IADIS International Journal on WWW/Internet
Vol. 18, No. 2, pp. 101-115
ISSN: 1645-7641

DYNAMICALLY PRIORITIZED FAILURE MANAGEMENT ACCORDING TO RELIABILITY MODEL IN LARGE-SCALE DATA CENTER

Hideki Okita[1], Hayato Hoshihara[2], Norihisa Komoda[3] and Toru Fujiwara[3]
[1]*Research and Development Group, Hitachi, Ltd. 1-280 Higashi-Koigakubo, Kokubunji, Tokyo, 185-8601, Japan*
[2]*IoT & Cloud Services Business Division, Hitachi, Ltd. 6-26-3 Minamioi, Shinagawa-ku, Tokyo, 140-0013, Japan*
[3]*Graduate School of Information Science and Technology, Osaka University, 1-5 Yamadaoka, Suita, Osaka, 565-0871, Japan*

ABSTRACT

We propose a dynamically prioritized failure management method according to the reliability model that the failure rate of virtual machine varies in its life cycle. When using a combination of server monitoring with ping and network connection check with Ethernet OAM, the system sets higher priorities to the port connected to a long running server, and the port within a certain time after the connection change or virtual machine addition is set. The system then selects the ports from the higher priority port to be monitored by Ethernet OAM. As a result of the evaluation by the simulation, by dynamically selecting the port to be monitored for Ethernet OAM using the proposed method, it was confirmed that more than a third of all failures were detected with Maintenance End Points which number is only a tenth of that of servers in a data center. In the data center for cloud services running many VMs, it is possible to shorten the recovery from VM failure while suppressing the number of objects monitored by Ethernet OAM by using this method.

KEYWORDS

Virtual Network, Network Management, Data Center, Cloud Service, OAM, MEP

1. INTRODUCTION

As cloud services are applied to wider business fields, the demand for stable operations of IT systems in data centers that provide cloud services is growing. It requires not only higher reliability of the IT systems and but also rapid recovery to the normal state at the failures of the IT systems. The rapid recovery requires not only rapid detection of the failures and but also

rapid locating the points of failure among various devices such as servers and network switches in data centers.

The load on administrators to manage the devices increases as the number of monitored devices in IT systems increases. The number of monitored devices is increasing especially in the data centers of cloud service providers and large companies due to the adoption of server virtualization technologies which enables to deploy multiple logical servers, called virtual machines (VMs), on a physical server. Also, network function virtualization (NFV) which virtualizes networks by virtual network function (VNF) is introduced in data centers. Network devices such as proxy servers, firewall devices, load balancers, and WAN optimization devices are running as VMs on servers (Luizelli, M.C. et al, 2015).

Communication protocols are standardized and widely used to monitor remotely server availability and network connectivity in data centers. In particular, ICMP (Internet Control Message Protocol) is the standard protocol for network management systems to monitor servers and network devices in TCP/IP networks by exchanging monitoring packets, well known as 'ping' (Postel, J., 1981).

Also, Ethernet OAM (Operations, Administration and Maintenance) is developed to monitor connectivity in Ethernet-based wide-area networks (WANs) (McFarland, M. et al, 2005). IEEE802.1ag (IEEE 802.1 WG, 2007) and ITU-T Y.1731 (ITU-T, 2015) are defined as the standard of Ethernet OAM. Ethernet OAM functions are generally implemented in network devices. Maintenance End Points (MEPs) functions of Ethernet OAM supported devices transmit and receive continuously monitoring frames to check connectivity as shown in Figure **1**. Since the wide-area networks are shared by multiple users, it is required to detect rapidly, sometimes in milliseconds, failures in wide-area networks. The monitoring frames are frequently sent for the rapid failure detection.

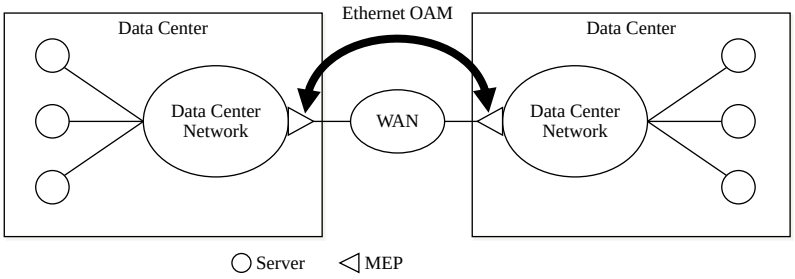

Figure 1. Failure Management of Ethernet-Based Wide-Area Network with Ethernet OAM

However, the combination of ping and Ethernet OAM is not sufficient for the failure management of large-scale data centers. As mentioned above, a lot of VMs, VNFs and physical servers are connected to data-center networks in large-scale data centers. Due to those increasing complexity and size, failures in data-center networks cause service failures in large-scale data centers. Thus, the need to monitor data-center networks has increased. On the other hand, Ethernet OAM is originally designed for monitoring aggregated links on wide-area networks among multiple data centers. In most cases, the number of devices that can be monitored with Ethernet OAM is less than the number of VMs and physical servers in a large-scale data center. It means that all failures in a data-center network are not detected with Ethernet OAM. The issue to apply Ethernet OAM to the failure management of data-center networks is how to choose

VMs or servers to be monitored with Ethernet OAM while minimizing the number of failures that are not detected. The objective of this paper is to provide a new method to select monitored VMs that are more likely to fail compared to other VMs in a data center.

In this paper, we focus on the reliability of VMs which vary through its lifecycle. We propose a method to model the varying failure rate of the VM and to elect the target to focus on based on the failure rate. The following sections of this paper are constructed as follows. Section 2 describes related research works to monitor virtual networks. Section 3 describes an efficient virtual network monitoring system based on the life cycle of physical servers and VMs in the data center. Section 4 describes the evaluation results of the effectiveness of the proposed method by simulation. In addition, we examine the characteristics of the assumed model parameters when they are different from the model parameters being monitored.

2. RELATED WORK

The network problem is a major factor of service failures and accounted for 76% of the failure factors according to the failure analysis in a large-scale Internet service (Oppenheimer, D. et al, 2003). Also, the failures due to network problems are not insignificant according to the investigation results of the research institution (Schroeder, B. and Gibson, G.A., 2006) and the survey result in a commercial data center (Birke, R. et al, 2014).

From the server management viewpoint, a method to monitor intensively the servers that affect the surrounding servers at the failure is studied to reduce the load on the monitoring system (Zheng, Z. et al, 2012). Also, a high-performance monitoring server using TCP libraries is developed to process more TCP-based monitoring messages in large data centers (Guo, C., 2015). A distributed architecture of monitoring system that monitors the adjacent database servers in the network for their health status is also studied (Singh, H., 2012).

From the network management viewpoint, anomaly detection methods for network devices based on passive measurement are studied for precise and sensitive failure detection by using various statistical information (Tang, Y. et al, 2005; Gomes, R.L. et al, 2016; Katzela, I. and Schwartz, M., 2015; Liu, D. et al, 2013; Thottan, M. and Ji, C., 2003; Lakhina, A. et al, 2005; Mi, H. et al, 2013), although those require more monitoring resources of the network monitoring systems. From the active measurement viewpoint, a framework for achieving proactive network management is developed to predict exceptions in IP/MPLS networks by using OAM functions (Dini, P. et al, 2004). Also, a framework to integrate service-level monitoring with fault management using Ethernet OAM is developed for interconnected networks of Ethernet service providers so that they can identify rapidly the root cause in the networks (Varga, P. and Moldovan, I., 2007). However, these studies focus on networks with fixed monitoring targets for network service providers.

Also, the number of network end points that a network switch can monitor with Ethernet OAM at once is limited to at most tens due to the limitation of hardware resource such as a CPU of the network switch. As the number of monitored end points increases, the network switch receives more Continuous Check (CC) messages from the end points. It causes increasing CPU usage of the network switch to process the messages. For example, the maximum number of the monitored end points that a network-switch product can monitor in a network is set to 100 in default.

Therefore, the data center of a large-scale cloud service provider that creates and runs thousands of VMs and hundreds of thousands of VLANs, cannot set all VMs and VLANs to be monitored with Ethernet OAM at the same time. As a result, while ping is used for all servers, the Ethernet OAM is used for limited servers. Therefore, servers that are not monitored with Ethernet OAM must be performed the connection check of the corresponding network part again once the failure of the server is detected at the service level by ping. There is a problem that it takes time to isolate the failure cause between the server and the network.

3. DINAMICALLY PRIORITIZED VIRTUAL NETWORK MONITORING

3.1 Method Overview

In this paper, we propose a new method of monitoring to reduce the average server failure locating time. Figure 2 shows the failure management in the method in a data center with Ethernet OAM and ping.

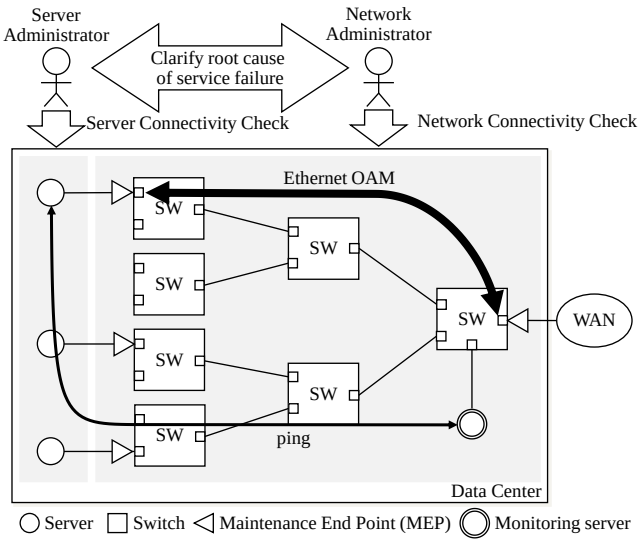

Figure 2. Failure Management of Data Center with Ping and Ethernet OAM

Usually, there are two types of administrators in a data center; server administrators who use ping to monitor servers and network administrators who use Ethernet OAM to monitor networks in the data center. They should cooperate to clarify the root cause of service failures in the data center. When a server administrator detects a service failure by missing responses of ping messages from a monitoring server, the root cause of the failure is not yet clarified. A network administrator thus explores the Ethernet OAM monitoring point called Maintenance End Point (MEP) of the port that the server is connected. If the network administrator finds a failure with Ethernet OAM, the cause of the service failure exists in the network side. On the other hand, if

Ethernet OAM does not detect a failure, it is considered that the cause of the service failure exists in the server side.

We introduce a new concept of dynamically selecting VMs to be monitored based on the stage of the VM lifecycle. In the past, the monitoring priorities of VMs are fixed throughout the lifecycle. However, when an IT system deploys a new physical server to activate a VM and changes its settings, if the elapsed time since it was activated is long, the hardware running the VM is likely to fail. Therefore, by increasing the allocation monitoring resources for VMs in such stage, and by decreasing the allocation monitoring resources for VMs in other stages, it is possible to shorten the average failure detection without increasing monitoring resources.

In order to select the monitored port, it is necessary to define and calculate the priority which changes in the time series according to the stage of the life cycle for each VM as an indicator of the selection. Therefore, the monitoring priority of the VM is changed according to the time series change of failure rate per VM. The pattern of failure rate for the operating time of a typical hardware including HDD on the server in the data center follows the so-called bathtub curve. The failure rate showed a high value early, decreased and eventually stabilized to a low value over time, and the high value is again shown by wear at the end of the life cycle (Yang, J. and Sun, F.B., 1999; Schroeder, B. and Gibson, G.A., 2007). Therefore, since the initial failure rate is high at the time of the introduction of the server, the monitoring priority of the VM running on the server is high, and the priority due to the initial failure is lowered over the period. On the other hand, the monitoring priority rises due to hardware wear over time.

Figure 3 shows which VMs in the data center are selected for monitoring based on the monitoring priority calculated for each VM, and also shows the time variation of the selected VM combinations. The four graphs of the left part of Figure 3 show the time variation of the monitoring priority for each of the four VMs. In addition, the thick lines of each graph represent the state in which the VM was selected for monitoring.

In this example, the number of MEPs that can be allocated is limited to two. Two MEPs are first allocated to the network switch SW21 to monitor the connectivity to the ports connected to two servers when the servers activated two VMs at Feb. 2016. When the third server with a VM is connected to the network switch SW22 at Mar. 2016, the port that connects the first server is excluded from the monitored ports. And the port that connects the third server is added to the monitored ports. In addition, when the VM on the second server moves to the third server at Apr. 2016, the priority of the port of the network switch SW22 that the third server is connected is increased to reflect the rise of the failure rate due to the configuration change, and the port is added to the monitored ports. At the same time, the port of the network switch SW21 connecting the first server is added again to monitored ports as the failure rate of the first server rises.

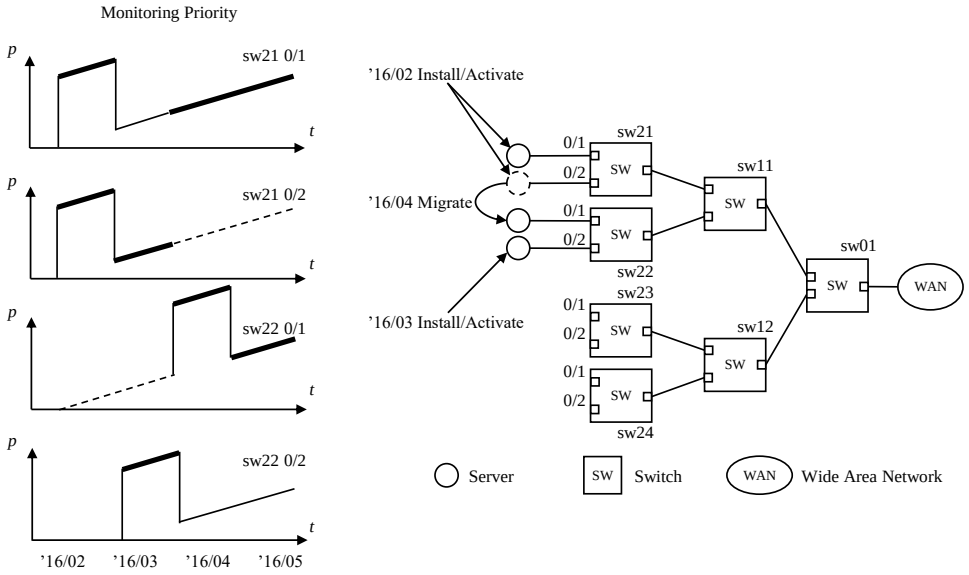

Figure 3. VM Monitoring Priority

3.2 Port Monitoring Priority

To prioritize the above mentioned monitored ports, the proposed method calculates the port monitoring priority for each port of the switch in the network based on the total failure rate. The port monitoring priority p can be expressed as the following equation using the server wear failure rate $\lambda_{\text{wear}}(t)$, server initial failure rate $\lambda_{\text{init}}(t)$, and server change-derived failure rate $\lambda_{\text{chg}}(t)$.

$$p = 1 - (1 - \lambda_{\text{wear}}(t))(1 - \lambda_{\text{init}}(t))\big(1 - \lambda_{\text{chg}}(t)\big)$$

The method calculates the failure rate of the server wear-out failure $\lambda_{\text{wear}}(t)$ as following. Since the components of the server wears out as time goes on, the failure rate increases as well. The parameters a and t_1 represent the speed of wear-out and the time when the server has been deployed, respectively.

$$\lambda_{\text{wear}}(t) = \begin{cases} 1 - e^{-a(t-t_1)} & (t \geq t_1) \\ 0 & (t < t_1) \end{cases}$$

The method then calculates the server initial failure rate $\lambda_{\text{init}}(t)$ from the uptime of the server. The failure rate $\lambda_{\text{init}}(t)$ of a server is assumed to follow the following equation. Since the initial failure decreases as time goes on, the failure rate decreases as well. The parameter σ_{init} indicates the speed of stability of the server. By such an expression, it expresses the state that the service failure occurs due to a configuration error for a certain time since the server has been deployed or changed or a virtual machine is deployed on the server.

$$\lambda_{\text{init}}(t) = \frac{W_{\text{init}}}{\sqrt{2\pi}} e^{-\frac{(t-t_1)^2}{2{\sigma_{\text{init}}}^2}}$$

Then, this method checks whether the selection port is moved from the server connection change information, and that the date and time are entries prior to the specified times. If there is an appropriate entry, we calculate the failure rate $\lambda_{\text{chg}}(t)$ from the server change based on the

elapsed time since the server connection occurred for each entry. If there is no entry, this method proceeds without calculating the failure rate $\lambda_{\text{chg}}(t)$ of the server changes. The failure rate $\lambda_{\text{chg}}(t)$ is expressed as a failure rate that combines the failure rates caused by individual connection changes as following. The failure rate caused by each connection change is represented by a normal distribution centered on $t = t_m$ (m = 0, 1, 2, ...) which is the timing of m^{th} connection change.

$$\lambda_{\text{chg}}(t) = W_{\text{chg}} - W_{\text{chg}} \prod_{m} \left\{ 1 - \frac{1}{\sqrt{2\pi}} e^{-\frac{(t-t_m)^2}{2\sigma_{\text{chg}}{}^2}} \right\} (m = 0,1,2,\cdots)$$

3.3 MEP-Enabled Port Selection

The network monitoring system using the proposed method chooses which port of the network switch of the data center is monitored for the Ethernet OAM based on the abovementioned port monitoring priority. The network monitoring system, based on the port monitoring priority calculated in the manner described above, selects the port to be monitored of all ports connected to the server. In this case, the system selects the monitored port so that it does not exceed the maximum programmable MEP number of each switch.

4. EVALUATION OF MONITORING EFFICIENCY

4.1 Evaluation Method

By simulation, we compared the average failure locating time of each server in the following three cases; (1) dynamically changed monitoring by Ethernet OAM based on the proposed method, (2) fixed monitoring the server running an important application, and (3) ping without Ethernet OAM. For this simulation, a small-scale discrete event network simulator was developed in C++. When this simulator is started, the object of the network node with the start-up time information is generated for each server. For each time step, the simulator checks if server failure happened or not for each object based on its uptime, configuration changes and the probability distribution of server failure. Also, it selects dynamically the objects that are monitored by using Ethernet OAM with MEP from all objects according to the proposed method in case (3). At the same time, the simulator checks if the server failures are detected with Ethernet OAM. If MEP is configured for a network node in failure, the Ethernet OAM detects quickly the failure. On the other hand, if MEP is not configured, the failure is detected by ping as usual. Based on the results, the simulator calculates the average failure locating time for the entire data center.

The common parameters of the implemented simulator are shown in Table 1. The simulator runs simultaneously 1,000 of network nodes as simulated servers with the 7 days of simulation step interval for 5 years. A new network node is generated as a new running server when a network node is evaluated as a failed server. Each network node increases periodically its failure rate since simulated servers change those connections to the data-center network every 100 days.

Table 1. Simulation parameters

Parameter	Value
Number of nodes	1,000
Simulation duration	5 years
Simulation step interval	7 days
Server connection change frequency	Once in 100 days

In this evaluation, two types of server reliability models; a wear-out intensive model and an initial-failure intensive model were simulated. The simulation parameters of the wear-out intensive model and those of initial-failure intensive model are shown in the second column and the third column of Table 2, respectively. In the former model, initial failures and change failures affect the health of servers more strongly than wear out. On the other hand, in the later model, wear out of servers affects more strongly. Figure **4** shows the time-varying failure rate of a server of the wear-out intensive model and that of the initial-failure intensive model.

Table 2. Simulation parameters of failure rate

Parameter	Wear-out intensive	Initial-failure intensive
Wear-out failure gradient a	1.0e-9	2/3e-10
Initial failure rate amplitude W_{init}	0.0125	0.05
Initial failure rate standard deviation σ_{init}	8.0e4	5.0e5
Change failure rate amplitude W_{chg}	0.05	0.05
Change failure rate standard deviation σ_{chg}	8.0e4	5.0e5

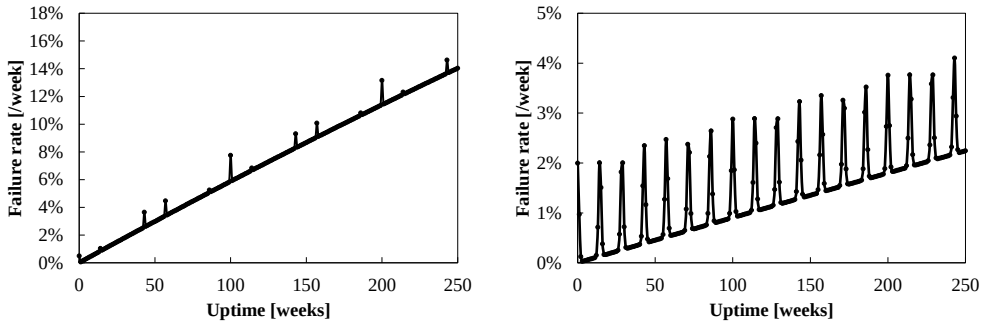

Figure 4. Server Failure Rate in Wear-Out Intensive case (Left) and That in Initial-Failure Intensive Case (Right)

4.2 Evaluation Results

We evaluate the improvement of the server failure locating time and the server failure detection rate by the proposed method. The server failure locating time is composed of the time that the monitoring system took for detecting a server failure by ping and the time that a network administrator took for identifying the network-side or the server-side as the cause of the server failure by using Continuity Check (CC) or Loop Back (LB) functions of Ethernet OAM. The server failure detection rate is defined as the percentage of servers that have been set to be monitored by using CC of Ethernet OAM with MEP among the servers that failed at the data

center during the simulation. The parameters used to calculate the server failure locating time according to the server failure detection rate are shown in Table 3.

Table 3. Evaluation parameters

Parameter	Value
Ethernet OAM CC interval	1 minute
Ping interval	15 minutes

The simulation results of the numbers of server failures are shown in Table 4. As the server change rate increases from 10% to 50%, the number of total failures is reduced from 1357.65 to an average of 213.47 in the wear-out intensive case. The average running time of the server is shortened as the server change rate increases. The server failure decreased since the servers were replaced before the server failure occurs due to the wear. On the other hand, in the initial-failure intensive case, the server change rate did not have large effect on the number of failures.

Table 4. Numbers of Server Failures

Server change rate [/week]	Wear-Out Intensive Case	Initial-Failure Intensive Case
10%	1357.65	1149.38
20%	700.13	1152.33
30%	444.97	1168.65
40%	307.11	1139.02
50%	213.47	1067.61

Also, Figure 5 and Figure 6 shows the simulation results of the server failure locating time and the server failure detection rate by the monitoring system. It shows, per server change rate, the number of failures, the server failure detection rate in the conventional method, and the server failure detection rate in the proposed method. The server failure detection rate represents the rate of the server that MEP is configured to the corresponding port and the system has detected the failure quickly by Ethernet OAM, of all the servers that failed through the simulation period. The MEP number was set to 16, and the server change rate was 10% per week to 50% per week every 10%. The average value of the server failure locating time was calculated by executing the simulation 100 times for each of the five server change rates.

In the wear-out intensive case, the results of average server failure locating time for server change rates from 10% to 50% in the wear-out intensive case were 754 seconds for ping only case, 749 seconds for the conventional method case and 734 seconds for the proposed method case, respectively, as shown in Figure 5. The change in server change rate did not affect the average server failure locating time or the average server failure detection rate. The proposed method reduced the average server failure locating time by 2.1% and 2.7% compared to the conventional method case and ping only case, respectively. Also, the proposed method improved the server failure detection rate by 5.32 points in average compared to the conventional method. It can be said that the proposed method increases the average server failure detection rate in data center and reduces the average server failure locating time regardless of the server change rate.

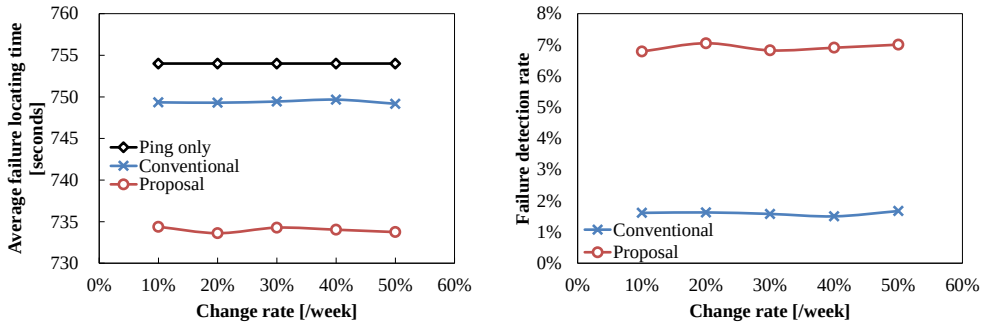

Figure 5. Average Failure Locating Time (Left) and Average Failure Detection Rate (Right) for Change Rates in Wear-Out Intensive Case

Also, in the initial-failure intensive case, the results are shown in Figure 6. As the server change rate increased from 10% to 50%, the average server failure locating time of the proposed method increased and got closer to the result of the conventional method since the server failure detection rate decreases from 4.1% to 2.3%.

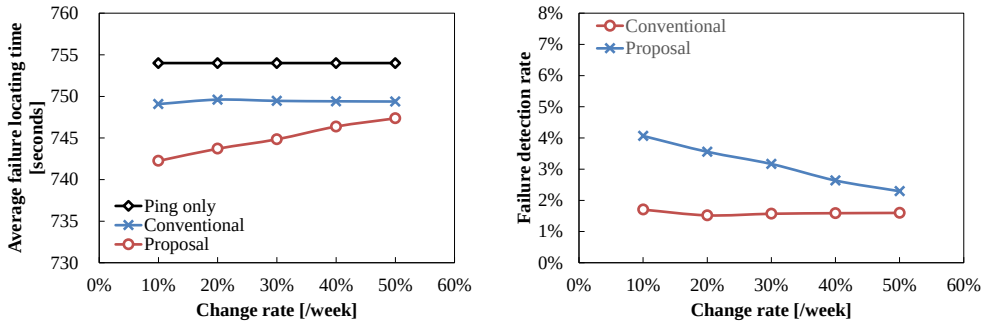

Figure 6. Average Failure Locating Time (Left) and Average Failure Detection Rate (Right) for Change Rates in Initial-Failure Intensive Case

Also, the effect on the average server failure locating time by the number of MEPs is evaluated under the server change rate 20% per week. In the case of the number of MEPs of 8, 16, 32, 64 and 128, each of the simulation is performed 100 times. In each case, the average server failure locating time was measured.

The results of this measurement in the wear-out intensive case are shown in Figure 7. As a result of this measurement, the average of about 702 server failures occurred. When 128 MEPs are used to monitor servers, the average server failure locating time was shortened from 754 seconds to 716 seconds when the server was monitored by the Ethernet OAM in the conventional method. Further, the average server failure locating time was shortened from 716 seconds to 653 seconds when servers are monitored with Ethernet OAM in the proposed method. The proposed method reduced the average server failure locating time by 8.8% and 13% compared to the conventional method case and ping only case, respectively. Also, the average server failure detection rate was improved from 13% with the conventional method to 35% with the proposed method. More than a third of all failures were detected with MEPs which number is only a tenth of that of servers in a data center.

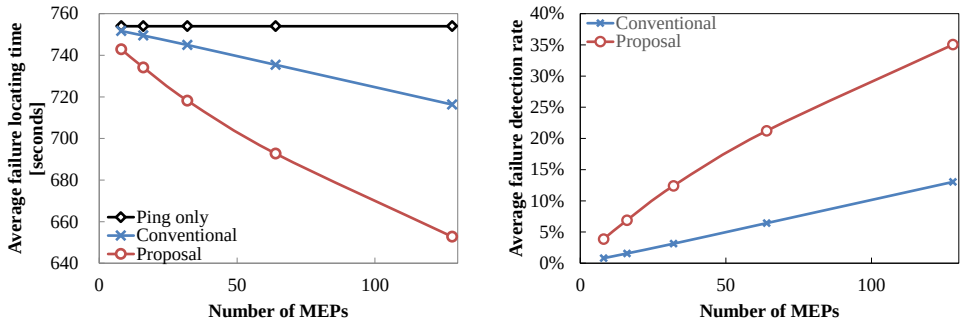

Figure 7. Average Failure Locating Time (Left) and Average Failure Detection Rate (Right) for the Numbers of Configured MEP in Wear-Out Intensive Case

The evaluation results of the initial-failure intensive case are also shown in Figure 8. The results showed almost same characteristics with those of wear-out intensive case. The average server failure locating time was shortened from 717 seconds with the conventional method to 670 seconds with the proposed method. Also, the average failure detection rate was improved from 13% with the conventional method to 29% with the proposed method.

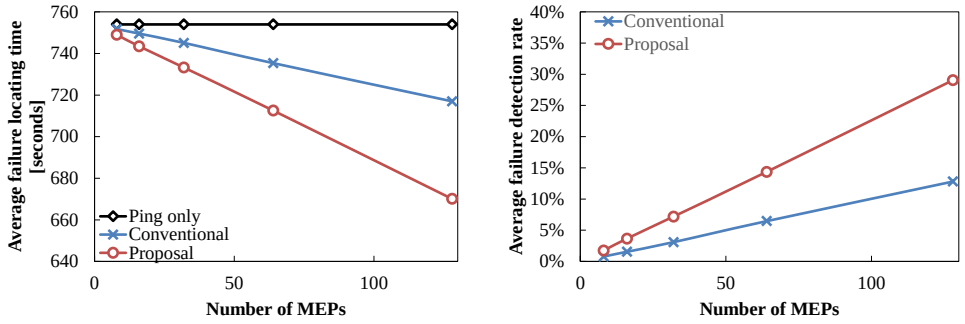

Figure 8. Average Failure Locating Time (Left) and Average Failure Detection Rate (Right) for the Numbers of Configured MEP in Initial-Failure Intensive Case

4.3 Sensitivity Analysis

As the results of the evaluation with the wear-out intensive model and 16 MEPs, the effect on the server failure detection rate is shown in the left part of Figure 9 when the parameter W_{init} which indicates the magnitude of the initial failure and the amplitude of the change failure used to estimate the server failure rate is different from the actual value. In addition, the right part of Figure 9 shows the effect of the parameter σ_{init} which represents the deviation in the time axis of the initial failure and the change failure used to estimate the server failure rate is different from the actual value. Even if the estimated value of the variance σ_{init} or amplitude W_{init} is shifted from the actual value, there is no significant change in the evaluation result of the server failure detection rate even in the case of the conventional method and the proposed method.

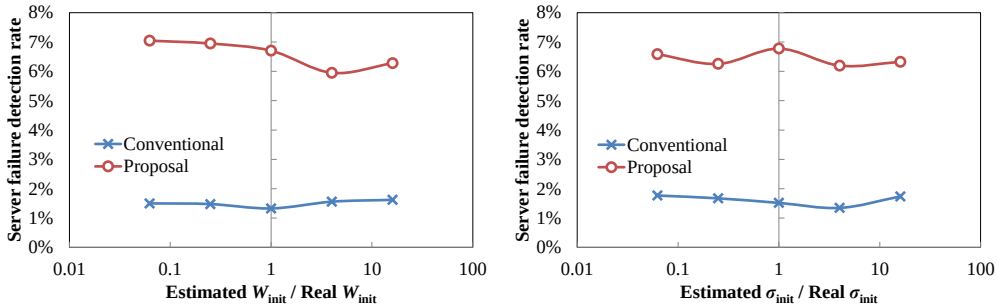

Figure 9. Sensitivity Analysis for W_{init} (Left) and for σ_{init} (Right) with 16 MEPs in Wear-Out Intensive Case

As the results of the evaluation with initial-failure intensive model and 16 MEPs, the effect of the parameter W_{init} on the magnitude of the initial failure and the amplitude of the change failure is different from the actual value used to estimate the server failure rate is shown in the left part of Figure 10. In addition, the effect of the parameter σ_{init} on the size of the variance of the time axis of the initial failure and the change failure used to estimate the server failure rate is different from the actual value is shown in the right part of Figure 10. In the case of the proposed method, the server failure detection rate has changed significantly when the deviation σ_{init} is shifted. Specifically, when the ratio of the estimated value of σ_{init} to the actual deviation σ_{init} is 0.5 or less, the server failure detection rate is almost unchanged from the conventional method. On the other hand, when the ratio of deviation σ_{init} is 1 or more, the proposed method exhibits a higher server failure detection rate of about 2.5 points compared to the conventional method.

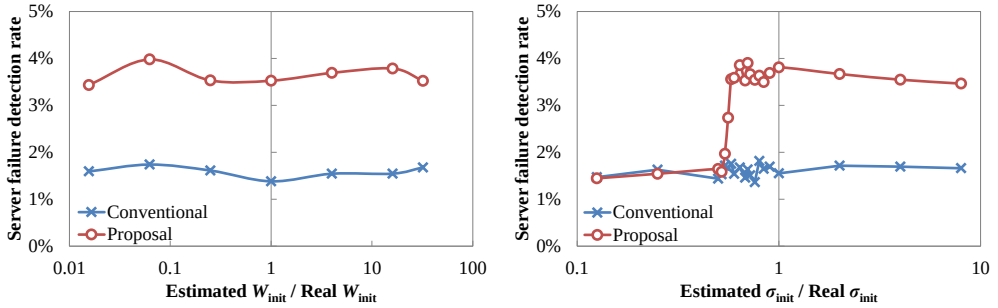

Figure 10. Sensitivity Analysis for W_{init} (Left) and for σ_{init} (Right) with 16 MEPs in Initial-Failure Intensive Case

The results of the evaluation with the wear-out intensive model and 128 MEPs are shown in Figure 11. Also, the results of the evaluation with the initial-failure intensive model and 128 MEPs are shown in Figure 12. As same with the results of the evaluation with 16 MEPs, even if the estimated value of the variance σ_{init} or amplitude W_{init} is shifted from the actual value, there is no significant change in the evaluation result of the server failure detection rate Also, the proposed method exhibits a higher server failure detection rate when the ratio of deviation σ_{init} is 1 or more in the initial-failure intensive case. These results show that the number of MEPs does not have the effect on the characteristics of sensitivities of server failure detection rates.

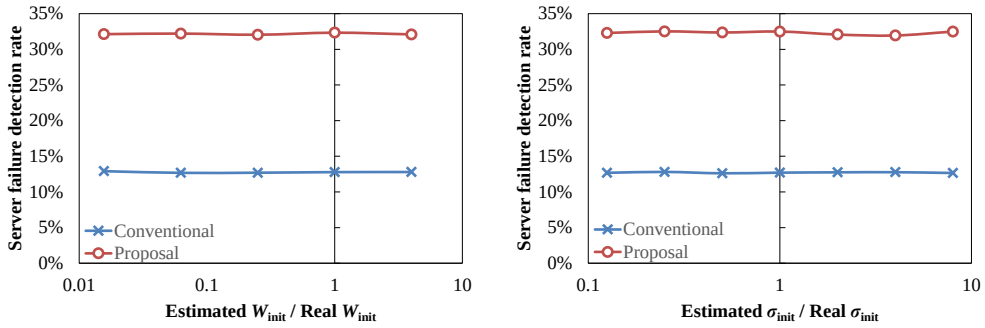

Figure 11. Sensitivity Analysis for W_{init} (Left) and for σ_{init} (Right) with 128 MEPs in Wear-Out Intensive Case

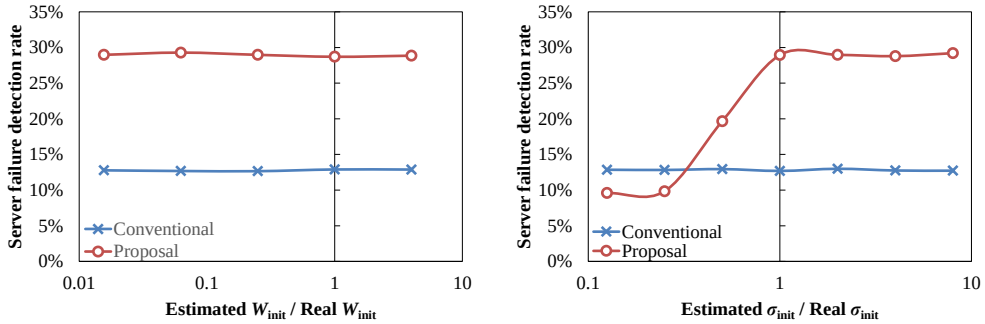

Figure 12. Sensitivity Analysis for W_{init} (Left) and for σ_{init} (Right) with 128 MEPs in Initial-Failure Intensive Case

5. DISCUSSION

As shown in Figure 7, the average server failure detection rate can be improved from about 7% to 35% when the number of MEPs activated in the network of data centers running 1000 servers is increased from 16 to 128. Therefore, the number of MEPs should be determined according to the target of the failure detection rate or the failure locating time of the data center. Also, we consider the results of the above sensitivity analysis for the case when the initial failure and change failure is dominant. If the ratio of the deviation σ_{init} of the estimated server failure rate to that of the actual server failure rate is less than 0.6, the server failure detection rate of the proposed method decreases to the same level with that of the conventional method. The cause of this behavior can be considered as follows. It is considered that if the actual value of the variance is greater than the estimate, it is more likely that a server that is not set as a monitored target by a MEP will fail. As a result, it is thought that it is the same as the case where the monitored targets by MEPs are selected substantially randomly. To avoid this problem, it is necessary to accurately calculate the deviation σ_{init} of the actual server failure rate in advance based on the failure history of servers in a data center in the past as much as possible.

6. CONCLUSION

We proposed a new network monitoring method which coordinates server management and network management. Specifically, we developed a dynamically prioritized failure management method that dynamically changes the server to be monitored with Ethernet OAM according to the server failure rate estimated based on the uptime and configuration changes of the server. As an evaluation result by the network simulator, more than a third of all failures were detected with MEPs which number is only a tenth of that of servers in a data center. It can be said that coordinating server management and network management makes efficient the failure management in the large-scale data center.

REFERENCES

Birke, R. et al, 2014. Failure analysis of virtual and physical machines: Patterns, causes and characteristics. *Proceedings of 2014 Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'14)*, Atlanta, U.S.A.

Dini, P. et al, 2004. IP/MPLS OAM: Challenges and directions. *Proceedings of IEEE International Workshop on IP Operations and Management*, Beijing, China.

Gomes, R.L. et al, 2016. Software defined management of edge as a service networks. *In IEEE Transactions on Network and Service Management*, vol.13, no.2, pp.226–239.

Guo, C. Et al, 2015, Pingmesh: A large-scale system for data center network latency measurement and analysis, *Proceeding of ACM SIGCOMM 2015*, London, United Kingdom.

IEEE 802.1 WG, 2007. IEEE Std 802.1ag-2007 virtual bridged local area networks, amendment 5: Connectivity fault management. *IEEE Standards*, IEEE Std 802.1ag-2007.

ITU-T, 2015. Operation, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks. *ITU-T Recommendation*, ITU-T G.8013/Y.1731.

Katzela, I. and Schwartz, M., 2015. Schemes for fault identification in communication networks. *In IEEE/ACM Transactions on Networking*, vol.3, no.6, pp.753–764.

Lakhina, A. et al, 2005. Mining anomalies using traffic feature distributions. *Proceedings of ACM SIGCOMM 2005*, Philadelphia, U.S.A.

Liu, D. et al, 2013. Network traffic anomaly detection using clustering techniques and performance comparison. *Proceedings of IEEE CCECE 2013*, Regina, Canada.

Luizelli, M.C. et al, 2015. Piecing together the nfv provisioning puzzle: Efficient placement and chaining of virtual network functions. *Proceedings of 14th IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*, Ottawa, Canada, pp.98–106.

Mi, H. et al, 2013. Toward finegrained, unsupervised, scalable performance diagnosis for production cloud computing systems. *In IEEE Transactions on Parallel and Distributed Systems*, vol.24, no.6, pp.1245–1255.

McFarland, M. et al, 2005. Ethernet oam: Key enabler for carrier class metro ethernet services. *In IEEE Communications Magazine*, vol.43, no.11, pp.152–157.

Oppenheimer, D. et al, 2003. Why do internet services fail, and what can be done about it?. *Proceedings of 4th USNIX Symposium on Internet Technologies and Systems (USITS'03)*, Seattle, U.S.A.

Postel, J., 1981. Internet control message protocol (ICMP). *IETF RFC*, RFC 792.

Schroeder, B. and Gibson, G.A., 2006. A large-scale study of failures in high-performance computing systems. *Proceedings of 2006 International Conference on Dependable Systems and Networks (DSN'06)*, Philadelphia, U.S.A.

Schroeder, B. and Gibson, G.A., 2007. Disk failures in the real world: What does an MTTF of 1,000,000 hours mean to you?. *Proceedings of FAST'07*, San Jose, U.S.A.

Singh, H., 2012, Fault-tolerance in Windows Azure SQL database, *Azure Blog*, available at: https://azure.microsoft.com/en-us/blog/fault-tolerance-in-windows-azure-sql-database/ (accessed 28 December 2020).

Tang, Y. et al, 2005. Active integrated fault localization in communication networks. *Proceedings of 9th IFIP/IEEE Interna tional Symposium on Integrated Network Management (IM 2005)*, Nice, France, pp.543–556.

Thottan, M. and Ji, C., 2003. Anomaly detection in IP networks. *In IEEE Transactions on Signal Processing*, vol.51, no.8, pp.2191–2204.

Varga, P. and Moldovan, I., 2007. Integration of service-level monitoring with fault management for end-to-end multi-provider ethernet services. *In IEEE Transactions on Network and Service Management*, vol.4, no.1, pp.28–38.

Yang, J. and Sun, F.B., 1999. A comprehensive review of hard-disk drive reliability. *Proceedings of Annual Reliability and Maintenability Symposium (RAMS)*, Washington, DC, U.S.A., pp.403–409.

Zhen, Z. et al, 2012, Component ranking for fault-tolerant cloud applications, *In IEEE Transactions on Services Computing*, vol.5, no.4, pp.540-550.