Topology Discovery Method using Network 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

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*— For the service assurance operation of telecommunications carriers, accurate information about a network topology that indicates the connection relationships between pieces of network equipment is necessary. However, the network of a telecommunications carrier has several hundreds of thousands of pieces of equipment. Furthermore, its topology is frequently supplemented and modified due to daily construction work and troubleshooting. As a result, this causes incorrect topology information to be 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 on a commercial network. The experimental results show that the proposed method discovers topology with higher accuracy than classical topology discovery approaches.**

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

I. Introduction

For service assurance operation of telecommunications carriers, topology information must be correctly maintained because it is used to isolate the location of the failure accurately. “Topology information” indicates the connection relationships between pieces of network (NW) equipment. When equipment fails, the maintainer uses the topology information to identify the equipment connected with the failed equipment. At that time, it is important to manage the correct topology information because the maintainer’s tasks become difficult if the topology information is in correct.

However, the topology information is difficult to keep up to date properly because it is supplemented and changed frequently. The topology information is supplemented or changed by construction work (such as installing cables to new equipment when equipment is added) and troubleshooting(such as cable re-attachment work accompanying the exchange in failure parts and spare parts).Since hundreds of thousands of pieces of equipment managed by a communication carrier are subjected to such work and troubleshooting, topology information is supplemented and updated several hundred times (or more) every day. 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 paper, we propose a new topology discovery technology that utilizes the characteristic that when equipment discovers an abnormality or recovery in its connection with associated equipment, the connected equipment issues 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 results showing that the proposed method can be applied to a commercial NW and discover topology with higher accuracy than classical topology discovery approaches

978-3-903176-31-7 © 2020 IFIP

In the following sections, the 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 are presented in Section 4. A conclusion of the paper is given in Section 5.

II. Related research

In this section, related technologies are introduced, problems arising when they are applied to a telecommunications-carrier NW are described, and the novelty of the proposed method is explained.

A. *Topology discovery technology for the IP layer*

Many topology discovery technologies have been proposed, centering on methods that utilize various protocols: handling connections between routers and connections between routers and switches. Flathagen and Bentstuen proposed a method for discovering the topology between switches through which an software defined network (SDN) controller transfers data [1]. It uses the OpenFlow Discovery Protocol (OFDP) customized the Link Layer Discovery Protocol (LLDP) for an SDN. Son et al. proposed an algorithm for discovering topologies between routers and between routers and switches in open shortest-path first (OSPF) backbone networks by using ospfNbrIpAddr the Management Information Base (MIB) [2]. Qiuxiang proposed a two-step algorithm that accesses equipment by using the simple network management protocol (SNMP), discovers the interface (IF) and subnetwork of the router through ipRouting Table Traversal, and discovers hosts in the subnet via a ping (packet internet groper) of the internet control message protocol (ICMP) [3]. Features of a topology discovery algorithm for the IP layer—using each of the above-mentioned protocols—were summarized by Zhao et al. [4] in an easy-to-understand manner. Xiao et al. proposed a method of implementing a topology discovery algorithm for the Ethernet data-link layer based on SNMP and a media access control (MAC) address table was proposed [5]. Nowicki and Malinowski proposed an algorithm that discovers the topology by arranging agents on a switch and then observing the communication between the agents [6]. A topology discovery technology based on the spanning-tree protocol was proposed by Peng et al. [7].

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

Several technologies for discovering the topology in optical transport equipment and PON sections have been proposed. Targeting optical transport equipment, Jaumard et al. proposed an algorithm that defines each port signature and compares the signatures sent and received by two ports to uniquely pair topologies [8]. Zhang et al. proposed discovering a topology by comparing the uniquely defined identifiers assigned to ports in sections covering ONUs to OLTs [9]. A feature of this method is that information can be collected from all OLTs at the network-management system by using the SNMP get-response protocol.

C. *Topology discovery method using traffic information 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. As stated in the above-described related research, to apply technologies that assume the use of protocols within each layer, the routers, switches, and optical transport equipment need to be developed on each layer on the basis of a common protocol. However, no such common protocol currently exists. On top of that, when technologies for discovering topology specialized for each layer are used in combination, a concern is that the optimum combination of technologies at all such times needs to be studied in accordance with the progress of each technology and the change of protocol specifications.

Accordingly, the purpose of our research is to be able to discover the topology of IP and optical transport layers which has not been realized so far, moreover to establish a topology discovery technology that can be used the all layers in multi-layer carrier NWs. So far, we have proposed a topology-discovery method by comparing the traffic volume at each IF of each piece of NW equipment [10]. We considered that all topologies can be discovered without limiting the layers as in the previous studies [1] - [9], because the traffic information can be obtained using standard MIB.

However, topology-discovery method using traffic information has several issues. The topology discovery method using traffic information detects the amount of traffic change and the connection relationship. Firts, the method has a problem that the connection relationship cannot be discovered correctly when there are multiple IFs that do not have characteristic traffic. Moreover, the biggest issue is the amount of traffic could not be acquired for certain equipment due to the specifications of the equipment. In case of our NW, traffic information of about 25% of the optical transport equipment could not be acquired.

Therefore, from a different viewpoint, we propose a new method for discovering topology using equipment alarm information. Since the alarm information is basically information that can be obtained from any device, it is thought that the conventional problems can be solved.

III. Proposed topology discovery method using equipment alarm information

The proposed technology discovers the topology by utilizing the following characteristic: when equipment detects an abnormality or recovery related to its connection with opposing equipment (due to construction work or failure), those related pieces of equipment issue alarms at almost the same time. Those alarms include information on the IF that detected the abnormality or recovery. When two alarms are issued 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.

A. Modelling alarm information

The purpose of modeling is to minimize the effect on the algorithm of introducing or adding a new equipment by allowing the al arm information to be handled abstractly by the algorithm. First, the type of alarm is defined as *v*, which is either indicating equipment failure (e.g., an equipment-failure alarm) or an IF-related abnormality or recovery (e.g., a link-down/up 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 or recovery) is defined as *e*. It is supposed that an alarm is composed of these four elements: *v*, *l*, *t*, and *e*. These alarm models can also be implemented based on the standard MIB. For example, in the case of LinkDown, the IF information is acquired from the ifIndex of OID 1.3.6.1.6.3.1.1.5.3 in SNMP[11]. However, there are some of equipment that do not implement the alarm issuing with the standard MIB, so it is necessary to expand using a private MIB depending on the equipment.

B. Topology discovery method using alarms

On the basis of the alarm model described in the previous section, a method is proposed is described. This proposed method narrow down the alarms generated by the same event (fault or construction work) from the tens of thousands of alarms generated per day and to discover the topology relationship from those narrowed-down alarms. 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 events. Then, it is determined that there is a connection relationship between *e* included in each alarm *a*. However, even if the event is not the same, an alarm will sometimes 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 five steps.

(1).Alarm information is acquired and sorted in accordance with time of occurrence. Then, the sorted alarms are converted into an alarm model, and alarm type *v* other than IF-related abnormalities are deleted. Finally, an alarm list is generated from the remaining alarms.

(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 (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 are deleted except those occurring near the physical position l of the equipment that issued the alarm. Then, l to be narrowed down is set in accordance with the deployment status of the equipment. For example, when the topology between the optical transport layer and the IP layer is to be discovered, two pieces of equipment are basically housed in the same building, so all elements other than l of that building are deleted. In contrast, when the topology between routers and switches or between optical transport equipment is to be discovered, the connection basically spans buildings, all elements are deleted except for l of the same area (administrative divisions of Japan).

(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.

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

IV. Evaluation of proposed method

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. In contrast, 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 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, optimal t_{opt} is difficult to determine because each timestamp of alarm does not have a unified policy.

Two points are evaluated.

- Determining t_{opt}
- Confirmation of the discovery accuracy

A. Evaluation conditions

We evaluated whether the proposed method can discover connection relationships in the IP-optical transport layer that could not be discovered in related research. We evaluate

TABLE Ⅰ. Set values of evaluation parameters

Parameter	**Value**
t_{opt}	between ±0s and ±70s (in 5 second intervals)
l	Same building
v	IF-related abnormality alarm
e	IF of router or optical transport equipment

TABLE Ⅱ. Results of evaluation

t_{opt}	±0	±5	±10	±15	±20	±25	±30	±35	±40	±45	±50	±55	±60	±65	±70
all number of discovery connection relationships	0	6	9	10	10	10	10	11	11	12	12	12	12	13	12
the number of correctly discovered connection relationships	0	5	8	9	9	9	9	10	10	10	10	10	10	10	10
the number of incorrectly discovered connection relationships	0	1	1	1	1	1	1	1	1	2	2	2	2	3	2
precision	0%	83%	89%	90%	90%	90%	90%	91%	91%	83%	83%	83%	83%	77%	83%
recall	0%	25%	40%	45%	45%	45%	45%	50%	50%	50%	50%	50%	50%	50%	50%

TABLE Ⅲ. Results of precision and recall comparison

	precision	recall
Topology discovery method using traffic information	52%	52%
Proposal method（t_{opt} =±40s）	91%	50%

whether it is possible to discover the connection relationship for 20 specific failures that occurred in the IP-optical transport layer in 29,391 alarms per day (14,933 optical transport layer alarms and 14,458 IP layer alarms). The precision is the proportion of the discovered connection relationships that could be discovered correctly. The recall is the ratio of the number of correctly discovered connection relationships among the maximum 20 connection relationships that can be discovered by 20 failures.

Table 1 shows each setting parameter. As described above, t_{opt} needs to be set to multiple values because the optimum value needs to be known and the precision and recall at each t_{opt} are evaluated. Specifically, a_n generated in 5-second intervals between ±0s and ±70s with respect to the alarm a_m of the comparison source is narrowed down as a connected alarm.

B. Results of evaluation and considerations

Table 2 shows the evaluation results of discovering the connection relationship when t_{opt} is changed every ±5 seconds. When t_{opt} was ±35 s to ±40 s, there were 10 correct detections and 1 false detection, which was the smallest result. When t_{opt} exceeds ±40 s, the total number of discovery connection relationships increased, and when t_{opt} was ±65 s, there were 13 correct detections, which was the highest result, but the number of false detections increased. This is because the method determines irrelevant alarms have connection relationships due to the long interval for collecting alarms.

On the other hand, no detection was possible when t_{opt} was ±0s, and the next lowest detection number was 6 when ±5s. The shorter the interval of t_{opt}, the smaller the number of detections tends to be. This is because the alarm time lag cannot be absorbed. Next, the precision was highest when t_{opt} was ±35s to ±40s, which was 91%. One alarm that was erroneously detected is the result of detecting an alarm generated in the same building at the same time due to another failure as having a connection relationship. Furthermore, regarding the recall rate, for the 20 cases to be detected, the highest t_{opt} was ±35 s to ±40 s, and the result remained at 50%. The 10 cases that could not be detected this time are due to multiple alarms being generated at the same time due to a failure, and another alarm remaining as a candidate, which could not uniquely narrow down the connection relationship.

C. Comparison with the topology detection technology using traffic information

Table 3 shows the result of comparison between the proposed method and the existing topology discovery method that uses traffic information [10] from the viewpoint of precision and recall. In the evaluation of the existing technology, the amount of traffic acquired from each device in the IP layer and the optical transport layer where the traffic can be acquired was verified in the same commercial NW. The traffic data is 15-minute intervals for 12 hours.

In this verification, the precision was 52% when the existing method was applied but 91% for the proposed method. This comparison result shows that the proposed method has much higher accuracy than the existing method. The existing method detects the amount of traffic change and detects the connection relationship. Therefore, when there are multiple IFs that do not have traffic characteristics or fluctuate significantly, the wrong IFs are detected to have a connection relationship. On the other hand, it was found that the proposed method can detect the connection relation correctly without depending on how the alarm of the device used is output.

On the other hand, the recall was 52% when the existing technology was applied, whereas it was 50% when using the alarm in the proposed method. Therefore, the proposed method needs further improvement.

V. CONCLUDING REMARKS

In this paper, a method was proposed and evaluated for discovering the topology of a NW configuration from time information of alarms generated between multiple pieces of equipment and information about the alarm location. Evaluations results showed that the proposed method was significantly more accurate than the existing technology. From now onwards, the proposed method will be improved and its application area expanded in order to increase the number of discovered topologies and improve evaluation accuracy.

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] Y. Qiuxiang, "Algorithm research of topology discovery on SNMP," International Conference on Computer Application and System Modeling, China, November 2010, pp. V12-496-V12-497.

[4] Y. Zhao, J. Yan, and H. Zou, "Study on network topology discovery in IP networks," IEEE International Conference on Broadband Network and Multimedia Technology, China, November 2010, pp. 186-190.

[5] W. Xiao, R. Wang, and X. Huang, "Design and implementation of Ethernet topology discovery algorithm," IEEE International Conference on Cloud Computing and Intelligence Systems, China, November 2013, pp. 767-770.

[6] K. Nowicki and A. Malinowski, "Topology discovery of hierarchical Ethernet LANs without SNMP support," Annual Conference of the IEEE Industrial Electronics Society, Japan, November 2015, pp. 005439-005443.

[7] H. Peng et al., "Physical topology discovery based on spanning tree protocol," International Conference on Computer Application and System Modeling, China November 2010, pp. V14-308-V14-311.

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

[9] Y. Qiuxiang, "Design and Implementation of Topology Automatic Discovery Algorithm in PON NMS," International Conference on Instrumentation, Measurement, Computer, Communication and Control, China, December 2012, pp. 1490-1493.

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

[11] RFC 1098, A Simple Network Management Protocol (SNMP)