Assessing service survivability under failure conditions in reliable multipath network testbed

Ryota Kawase\textsuperscript{1a)}, Taichi Okumura\textsuperscript{1}, Masaki Murakami\textsuperscript{1}, Yoshihiko Uematsu\textsuperscript{1}, Takashi Kurimoto\textsuperscript{1}, Satoru Okamoto\textsuperscript{1}, and Naoaki Yamanaka\textsuperscript{1}

\textsuperscript{1} Graduate School of Science and technology, Keio University

Hiyoshi, Kohoku-ku, Yokohama, Kanagawa 223-8522, Japan

\textsuperscript{a)} ryota.kawase@yamanaka.ics.keio.ac.jp

Abstract: This study reports that the expected capacity guaranteed routing (ECGR) testbed was built and the face recognition service was provided in the testbed. ECGR, which guarantees that the expected capacity calculated based on link failure probability exceeds the requested capacity of flows, has been proposed. On the ECGR testbed, we verify that the assigned expected capacity meets the required capacity. Fault tolerance experiments were conducted to evaluate the impact of not only single link failure but also multiple link failures on the service. From these evaluations, we verified that it is possible to provide highly reliable services on the ECGR.

Keywords: multipath routing, failure, expected capacity guarantee routing, face recognition, human tracking

Classification: Transmission systems and transmission equipment for communications

References

[1] O. Gerstel and R. Ramaswami, “Optical layer survivability-an implementation perspective,” in IEEE Journal on Selected Areas in Communications, vol. 18, no. 10, pp. 1885-1899, Oct. 2000, doi: 10.1109/49.887910.

[2] S. S. Lumetta, M. Medard and Yung-Ching Tseng, “Capacity versus robustness: a tradeoff for link restoration in mesh networks,” in Journal of Lightwave Technology, vol. 18, no. 12, pp. 1765-1775, Dec 2000, doi: 10.1109/50.908723.

[3] J. Zhong, W. Guo and Z. Wang, “Study on network failure prediction based on alarm logs,” 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-7, DOI:10.1109/ICBDSC.2016.7460337.

[4] K. Ishibashi, T. Hayashi and K. Shiomoto, “Advanced network design and operation by machine learning and data analysis,” (written in Japanese) NTT Technical Journal, vol. 27, no. 12, pp. 29-33, December 2015.

[5] S. Sekigawa, S. Okamoto, N. Yamanaka and E. Oki, "Expected Capacity Guaranteed Routing based on Dynamic Link Failure Prediction," 2019 International Conference on Computing, Networking and Communications
1 Introduction

The failure probability of networks will be increasing due to generalization of network equipment. To overcome high link/node failure probability, dedicated path protection (DPP) which sets two nodes and disjointed link paths between source and destination nodes is popular [1, 2]. DPP requires twice the bandwidth resources of paths because it reserves a spare path uniformly for each path. In addition, since backup paths with the same capacity are prepared for paths with different failure probabilities, a problem exists that backup paths assigned to paths with low failure probabilities tend to become wasted resources. In recent years, failure prediction of networks has researched in various fields [3, 4]. By predicting failure probability, it is possible to allocate capacity according to the failure probability of the path.

Therefore, a new concept, expected capacity guaranteed routing (ECGR), has been proposed [5]. ECGR calculates expected capacity based on the failure probability of the link to achieve the requested expected capacity or higher. Therefore, it is possible to allocate routes according to the magnitude of the link failure probability. Also, by applying a mixed integer linear programming (MILP), the optimal route is selected so that the sum of the product of the distance between the links and the amount of traffic flowing on the links is minimized. Hence, by changing the number of routes to be used according to the requested capacity expected capacity, ECGR can improve the fault-tolerance while preventing a decrease in the efficiency of network resource utilization compared to conventional methods.

In recent years, the network devices in the access metro network have become more and more white-boxed, and it is expected that the surplus computational resources of the CPU resources of the network devices will be provided to the users. By having the surplus computing resources process some of the jobs in the service, the network resources can be used more efficiently. In order to provide services using network devices in the access metro network, it is necessary to have a reliable routing technology that takes into account the failure of each network device. In this research, the validation of the ECGR method to provide reliable services is presented.

2 ECGR testbed

In this research, we constructed an ECGR testbed network based on a multipath forwarding network as shown in Fig. 1, in order to demonstrate the feasibility of providing highly reliable services in ECGR network.

The multipath forwarding network consists of five network switches. In this research, we actually constructed a multipath network using network switches and routers. A picture of it is shown in the lower left corner of Figure 1. Two software routers for a mapper and a demapper are connected as ECGR source/destination.
nodes. The mapper assigns a sequential number to the packets and distributes them based on the results of the ECGR calculations, whereas the demapper performs packet ordering. The mapper also gives a Virtual LAN (VLAN) id to multipath network for forwarding.

Fig. 1. ECGR testbed overview.

The multipath forwarding network is controlled by an ECGR manager and a software-defined networking (SDN) controller. The ECGR manager solves a multipath route selection and bandwidth allocation problem when a service request arrives. Then, ECGR manager sends the result to the SDN controller via REST API. Next, SDN controller reconfigures mapper and demapper using telnet, and multi-path setting using OpenFlow.

3 Experiment of service provisioning

In this research, as an example of a service, a human tracking service is provided in the testbed. Figure 2 shows two types of human tracking services. In the cloud based human tracking service, cloud servers store face recognition files of the missing person to be searched. These files are learned by extracting facial features from multiple photos of the same person so that it can identify the person's face from other photos. The video transmitted from the camera is sent to cloud servers, where the matching is performed. In this case, the time required for person matching become bottlenecks, so high performance machines are required for real-time person tracking. On the other hand, in the cache based human tracking service, face recognition files of a search target that is matched once at cloud servers is stored in the edge server as a cache. From the second detection onward, the edge server detects and tracks the person, thereby reducing the amount of face recognition files to be matched and the number of times to access the cloud, thus enabling real-time person tracking even without high performance machines. Therefore, in this service, even the extra computational resources of the access metro network, which have relatively lower performance than the cloud servers, are expected to be used as machines to provide the service.

As a first step to realize the human tracking service using the computational resources of the access metro network, we confirm the operation of the face recognition service on the ECGR transfer network applied to the access metro network. The face recognition service recognizes and tracks a pedestrian's face.
reflected in the angle of view. As shown in Fig. 1, video frames from the mapper go through the ECGR forwarding network and are processed by the face recognition server on the demapper side. The face recognition service needs to transmit frames according to a reliable routing method, because if the reception of video frames is interrupted, there is a risk of forcing the application to stop. In this research, we verify the feasibility of providing reliable services in the ECGR transfer network.

![Cloud Based Human Tracking Service](image1)

**Fig.2.** Concept of cache based human tracking service.

## 4 Experimentation result

In the experiment, more than one link would occur a failure. The size of one video frame is about 21 Mbit, and a bandwidth of 630 Mbps or more is required for transmission at 30 fps to avoid interruptions. Therefore, when a request for 700 Mbps was sent to the ECGR controller, a path with a low failure probability of 700 Mbps and a path with a high failure probability of 253 Mbps was allocated and transmitted with a throughput of 953 Mbps.

The next step is to make sure that the total expected capacity value meets the required capacity. The following explains how to calculate the expected capacity. The expected capacity value depends on the reliability of the path. The failure probability is also an important parameter to evaluate the reliability. The failure probability of link \((i,j)\) is expressed by Eq. (1).

\[
R_{ij} = e^{-\lambda_{ij}t}
\]  

(1)

In, Eq.(1), \(\lambda_{ij}\) is the failure probability of link \((i,j)\), is the rate at which a failure occurs in link \((i,j)\) within a unit of time. \(R_{ij}\), the reliability of link \((i,j)\), is the probability that the link \((i,j)\) is working within \(t\) time.

Figure 3(a) shows the respective paths for multipath transmission of video frames in the ECGR network. The reliability of path A here is expressed as the product of the reliability of all links, which is shown in Eq. (2).
\[ R_A = R_{24} \cdot R_{46} = e^{-\lambda_{24}t} \cdot e^{-\lambda_{46}t} \]  

(2)

Hence, the total expected capacity value of path A and path B is expressed by Eq. (3).

\[ (Total \ Expected \ Capacity) = b_A \cdot R_A + b_B \cdot R_B \]  

(3)

\( b_A \) [Mbit/sec] is the bandwidth assigned to path A, and \( b_B \) [Mbit/sec] is the bandwidth assigned to path B.

Using the traffic capacity and reliability of each path, the total expected capacity is calculated as in Eq. (4).

\[ (Total \ Expected \ Capacity) = 253 \cdot 0.729 + 700 \cdot 0.755 = 712 > 700 \]  

(4)

The result of Eq. (4) shows that the total expected capacity exceeds the required capacity of 700 Mbps. Thus, the bandwidth is allocated to each route so that the total capacity expectation meets the required capacity. In addition, the bandwidth to be allocated could be reduced to about two-thirds of the bandwidth allocated by DPP.

When path A was disconnected, path B met the 700Mbps requirement and the face recognition service continued without any interruption of video frames.. The view of face recognition service is shown in Figure 3(b). When path B was disconnected, the video frames were transferred at 253 Mbps, so the fps was reduced to one-third of that when no failure occurred, but the face recognition service was confirmed to continue. When failures occurred on both path A and path B, the video frames could not reach the face recognition server. Therefore, the application was terminated forcibly and the face recognition service could not survive.

Then, the probability that the face recognition service could not survive is calculated as the product of the failure rate of path A and the failure rate of path B, which is 6.9%. The events in which the face recognition service does not survive are the extra events of the events that do survive. Since the sum of the probabilities of these events is 1, the survival rate of the face recognition service is obtained as 93.1%.
Therefore, ECGR was able to achieve a high service survival rate while satisfying the required capacity with less bandwidth resource allocation.

5 Conclusions

We built the ECGR testbed and provided the face recognition service in the testbed. As a result, ECGR testbed was able to achieve efficient use of bandwidth resources and high reliability in service provision.

Acknowledgments

This work is partly supported by the R&D of innovative optical network technologies for supporting new social infrastructure project (JMPI00316) funded by the Ministry of Internal Affairs and Communications Japan.