Topology Discovery for Telecommunications-carrier Networks using Equipment Alarms

Atsushi Takada
NTT Network Service Systems Laboratories
NTT Corporation
Tokyo, Japan
atsushi.takada.nv@hco.ntt.co.jp

Naoki Hayashi
NTT Network Service Systems Laboratories
NTT Corporation
Tokyo, Japan
naoki.hayashi.ug@hco.ntt.co.jp

Mizuto Nakamura
NTT Network Service Systems Laboratories
NTT Corporation
Tokyo, Japan
mizuto.nakamura.gm@hco.ntt.co.jp

Naoyuki Tanji
NTT Network Service Systems Laboratories
NTT Corporation
Tokyo, Japan
naoyuki.tanji.vw@hco.ntt.co.jp

Toshihiko Seki
NTT Network Service Systems Laboratories
NTT Corporation
Tokyo, Japan
toshihiko.seki.en@hco.ntt.co.jp

Kyoko Yamagoe
NTT Network Service Systems Laboratories
NTT Corporation
Tokyo, Japan
kyoko.yamagoe.wx@hco.ntt.co.jp

***Abstract*— As for the service assurance operation of telecommunications carriers, accurate information about a network topology which indicates the connection relationships between pieces of network equipment is necessary. However, the network of a telecommunications carrier has several hundreds of thousands of equipment, and its topology is frequently supplemented and modified due to daily construction work and troubleshooting. It is a therefore a problem when incorrect topology information is mixed into the overall topology information. In this paper, we propose a method that can discover the topology between equipment by using alarm information issued by those equipment during construction work or when a failure occurs. The proposed method was evaluated using alarm information generated under in certain commercial configurations (sections containing specific routers), and it was confirmed that the current topology could be discovered with 100% accuracy, even though only 1.7% of the total topology was evaluated in one day.**

Keywords— service assurance operation, network connection relationship, topology discovery

I. INTRODUCTION

As for service assurance operation of telecommunications carriers, it is imperative to maintain topology information correctly. "Topology information" indicates the connection relationships between pieces of network(NW) equipment. When equipment fail, to decide the urgency of the response to that failure, the maintainer of the equipment needs to know in which area and the number of users affected by the failure of service. At that time, the maintainer uses the topology information to identify the equipment connected with the failed equipment and grasp the effect of the failure in that section on services. Moreover, when the maintainer receives the user's inquiries, the maintainer compares the contents of the inquiries with the topology information in order to identify which equipment is faulty. However, it is important to manage the correct topology information because the maintainer's tasks become difficult if the topology information is incorrect.

In the meantime, the topology information of telecommunications carriers is difficult to keep all the topology information up to date properly because the topology information of telecommunications carriers is supplemented and changed frequently. Since hundreds of thousands of equipment managed by a communication carrier are subjected to construction work and troubleshooting, topology information is supplemented and updated several hundred times (or more) every day. On top of that, it is necessary to handle the physical work of construction and troubleshooting manually, so it is difficult to automate the results of that manual work completely so that they are reflected in the management database of topology information. As a result, when manually recording a large amount of supplemented or updated topology information, the person doing that manual work inevitably makes mistakes; consequently, it is very difficult to keep the topology information correct at all times.

In this study, a new topology discovery technology is proposed. Regardless on the layer in question, the proposed technology utilizes the characteristic that when equipment discovers an abnormality in its connection with an associated equipment, the connected equipment issue an alarm at almost the same time. The main contributions of this paper are listed below.

- Proposal of a novel topology discovery method using equipment-alarm information
- Evaluation result showing that the proposed method can be applied to part of a commercial configuration (a particular router-connection section) and discover 1.7% of the entire topology with 100% accuracy in one day

In the following sections, related research and its problems as well as the novelty of proposed contents are introduced in Section 2. The proposed method is described in Section 3. Results of an evaluation in Section 4.A conclusion of the paper is given in Section 5.

II. RELATED RESEARCH

Topology discovery technology is being studied and discussed by many researchers. In this section, those related researches are introduced, problems arising when such technology is applied to a telecommunications-carrier NW are described, and the novelty of the proposed method is explained. Two major types of topology discovery methods are currently available. One type, namely, topology discovery technology that targets the "IP layer" containing layer-3 routers (hereafter, simply "routers") and layer-2 switches (hereafter, "switches") , is described in Section A. The other type, namely, topology discovery technology that targets the

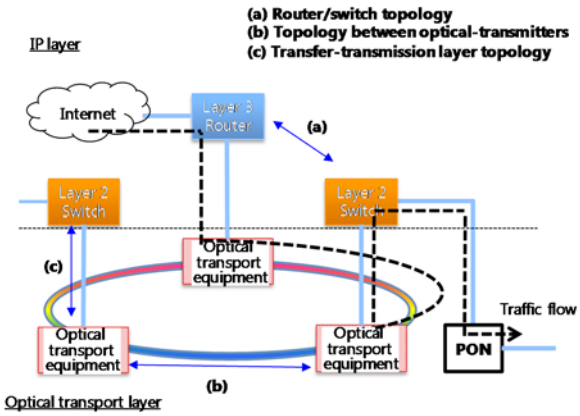


Fig. 1. Topology section of NW of a telecommunications carrier

"optical transport layer" containing layer-1 and layer-0 optical transport equipment (hereafter, "Optical transport equipment"), is described in Section B. Problems involved in the related research and the novelty of the proposed method are described in Section C.

A. *Topology discovery technology for the IP layer*

Many topology discovery technologies—centering on methods that utilize various protocols—handling connections between routers and connections between routers and switches have been proposed. A method for discovering the topology between switches through which an SDN controller transfers data was proposed by Flathagen and Bentstue [1]. It uses OpenFlow Discovery Protocol (OFDP) customized the Link Layer Discovery Protocol (LLDP) for a software-defined NW (SDN). An algorithm for discovering topologies between routers and between routers and switches in OSPF (open shortest-path first) backbone networks by using ospfNbrIpAddr MIB (Management Information Base) was proposed by Son, et al. [2].

B. *Topology discovery technology for the optical transport layer*

Although few topology discovery technologies for the Optical transport layer have been proposed, several technologies for discovering the topology in optical transport equipment sections have been proposed. Targeting optical transport equipment, an algorithm that defines each port signature and compares the signatures sent and received by two ports to uniquely pair topologies was proposed by Jaumard, et al. [3].

C. *Problems concerning related research and novelty of the proposed method*

Conventional related research is discussed with the aim of discovering the topology of each layer, so the applicability of the so-far proposed algorithms to different layers is limited. Therefore, it is difficult to apply those algorithms to the NW of a telecommunication carrier that is configured by combining equipment on various layers. Concretely, the NW of a telecommunications carrier must provide a large-capacity, high-speed communication service to users thousands of kilometers away. For that reason, as for configuration of a NW of a telecommunications carrier, the routers and switches that make up the network are installed in buildings located every few kilometers, and data traffic flowing between the buildings is multiplexed and transmitted by optical fiber connecting optical transport equipment. At that time, the to-be-discovered topology in the network of the communication carrier mainly covers the following four sections (Fig. 1).

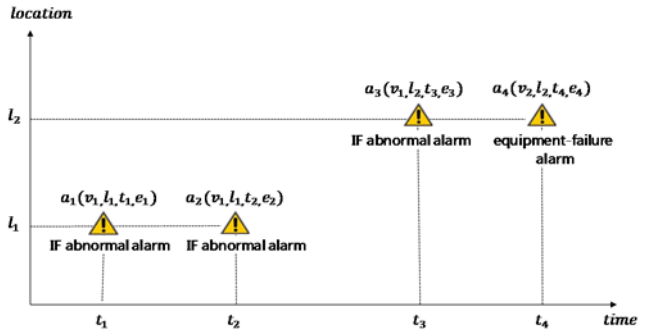
- Section (a) Topology between a router and a switch: a logical connection (actually via optical transport equipment).
- Section (b) Topology between optical transport equipment: a connection between optical transport equipment located in buildings several kilometers apart.
- Section (c) Topology between IP and optical transport layers: a connection across those layers.

Related researches [1], [2] mainly cover technology for discovering topology (a) [between routers and switches], related research [3] covers technology for discovering topology (b) [between optical transport equipment]. However, a technology for discovering the topology between the IP and optical transport layers [topology (c)] has not yet been proposed. As stated in the above-described related research, to apply technologies that assume the use of protocols within each layer, it is necessary to develop the routers, switches, and optical transport equipment on each layer on the basis of a common protocol. However, such a common protocol is currently not available. On top of that, when technologies for discovering topology specialized for each layer are used in combination, it is a concern that it is necessary to study the optimum combination of technologies at all such times in accordance with the progress of each technology and the change of protocol specifications.

Accordingly, the purpose of this research is to establish a topology discovery technology that can be used across layers regardless of the layers in multi-layer carrier NWs. The authors have been studying topology discovery technology using traffic information [4]. So far, we have proposed a topology-estimation method that estimates whether two NW equipment are connected by comparing the traffic volume at each IF of each NW equipment. However, as for certain equipment, amount of traffic cannot be acquired due to the specifications of the equipment. It is therefore a problem that in the case that the NW of the telecommunications carrier is composed of equipment from various vendors, it is not possible to discover all the topologies from traffic information only. Accordingly, in this study, a new method for discovering topology using alarm information is proposed.

III. Proposed Topology Discovery Method Using Alarm Information

The proposed technology discovers the topology by utilizing the following characteristic: when equipment detect an abnormality related to its connection with an opposing equipment (due to construction work or failure), those related equipment issue alarms at almost the same time. Those alarms include information on the IF that detected the abnormality. When two alarms are issued at the same time by the same event, it is considered that the IFs indicated by those alarms have a connection relation. Since this characteristic is common to routers, switches, and optical transport equipment, taking advantage of it enables layer-independent topology discovery. The alarms to be handled are modelled as described in Section A, and the proposed topology discovery method using alarms is described in Section B.



Alarm information(example)

	v : type of alarm	l : physical position of equipment	t : time the alarm occurred	e : equipment type and name of IF
a_1	IF abnormal alarm	Building A	1:13:20	Equipment A Port1
a_2	equipment-failure alarm	Building A	1:13:22	Equipment B Port12
a_3	IF abnormal alarm	Building B	1:14:10	Equipment C Port4
a_4	IF abnormal alarm	Building B	1:14:14	Equipment D Port4
...	...	...	...	...

Fig. 2. Illustration of alarm model

A. *Modelling alarm information*

The purpose of modeling is to minimize the influence on the algorithm of introducing or adding a new equipment by allowing the alarm information to be handled abstractly by the algorithm. Normally, the triggers for alarms can be classified as two cases: (i) an abnormality occurs in the equipment itself due to a failure or construction work; and (ii) an abnormality occurs in the cable connecting the d equipment. An example of case (i) is when a equipment port fails. At that time, as for the equipment with the failed port, an alarm indicating the equipment failure (i.e., the port is abnormal) is issued. At that time, equipment connected to each other issue an alarm indicating an IF-related abnormality. As an example of case (ii), a cable connecting equipment was swapped during construction work. At that time, the equipment at both ends of the cable both issue an alarm indicating an IF-related abnormality. In both cases, the type of alarm is defined as *v*, which is either indicating equipment failure (e.g., an "eqpt-failure" alarm) or an IF-related abnormality (e.g., a "link-down" alarm). The physical position of the equipment that issued the alarm (building, area, etc.) is defined as *l*. The time the alarm occurred is defined as *t*. Information about the equipment that issued the alarm and the IF (i.e., equipment type and name of IF that detected the abnormality) is defined as *e*. It is supposed that an alarm is composed of these four elements: *v*, *l*, *t*, and *e* (Fig. 2).

B. *Topology discovery method using alarms*

Based on the alarm model described in the previous section, a method of narrowing down the alarms generated by the same event (fault or construction work) from the tens of thousands of alarms generated per day and discovering the topology relationship from those narrowed-down alarms is proposed hereafter. Figure.3 shows overview of the proposed method. Among multiple alarms, the ones with the same *l* and *t* or those close to each other are regarded as the alarms generated in the same event and related. Then, it is determined that there is a connection between *e* included in each alarm *a*. However, even if it is the same event, it is a few that an alarm will generate at exactly the same time, so a time width for association is necessary. This is set as t_{opt} in advance. The proposed method involves the following five steps.

(1). Alarm information is acquired and sorted according to time of occurrence. Then, the sorted alarms are converted to an alarm model, and alarms other than equipment failures and IF-related abnormalities (e.g., telnet connection notifications sent to the equipment) are deleted. Finally, an alarm list is generated from the remaining alarms.

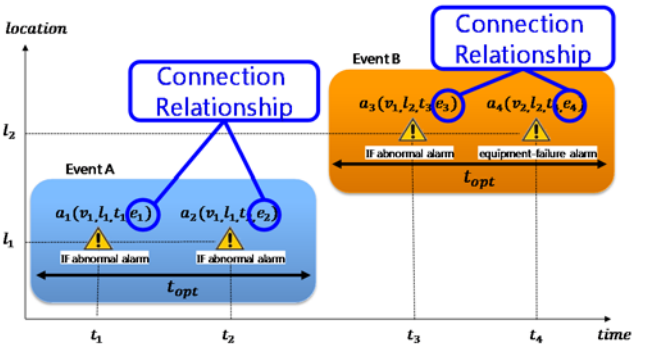


Fig. 3. Image of Topology Dicovery

(2). Alarms are read in order from the top of the alarm list, and a separate alarm (a_n) generated around occurrence time t_m of the alarm in question (a_m) is extracted from the alarm list. Optimal time width before and after t that associates alarms a_m and a_n at this time is defined as t_{opt}. A list of topology candidates is generated by determining that the equipment that issued the two alarms (a_m and a_n) and information (e_m and e_n) are connected with the IF. Note that depending on the length of t_{opt} to be set, the extracted a_n is not always singular. In that case, multiple es are stored in the topology-candidate list for one e_m.

(3). From the topology-candidate list generated in step (2), all alarms except those occurring near physical position *l* of the equipment that issued the alarm are deleted.
Then, *l* to be narrowed down is set according to the deployment status of the equipment. For example, when the topology between the optical transport layer and the IP layer is to be discover [(d) in Fig. 1], two pieces of equipment are basically housed in the same building, so all elements other than *l* of that building are deleted. On the contrary, when the topology between routers and switches or between optical transport equipment ((a) and (c) in Fig. 1) is to be discovered, the connection basically spans buildings, all elements except for *l* of the same area (administrative division of Japan) are deleted.

(4). In the topology-candidate list narrowed down in step (3), candidates showing the same topology are deleted.
Finally, if the candidate list is unique, it is taken that the equipment and IF are connected and indicated by information *e* about the equipment issuing each alarm is discovered. If it cannot be narrowed down uniquely, it is output as is as the topology candidate result list.

(5). Steps (2) to (4) are repeated for all alarms on the alarm list.

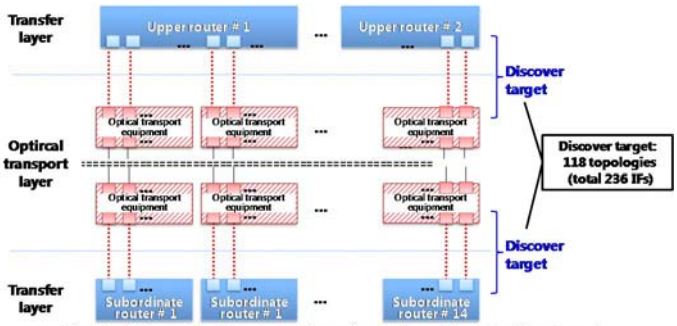


Fig. 5. Schematic diagram of configuration of evaluation target

IV. Evaluation of Proposed Method

As for the proposed method, if t_{opt} used is too long, an IF indicated by an unrelated alarm will also be discovered as being connected. On the contrary, if t_{opt} is too short, the time lag between alarms cannot be absorbed, and IFs that are connected cannot be discovered. Moreover, the time stamp given to the alarm differs in accordance with the specifications of the operation system (OpS), such as the time that the equipment issues the alarm, and the time that the OpS receives the alarm. On top of that, the timing of the time stamp given when the equipment issues an alarm varies in accordance with the equipment specifications. In other words, it is difficult to determine optimal t_{opt} because each alarm has a unified policy and its time of occurrence is not set.

The following two points are evaluated.

- Determining t_{opt}
- Confirmation of the effect of the proposed method (number of discovered topologies) and its discoverion accuracy (correct-answer rate) by using alarms caused by failures

The evaluation conditions are described in Section A, and the evaluation results when t_{opt} is changed are presented in Section B.

A. Evaluation conditions

Whether the proposed method can discover the topology between the IP and optical transport layers (which could not be discovered in the above-described related research) was evaluated first. As for the primary evaluation, to confirm the usefulness of the proposed method, the evaluation target was limited to alarms for certain commercial configurations (a specified router-connection section). In that section, which is connected via optical transport equipment (Fig. 4), there are 118 connections (236 IFs) between routers and the optical transport equipment. In this evaluation, one day's worth of nationwide alarms was used, and 4,359 and 11,908 alarms were acquired from the IP-layer OpS and the optical transport-layer OpS, respectively. The parameters used for various evaluations are listed in Table 1. By evaluating multiple t_{opt} patterns, it is possible to determine t_{opt} . IF-related abnormality alarms that occurred in the same building in t_{opt} were extracted from the IF-related abnormality alarms occurring over a certain time, and whether the IF indicated by each alarm could be discovered as a topology was evaluated.

B. Results of evaluation and considerations

The results of the evaluation are listed in Table 2. Number of discoverions [(1)] is the number of cases in which each IF for e_m indicated by alarm a_m of the router and e_n indicated by alarm a_n of the optical transport equipment is discovered as a unique topology. In this evaluation, when t_{opt} was set from ten seconds to one hour, two out of 118 connections were discovered. On the contrary, when t_{opt} was set to three hours, one of the two connections discovered when t_{opt} was set from ten seconds to one hour could not be uniquely determined; that is, different IFs indicated by other alarms were also discovered as topology candidates. Moreover, when t_{opt} was set to 1 s, the alarm of the candidate opposing IF could not be acquired, so the IF could not be specified.

TABLE I. Set Values of Evaluation Parameters

Parameter	Value
t_{opt}	±3 h, ±1 h, ±1 m, ±10 s, ±1 s,
l	Same building
v	IF-related abnormality alarm
e	IF of router or optical transport equipment

TABLE II. Evaluation Results

t_{opt}	±3 h	±1 h	±1 m	±10 s	±1 s
(1) Number of discoverions	1	2	2	2	0
(2)Number of correct answers (correctness rate) in (1)	1 (100 %)	2 (100 %)	2 (100 %)	2 (100 %)	0 (-)

The number of correct answers (correctness rate) in (1) [(2) in Table 2] is the result of confirming the number of correct answers and the correct answer rate for the topology discovered in the number of discoverions [(1)]. In this evaluation, comparing the discovered topology with the actual topology confirmed that all discoverions were correct and the accuracy rate was 100%. Note that if t_{opt} is set longer than necessary, the calculation load will increase, so ± 10 s is considered desirable.

V. Concluding Remarks

In this paper, a method for discovering the topology of a NW configuration from time information of alarms generated between multiple equipment and information about the alarm location was proposed and evaluated. From now onwards, it is necessary to verify with multi-vendor equipment, moreover determine whether discovery is possible for all topologies in the sections (a)-(c) in Fig. 3 other than those verified this time.

References

[1] J.Flathagen, and O.I.Bentstuen, "Proxy-based Optimization of Topology Discovery in Software Defined Networks," International Conference on Military Communications and Information Systems, Montenegro, May 2019, pp.1-5

[2] C.Son et al., "Efficient physical topology discovery for large OSPF networks," IEEE Network Operations and Management Symposium, Brazil, August 2008, pp. 325-330.

[3] B.Jaumard, A.Muhammad, R.Fahim, "Topology discovery of Synchronous Optical NETworks," International Conference on Computing, Networking and Communications, USA, January 2017, pp. 194-199.

[4] Mizuto Nakamura, et al., " Study on multi-layer configuration management technology using traffic information," International Conference on IP + Optical Network, Japan May 2019