding algorithms for network virtualization[J]. IEEE Transactions on Network & Service Management, 2013, 10(2):105-118.
- [8] YEOW W L, WESTPHAL C, KOZAT U C. Designing and embedding reliable virtual infrastructures[J]. ACM SIGCOMM Computer Communication Review, 2011, 41(2):57-64.
- [9] CAI Z, LIU F, XIAO N, et al. Virtual network embedding for evolving networks[C]// Global Telecommunications Conference. IEEE, 2010:1-5.
- [10] SASAKI G H. Quality of protection (QoP): a quantitative unifying paradigm to protection service grades[J]. Proceedings of SPIE - The International Society for Optical Engineering, 2001, 3(10):12-23.
- [11] 刘光远, 双锴, 苏森. 区分服务 QoP 的可生存虚拟网络映射算法研究[J]. 通信学报, 2013, 34(12):79-83.

- LIU G Y, SHUANG K, SU S. Survivable virtual network mapping with differentiated services QoP[J]. Journal on Communications, 2013, 34(12): 79-83.
- [12] PUTRA E H, HIDAVAT R, WIDYAWAN, et al. Cross-layer design of wireless multimedia sensor network based on IEEE 802.11e EDCA and H.264/SVC[C]// International Conference on Science in Information Technology. IEEE, 2015:67-72.
- [13] FU M, HE M, LE Z, et al. Performance evaluation of the survivability schemes in WOBAN: a quality of recovery (QoR) method[J]. International Journal of Communication Systems, 2015, 28(5):818-841.
- [14] KHAN M M A, SHAHRIAR N, AHMED R, et al. Multi-path link embedding for survivability in virtual networks[J]. IEEE Transactions on Network & Service Management, 2016, 13(2):253-266.
- [15] AURZADA F, LEVESQUE M, MAIER M, et al. FiWi access networks based on next-generation PON and gigabit-class WLAN technologies: a capacity and delay analysis[J]. IEEE/ACM Transactions on Networking, 2014, 22(4):1176-1189.
- [16] SEBBAH S, JAUMARD B. Differentiated quality-of-recovery in survivable optical mesh networks using p -structures[J]. IEEE/ACM Transactions on Networking, 2012, 20(3):798-810.
- [17] RAHMAN M R, AIB I, BOUTABA R. Survivable virtual network embedding[C]//International Conference on NETWORKING. IFIP 2014: 40-52.
- [18] AYOUBI S, CHEN Y, ASSI C. Towards promoting backup-sharing in survivable virtual network design[J]. IEEE/ACM Transactions on Networking, 2016, 24(5):3218-3231.
- [19] NANDI S K. Topology generators for software defined network testing[C]// International Conference on Electrical, Electronics, and Optimization Techniques. IEEE, 2016:2984-2989.

[作者简介]



王汝言（1969-），男，湖北浠水人，博士，重庆邮电大学教授、博士生导师，主要研究方向为泛在网络、多媒体信息处理等。



高毅爽（1995-），男，四川广元人，重庆邮电大学硕士生，主要研究方向为光无线融合网络。



陈霄（1991-），男，河北邯郸人，重庆邮电大学硕士生，主要研究方向为光无线融合网络。