QoS Analysis on Cable Video Delivery Networks

Hiroaki Shikano[1], Takeshi Shibata[1], Qifeng Shen[2], Miyuki Hanaoka[1], Mariko Miyaki[1], Masahide Ban[1], Prasad Rallapalli[2] and Yukinori Sakashita[1]

[1] *R&D Group, Hitachi, Ltd., Yokohama, Kanagawa, Japan*

[2] *R&D Division, Hitachi America, Ltd., Santa Clara, CA, U.S.A.*

Keywords: Quality of Service Analysis, Cable Video Network, Multicast.

Abstract: Telecommunication service providers are now using analytics to differentiate their network services with better Quality of Service (QoS) and Quality of Experience (QoE) as well as to increase operational efficiency. Cable service providers have complex video delivery IP networks, and efficient management of such networks as well as reduction of service impairment time are imperative. We have developed a new cable service QoS analysis solution that provides an end-to-end view of the control and data-plane flows associated with delivery of a video channel and shows identified failure points. Initial evaluation revealed that the solution can reduce the service down time to 62.3% of what it would be without the solution.

1 INTRODUCTION

Various web services - such as video streaming services, voice services, and IoT (Internet of Things) services - are achieved on IP networks. Global IP traffic has increased more than five-fold in the past 5 years and is forecasted to increase nearly three-fold over the next 5 years (Cisco, 2014). Traffic management is essential for telecommunication service providers because heavy traffic loads affect Quality of Service (QoS) and Quality of Experience (QoE). Users are now more aware of the quality of services they receive, and bad service quality can result in churn.

Network management, however, is becoming more complex and difficult as network infrastructure evolves (Kim and Feamster, 2013). As a result, service providers are demanding service assurance management in order to prevent churn as well as to improve operational efficiency by reducing operating cost. To cope with these demands, collection and analysis of big data generated from network, network-related systems and equipment are necessary for network and service operations management (Liu, 2014; Garg and Bindal, 2015). Network analytics therefore plays an important role in helping service providers differentiate their network services, address both revenue and monetization needs, and increase operational efficiency.

This paper focuses on cable service providers (CSPs) using IP networks to transmit hundreds of TV channels to tens of millions of subscribers in nationwide markets. These providers are also facing difficulty in managing complex networks (Vasudevan and Ogozaly, 2009; Kalyur, 2009). This difficulty originates in using different video delivery protocols (i.e., multicasting), different TV channel distribution and advertisement insertion in different markets. The contribution of this paper is to provide a solution improving cable service quality as well as shortening service down time (i.e., time to identify problems and restore services) by performing QoS analysis of cable service networks.

2 CABLE SERVICES AND OPERATIONS

2.1 Cable Services

Cable service providers (CSPs) offer a variety of video services in multiple markets. There are three types of video services:

1. TV Broadcast service (also known as VOBB; Video over Broadband) is the delivery of traditional broadcast television channels ranging from those distributed by national networks to those distributed by local affiliates of these national networks, as well as locally produced channels such as those showing local city government events or

Shikano, H., Shibata, T., Shen, Q., Hanaoka, M., Miyaki, M., Ban, M., Rallapalli, P. and Sakashita, Y.
QoS Analysis on Cable Video Delivery Networks.
DOI: 10.5220/0006436600850092
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 1: DCNET*, pages 85-92
ISBN: 978-989-758-256-1

sports events. These are encoded with MPEG and delivered using IP multicast routing protocols on a routing network to maximize throughput, and they are sent all the way over HFC (Hybrid Fiber-Coaxial) systems to all the subscribers (end users) in all markets regardless of whether or not they are watching.

2. Switched Digital Video (SDV) service is not broadcast but selectively transmitted by a user's subscription. It is also delivered using IP multicast routing protocols.
3. Video on Demand (VoD) service is subscriber-selected video content delivered using IP unicast routing protocols.

This paper focuses on TV broadcast service because it is a fundamental service for cable service providers.

2.2 Cable Video Delivery Network

Figure 1 is a linear schematic view of the flow of video packets delivered from satellite or other links at a super head end (SHE) all the way to the edge of the IP network (EQAM; Edge Quadrature Amplitude Modulation) via backbone routers (BBR), core routers (CRR), distribution routers (DTR), and access routers (ACR). Our focus is on IP network from head ends to EQAM.

The detailed topology of the routing network in one regional and local network in a market is shown in Figure 2. The super head end is connected to the backbone network via BBR. A video stream comes from a SHE via BBR, CRR, DTR, and ACR to the EQAM, which is the edge of the routing network and is where packets are converted to the broadcasting stream delivered to subscribers. If local advertisement needs to be inserted, a video stream comes to an ad-insertion appliance, and the stream with local advertisement inserted comes to the EQAM. For redundancy it is also sent to the neighboring local head ends via CRR.

Video streams are delivered by multicast from an SHE to multiple local head ends. Multicast provides optimal routing for servicing millions of end users who may want to concurrently watch the same video broadcast channel. Typically a multicast group (e.g., TV channel) is uniquely identified by the source IP and group IP as (S, G). Cable service providers usually use PIM-SSM (Protocol Independent Multicast - Source Specific Multicast) and IGMPv3 (Internet Group Management Protocol version 3) protocols (B. Fenner and Kouvelas, 2006; Holbrook and Cain, 2006; Cain and Deering, 2002). PIM-SSM builds multicast trees that are rooted in just one source, offering a more secure and scalable model for a limited amount of applications, mostly broadcasting of content. Therefore, it suits cable video delivery because the IP source of video streams is known. It enables on-demand "join" to the multicast video service (S, G). At periodic intervals a heartbeat mechanism ensures that the feed continues to flow. This signaling (or control-plane traffic) is independent of the actual video streams also known as data-plane traffic.

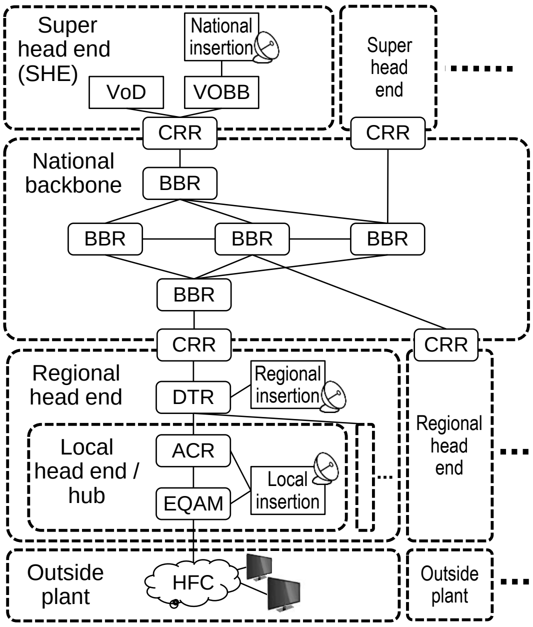


Figure 1: Overview of video service delivery network.

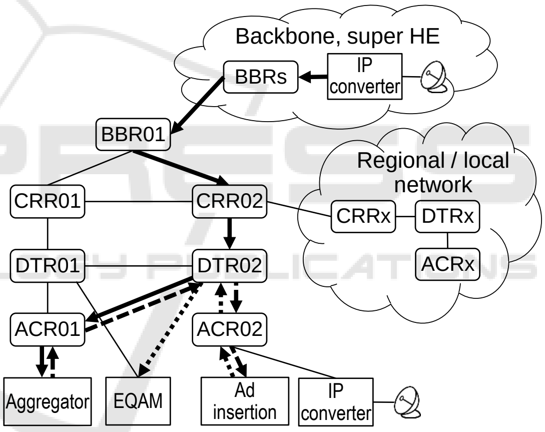


Figure 2: Example of multicast delivery of one channel.

Figure 2 also shows an example of multicast delivery of one channel (national broadcasting). In this example, the video stream is delivered with local advertisement insertion and aggregation, which makes the management complex. For example, a multicast video stream from the SHE goes into the aggregator via BBR01, CRR02, DTR02, and ACR01, and it terminates on the aggregator. Then another multicast stream is generated and goes into the ad inserter via ACR01, DTR02, and ACR02. Ads are inserted into the incoming second multicast stream, and thereafter a third multicast stream is generated and goes into the EQAM via ACR02 and DTR02. The third stream terminates on the EQAM, which ultimately reaches the subscriber.

2.3 Video Service Operations and General Issues

The current state of video service operations is not healthy, with a large number of video service impairments taking a long time for troubleshooting. According to our survey on a cable service provider, about 60% of the incidents that occurred were due to video processing and transport. The average duration of an incident was 231 minutes. The video service delivery problems result in service impairments such as blackout caused by video stream outage, video quality degradation (e.g., block noises on the screen), and frame drops caused by packet loss or packet delivery delay. Such problems usually originate in cable cuts (intentional or accidental), hardware/software failure or misconfiguration of routers, link equipment, or service appliances such as ad-inserters, aggregators, etc., failed failover of routers, and router or link capacity overload resulting from failover.

The followings are the dominant factors that lead to a long mean time for troubleshooting (i.e. detecting and repairing) video service delivery problems in the routing network.

- Limited end-to-end visibility for simple flows

  A CSP's network operations center (NOC) does not have accurate real-time, end-to-end visibility of the network flows involved in video service delivery. This results in a lot of guesswork based on sketchy information despite there being many kinds of probes and monitoring systems in place.
- Silos ("tribal knowledge") - no complete picture of current/future state

  Due to many factors such as complexity of the multiple types of technology stacks (networking gear, protocols), incomplete monitoring systems, insufficient documentation and ongoing standardization, loss/movement of technical personnel, etc., there is no complete picture of the current or future state of the system.
- Complex video services and routing flows

  IP multicast video routing generally uses arcane and complex technology with many implementation variations in terms of networking protocols. There are multiple technology stacks, and there are no standard books/recipes that can help operators troubleshoot video service delivery problems more efficiently. Bundling/aggregating/multiplexing channels to reduce bandwidth further complicates the picture because internal systems do not alert the NOC based on their internal monitoring, and usually the first sign of trouble is customer care getting calls from customers or getting news from social media. Furthermore, local advertisement insertion results in even more complexity.

2.4 Problem Statement and Goals

The goal is to reduce service impairment time; which is equal to the customer-experienced service interruption time. This will result in the improvement of customer satisfaction as well as network operation efficiency, which means the operating team will have more time for planning future network improvements or considering new services less time will be spent troubleshooting. To shorten service impairment time, we need to reduce both the time need to identify issues (MTTD; mean time to detect) and the time to restore services (MTTR; mean time to restore/resolve/repair) as described in Figure 3. We set the goal for reduction of the current service impairment time to 50% that with our proposed solution as the cable service provider requested.

3 CABLE NETWORK QoS ANALYSIS SOLUTION

3.1 High-level Description

As stated in Section 2.4, the goal is to reduce MTTD/MTTR of issues on a cable service network with limited end-to-end visibility complex network technologies, complex video services, and a complex routing network. We developed a new analytics solution that supports two main use cases listed as follows.

(1) Topology Discovery and Visualization

The solution provides network topology diagram views highlighting multicast trees of a video stream for a specific channel (i.e., a single-program transport stream) or a bundle of channels (i.e., a multiple-program transport stream). To speed issue identification, these views include both the multicast tree visualized on a physical topology diagram in multiple

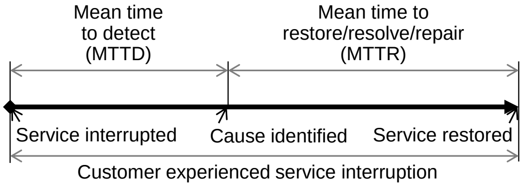


Figure 3: Problem statement.

hierarchical levels (i.e. nationwide, regional and local) and the end-to-end schematic diagram from the super head end (i.e. satellite signal receiver) to the EQAM (subscriber-side terminal of IP network).

For topology discovery and visualization, the sub use cases are:

(1-1) Describing Layer-2 / Layer-3 network topology
(1-2) Describing multicast tree topology by channel or bundle of channels on (1-1)

(2) Failure Detection / Identification based on Topology

Operators currently spend much time identifying issues after the first sign of trouble is reported (by customers calling customer care). The solution provides detection of failure and identification of failure points in the cable service network, and it shows the identified failure points on the topology diagram as described in (1).

The detection and identification is realized by the interplay between control (signaling) and data flows, e.g., by correlating the multicast signaling (PIM-SSM, IGMP) protocol related flows to the actual flow of the video packets. Additionally monitoring the video flow utilization in near-real time is also essential because a sudden drop in utilization usually signifies trouble.

For failure detection and identification, the sub use cases are:

(2-1a) Identifying total failure (e.g., video blackout) after a customer reports a problem
(2-1b) Identifying partial failure (e.g., video quality degradation) after a customer reports a problem
(2-2a) Identifying total failure before a customer reports a problem
(2-2b) Identifying partial failure before a customer reports a problem

3.2 Solution Architecture

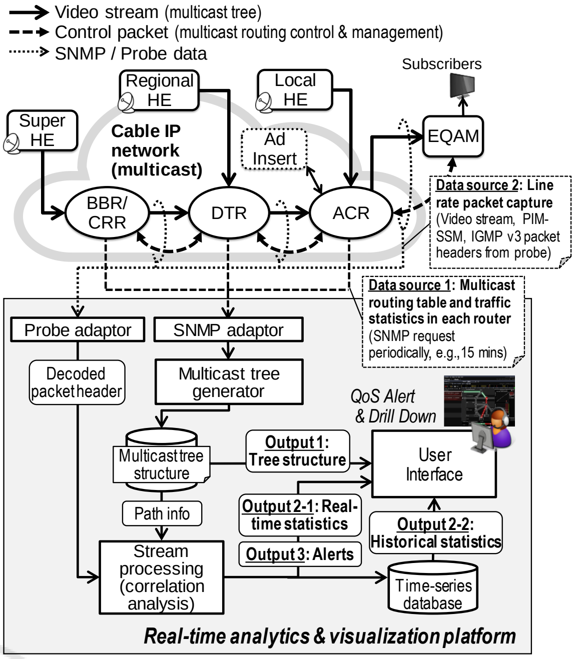

Video stream (multicast tree)
Control packet (multicast routing control & management)
SNMP / Probe data
Subscribers
Regional HE
Local HE
Super HE
Cable IP network (multicast)
Ad Insert
EQAM
BBR/ CRR
DTR
ACR
Data source 2: Line rate packet capture (Video stream, PIM-SSM, IGMP v3 packet headers from probe)
Data source 1: Multicast routing table and traffic statistics in each router (SNMP request periodically, e.g.,15 mins)
Probe adaptor
SNMP adaptor
Decoded packet header
Multicast tree generator
QoS Alert & Drill Down
Multicast tree structure
Output 1: Tree structure
User Interface
Path info
Output 2-1: Real-time statistics
Output 2-2: Historical statistics
Stream processing (correlation analysis)
Output 3: Alerts
Time-series database
Real-time analytics & visualization platform

Figure 4: Architecture of cable service QoS analysis solution.

Figure 4 illustrates the overall architecture of our solution. The solution utilizes a platform supporting real-time analytics and visualization. The system collects router information including configurations such as IP addresses, unicast routing tables (RIB), and multicast routing tables (MRIB) and performance metrics such as utilization via SNMP (Simple Network Management Protocol). It also utilizes packet information obtained from probes attached to links between routers.

Table 1 and Table 2 list the use cases described in Section 3.1 and the data sources utilized by each use case. We use SNMP MIB information for multicast tree discovery and use passive probes to monitor data-plane and control-plane flows. Existing technology for discovering L2/L3 network topology(Breibart, 2000; Puneet Sharma and Malpani, 2003) is utilized for use case (1-1). The following section describes how the use cases listed in Table 1 and Table 2 are implemented.

3.2.1 Multicast Tree View for Use Case (1-2)

For multicast tree discovery, the system will query SNMP MIB based on control-plane monitoring; it can get the multicast routing table from a specific router and for a specific multicast group on-demand when it finds a join or prune packet than results in a multicast routing table change. Given the intricacies of the multicast protocols, we have a subsystem to discover and visualize the multicast trees for a given multicast group and a separate subsystem to analyze the data-plane traffic.

Table 1: Use cases of topology discovery and visualization, and data sources.

Use cases	Input data
(1-1) Underlying L2/L3 network topology	- IP address of each router - Unicast routing table (RIB) in each router
(1-2) Multicast tree topology by channel	- Unicast topology (1-1 above) - Multicast routing table (MRIB) in each router

Table 2: Use cases of failure detection / identification, and data sources.

Use cases	Input data		
	C-plane: Multicast tree (1-2)	D-plane: Statistics	D-plane: Packet
(2-1a) Identify TOTAL failure after customer call	X	X	
(2-1b) Identify PARTIAL failure after customer call	X		X
(2-2a) Detect TOTAL failure before customer call	X	X	
(2-2b) Detect PARTIAL failure before customer call	X		X

3.2.2 Correlating Multicast Tree and Data Plane Flows (C-D Plane Correlation) for Use Cases (2-1a) and (2-2a)

Using multicast tree topology, the system compares utilizations before and after those of particular router, or both edges of particular link, for each multicast group and checks whether the utilization is the same. If data (video stream) is not flowing even though the multicast tree exists, that will be a problem triggering an error and will be shown on a user interface. In this use case, we use two data sources: 1) the multicast tree discovered above and 2) data-plane flow information (i.e., utilization). Data-plane utilization will be obtained from probes rather than routers using SNMP since data from probes can offer finer time granularity (1 sec granularity) whereas with SNMP the time between polls is usually 15 minutes.

3.2.3 Correlating Multicast Tree and Control Plane Flows (C-C Plane Correlation) for Use Cases (2-1b) and (2-2b)

Control packets are sent to generate a multicast tree and are also used to maintain an existing multicast path. By monitoring control packets, we can detect some abnormal states even the end-user is not aware of them and can identify their possible causes. As in the data-plane flow monitoring for multicast trees, we use two data sources: 1) the multicast tree discovered and 2) control-plane packets (PIM and IGMP packets).

Keep-alive Join:
Join packets are usually sent every minute to keep the multicast path. If a router receives no packets for 210 seconds (B. Fenner and Kouvelas, 2006), the corresponding multicast entry will be removed. The monitoring system will generate error alert if there are no join packets in 210 seconds even if a multicast path exists. It also generates warning if there are no join packets in 120 seconds.

Warning for Join if Multicast Tree Does Not Exist:
Join packets should be sent only if a multicast path exists; therefore this will be a warning.

Warning on Prune:
If prune packets are sent, the system first gets SNMP info for that multicast group and regenerate a tree; therefore this will be a warning.

Incomplete Multicast Tree:
During multicast tree generation, we can identify an incomplete multicast tree; paths are generated from source to somewhere, and somewhere else to EQAM (end of IP), although source to EQAM is not connected end-to-end. If join packets are NOT sent for the "not-connected path", the router that should send join packets may have problem. If join packets are sent but a multicast table does not exist (and consequently, a multicast tree is not generated), then the router that receives join packets may have problem.

3.2.4 Correlating Pre and Post Ad Insertion Flows

Once we identify the mapping between pre- and post-ad-insertion flows, correlating end-to-end tree and data-/control-plane flows will be similar to that described above. The only difference is that the size is not an exact match. For the first version of the solution, we detect only outage of a post-multicast stream, which makes a certain amount of difference in utilization between pre- and post-ad-insertion flows. Therefore the system creates an alert if that difference exceeds a threshold value that may be given manually.

3.3 User Interfaces and Interactions

NOC operators monitor cable network status and troubleshoot network-related issues in collaboration with customer care personnel who receive customer calls, service operators who monitor cable service quality, and local network engineers stationed at service sites such as head ends. Our solution's UI has the components described as follows, supporting the two main use cases: (1) topology discovery and visualization, and (2) failure detection/identification based on topology as stated in Section 3.1.

Dashboard

Operators need to know which channels in which areas have alerts immediately. The system offers a channel and market status overview screen describing which areas/channels have alerts as well as a channel status screen describing which channels in a specific market have alerts. Operators can directly move to a live multicast tree view of a market by clicking market/channel. If there are alerts on a specific channel in a specific market, operators can drill down to the multicast tree view corresponding to the alerts on that channel in that market.

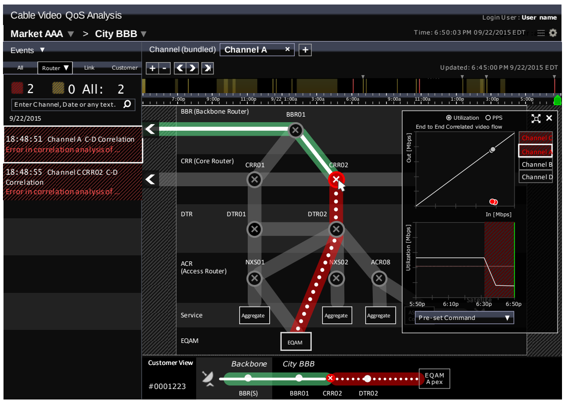
Hierarchical Tree View and Linear Schematic View

Figure 5 shows a UI mockup screen with a hierarchical tree view that enables operators to quickly grasp the current actual configuration of the network, including multicast paths and differences from what ought to be, and to recognize which points of the network (node/link) have issues.

It also shows the screen with a linear schematic view that enables operators to quickly grasp which points of a network delivering a specific channel to a specific customer have issues by providing an end-to-end view of the network topology. This view can be utilized for reducing MTTD when customers report service troubles. Operators first specify customer identification information to identify which EQAM covers that customer and then specify a channel in trouble to identify the source (head-end) of the channel or multicast group.

Alerts Driven Interaction

Alerts are important for operators to start identifying problems. The UI visualizes alerts as a



18:48:51 Channel A C-D Correlation
Error in correlation analysis of ...

18:48:55 Channel C CRR02 C-D Correlation
Error in correlation analysis of ...

Figure 5: UI screen mockup: topology view with correlation and performance graphs overlaid.

list with necessary information such as the time the alert occurs, which channel is related, which router/link has a potential cause, alert severity (error or warning), the reason the alert was created, and a description of potential cause. If an alert has effects on multiple channels, operators can recognize what channels are affected. By selecting one alert row, operators will have actual multicast topology on the above map and routers/links possibly causing that alert. Operators can see with the map view which nodes/channels are being affected, and they also can narrow down the list by time or severity so that they easily understand the priorities of alerts.

Drill Down - Correlation & Performance Graphs

Operators can drill down to a correlation graph describing a potential cause of the alert as shown in Figure 5. For example, suppose a video stream does not go through one router because of router trouble even though there is a multicast path between one input port and one output port of the router. The system creates an alert for this incident based on correlation analysis of the input and output ports on the router. Operators can drill down to the actual correlation graph causing this alert by mouse-focusing the router icon to see how much correlation value is out and how long the incident continues.

Operators can further drill down to performance graph with statistical information of network flows on the target router to understand cause of the issue. This view has utilization/packet counts for all the streams flowing on the router, and those for a specific channel stream can be selected by clicking one line of the channel stream in the middle graph or by entering the channel name in a search box.

Drill Down - Command Execution
Operators identify which router has an issue, and they need to manipulate that router to obtain more details (such as detailed status, configurations, and logs) by executing commands. This takes time and can cause human-error issues such as command misexecution. The UI has an execution interface of pre-fixed commands. Operators can select a prefixed command from a list shown on the router icon and get the output of command execution on the same screen.

4 EVALUATION OF CABLE NETWORK QoS ANALYSIS SOLUTION

For initial evaluation of the proposed solution, we examined network operations at a cable service provider and classified the types of the operations performed in the event of IP-related incidents (which the proposed solution can detect and identify) into the following four categories:

(A) Rebooted: Issues repaired by rebooting equipment.

(B) Operated: Issues repaired by operating equipment (e.g., by hardware/software operations effected by issuing commands or interacting with a GUI).

(C) Replaced: Repaired by replacing parts (e.g., an interface card) or equipment.

(D) Recovered: Problems were identified but had been resolved at the time of operations. (i.e., issue cleared while being investigated.)

Table 3 describes the percentage of each categorized operation over all the IP-related incidents occurred during a certain period. It also shows average time to close one incident by each categorized operation. About a half of the incidents were solved mostly by operating equipment (B), which took 3 hours 49 minutes on average per incident, and 22% were resolved by rebooting (A) taking 1 hour 43 minutes and replacing (C) taking 4 hours 9 minutes. 5% of the incidents were resolved in 44 minutes without any operations (D). Though there were no specific data showing a breakdown of MTTD and MTTR, it can be guessed that identifying an issue takes the same amount of time as spontaneous recovery (D). So we assume average MTTD for all the incidents is 44 minutes. The left part of Table 4 describes MTTD and MTTR calculated using the average times shown in Table 3 as current values.

Table 3: Type of operations for troubleshooting and average time to repair.

Operation type	Portion in all incidents	Avg. time [min]
(A) Rebooted	22.9%	163
(B) Operated	48.6%	229
(C) Replaced	22.9%	293
(D) Recovered	5.7%	44

We then calculated MTTD and MTTR when the proposing solution is introduced. The right part of Table 4 shows the average MTTD and MTTR of each categorized operation with our solution applied. In our supposition for MTTD, the average time to detect and identify an incident with the proposing solution is set to 15 minutes for all the incidents, as SNMP information is collected every 15 minutes and IP-related issues are notified to operators with failure point as soon as they are detected by the system. For MTTR the average times to reboot, operate, and replace were set to 67 minutes, 100 minutes, and 249 minutes, respectively. For the MTTR of the replacing, the time consumed is based on physical operations and therefore the proposed method does not reduce the time. Therefore we used the same MTTR with the current one. For the MTTR of the rebooting and the operating, the proposed method has a function to remotely execute typical commands to supported equipment. We supposed that half of the incidents can be handled by remote operations, which are assumed to take 15 minutes, and we took the average values of 15 minutes and the current MTTR values for the rebooting and the operating.

The average impairment time (i.e., MTTD + MTTR) is reduced to 62.3% of that without the proposed solution, which is shown at the bottom of Table 4 as total reduction by considering weight of each categorized operation. Looking at the incidents that happened more frequently (i.e., the ones resolved by rebooting and operating, which were 70% of the total incidents), the average impairment time can be reduced to 50%, which satisfies our goal set in Section 2.4. However, for the incidents resolved by Replacement, the reduction is low. This is because more time is consumed in direct operations or local works the solution does not cover.

5 CONCLUSION

Cable service providers are facing difficulty in managing service assurance due to their complex networks. We have recognized that limited end-to-end visibility of multicast video streams, operators'

Table 4: Evaluation of MTTD and MTTR by classified resolutions.

		Avg. time based on survey [min]			Avg. time w/ proposal [min]			Reduction
Operation type	% (a)	MTTD	MTTR	Sum (b)	MTTD	MTTR	Sum (c)	(c/b)*a
(A) Rebooted	22.9%	44	119	163	15	67	82	50.3%
(B) Operated	48.6%	44	185	229	15	100	115	50.2%
(C) Replaced	22.9%	44	249	293	15	249	264	90.2%
(D) Recovered	5.7%	44	0	44	15	0	15	34.3%
Total reduction by considering weight of each categorized operation (a)								62.3%

knowledge, and complexity of video services and routing flows lead to a long mean time for troubleshooting service delivery problems in the routing network. We have developed cable service QoS analysis solution that provides an end-to-end view of the control and data-plane flows associated with delivery of a video channel and shows identified failure points on the view. The solution supports topology discovery and visualization of the network and multicast trees, and it detects and identifies failure points by correlating multicast tree data and data/control-plane flows. Therefore operators can quickly identify issues and service impairment time is shortened.

We examined a list of the incidents at customer sites and evaluated the effectiveness of the proposed solution. Our initial evaluation revealed that it can detect all the IP-network related incidents, and the average service impairment time can be reduced to 62.3% of what it would be without the solution. For the incidents that happened most frequently, i.e., the ones resolved by rebooting and operating (70% of the total incidents), the average impairment time can be reduced to 50%, which satisfies our goal. Future works include development of the prototype system and verification of the solution in an actual environment.

REFERENCES

B. Fenner, M. Hadley, H. H. and Kouvelas, T. (2006). Protocol independent multicast – sparse mode (PIM-SM) protocol specification (revised). In *RFC4601*. PIM-WG, IETF.

Breibart, Y. (2000). Topology discovery in heterogeneous IP networks. In *INFOCOM 2000*, pages 26–30.

Cain, B. and Deering, S. (2002). Internet group management protocol, version 3. In *RFC3376*. IETF.

Cisco (2014). Cisco visual networking index: Forecast and methodology. In *Cisco White Paper*.

Garg, A. and Bindal, M. (2015). Enhancing QoS and QoE using big data in IPTV domain. In *Proc. of 2015 International Conference on Soft Computing Techniques and Implementations (ISCTI)*, pages 163–165.

Holbrook, H. and Cain, B. (2006). Source-specific multicast for IP. In *RFC4607*. IETF.

Kalyur, A. (2009). Video quality assurance across IP networks: Challenges, requirements & winning strategies. In *NCTA Technical Papers*, pages 20–24. The Internet & Television Association (NCTA).

Kim, H. and Feamster, N. (2013). Improving network management with software defined networking. In *IEEE Communication Magazine*, pages 114–119.

Liu, J. (2014). Monitoring and analyzing big traffic data of a large-scale cellular network with Hadoop. In *IEEE Network*, volume 28, pages 32–29.

Puneet Sharma, E. P. and Malpani, R. (2003). IP multicast operational network management: Design, challenges, and experiences. In *IEEE Network*, volume 17, pages 49–55.

Vasudevan, S. and Ogozaly, R. W. (2009). The headend revisited: A multi-service video data center for the modern MSO. In *NCTA Technical Papers*, pages 25–38. The Internet & Television Association (NCTA).