Root-Cause Diagnosis for Rare Failures using Bayesian Network with Dynamic Modification

Yoichi Matsuo, Yuusuke Nakano, Akio Watanabe, Keishiro Watanabe, Keisuke Ishibashi, Ryoichi Kawahara
NTT Network Technology Laboratories, NTT Corporation, Tokyo 180-8585, Japan
Email:{matsuo.yoichi, nakano.yuusuke, watanabe.a, watanabe.keishiro, ishibashi.keisuke, kawahara.ryoichi}@lab.ntt.co.jp

***Abstract*—We propose a root-cause diagnosis method for finding equipment suffering from rare failures in a communication network. Although many studies have been conducted on root-cause diagnosis for finding failed equipment using a Bayesian Network or other methods, there has not been sufficient research into finding rare-failure equipment. Current methods are mainly focused on typical-failure equipment and cannot find rare-failure equipment. This is because rare failures have two features; unexpected causal relations and observation errors. To adapt rare-failure features, we propose a method that consists of an extended causal model and an extended inference algorithm with dynamic modification of the causal relations and observation statuses in a Bayesian Network. We experimentally evaluated its effectiveness.**

I. Introduction

Network operations require a root-cause diagnosis method for finding failed equipment. If a failure is detected with a single alert generated by the failed equipment, finding the equipment is straightforward task. However, an equipment failure usually affects related (physically or virtually connected) network components, which then generate alert messages. In that case, the failed equipment (root-cause) is difficult to find from alerts and other observation data. To automate this task, several rule-based software products [2], [3] and methods based on a stochastic model [4]–[11] have been developed. These products and methods find failed equipment using causal relations between failed equipment and observation data, such as alerts and traffic. The causal relations in these products and methods are created by using expert knowledge or training data, and since in most failure cases, observation data explicitly change in accordance with expected causal relations, these products and methods can determine failed equipment. Therefore, if we can obtain a correct model of the causal relation and correct observation data as input for the model, we can find failed equipment.

However, these products and methods infrequently suffer from failures such as silent failures, mis-configurations and compound events, in which we cannot expect to obtain such correct causal relations or correct observation data. We call such failures "rare failures" to distinguish them from "typical failures". Even though such failures rarely occur, their impacts on services provided in the networks are larger than those of typical failures according to interviews with operators.

Rare failures can be attributed to two features; **unexpected causal relations**, which cause model errors, and **observation errors**, which cause input errors. Below, we describe both features and how they make it difficult to find failed equipment.

Unexpected causal relations between network equipment status and observation data make failed equipment hard to find. For instance, one of the methods of determining a causal relation is using expert knowledge, such as "If router A fails, alerts of router A and of other routers connected to router A should be generated." If an alert is generated by a typical failure, then expert knowledge will work and operators can determine the failed equipment. However, since rare failures such as compound failures generate alerts at unexpected equipment, failed equipment of rare failures are difficult for operators to determine.

One example of an observation error is a silent failure, which might not generate alerts explicitly. Another example is mis-configuration of the observation-data threshold, which generates alerts even though the network equipment is normal. Consequently, since some observed data are missing or methods obtain extra alerts, failed equipment becomes difficult to find.

We propose a root-cause diagnosis method that consists of an extended causal model and an extended inference algorithm, which can be applied to other methods [4]–[11] to better estimate rare-failure equipment. Current methods assume that we can construct a correct causal model. Even though Shrink [4] assumes that there are some miss-constructions with very low probabilities, it might not select the correct failed equipment when it infers rare-failure equipment. This is because very low probabilities do not work enough for unexpected causal relations. Current methods also assume that we can observe correct observation data, but this assumption does not work well for rare failures. Note that we use Shrink as the current method and that our proposed method is based on Shrink since it does not need training data of failures or it is easy to implement. However, our method can be based on any other methods.

The approaches of this study are below. We developed an extended causal model that has two maps based on a Bayesian Network (BN). The first map is a causal-relation modification map that modifies a causal relation to adapt to unexpected

The concept of this paper was partly presented without being reviewed in March 2017 at the IEICE General Conference, which is a domestic conference in Japan [1].

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

causal relations. The second map modifies observation errors. It modifies the status of nodes that represent whether a certain alert is generated or not. Using the above developed model, our extended inference algorithm simultaneously infers failed equipment and modifies causal relations and observation status by using two maps with a penalty term. The failure type estimation which decides whether a failure is typical or rare, and parallelization are also introduced for reducing computation cost. We evaluated our method by comparing it with Shrink [4].

The rest of this paper is as follows. In Section II, we introduce the problem of finding failed equipment using a BN. We explain our method in Section III and our experiments in Section IV. We conclude our paper in Section V.

II. Problem Formulation

In this section, we mainly explain the problem of finding failed equipment using the current method, Shrink [4]. Shrink uses a BN model, which is a stochastic model and can be expressed by a graph, to infer unobserved variables from observed variables. The BN consists of equipment nodes and observation-data nodes that are random variables, edges between equipment nodes and observation-data nodes that are conditional probabilities, and prior probabilities. Equipment nodes represent the status of equipment, such as routers, switches and servers in a network. Observation-data nodes represent the status of observation data, such as traffic, syslogs, and alerts in a network. Each status has a normal status and failure status. Let x_i be a node that represents the status of network equipment i such as routers and servers, and y_j be a node that represents the status of the observation data j such as alerts.

$$X = (x_1, x_2, \ldots, x_n), x_i \in \{0, 1\} \quad (1)$$

$$Y = (y_1, y_2, \ldots, y_m), y_j \in \{0, 1\}, \quad (2)$$

where n is the number of pieces of equipment and m is the number of observation data. 0 means normal, and 1 means failure. For instance, if an alert is generated at observation data j, we set y_j to 1. To use traffic data, we calculate an anomaly score of the traffic data and set a threshold. If the anomaly score of traffic data corresponding to j is beyond the threshold, we set y_j to 1. Though we set x_i and y_j to only take two values, 0 or 1 for simplification, one can set more values. For instance, Sherlock [8] uses three values, which indicates the degree of a failure situation.

The edges and conditional probabilities represent the existence of a causal relation and the degree of the causal relation, respectively. If equipment i has a causal relation with observation data j, we add an edge $e_{i,j}$ between x_i and y_j. Let E be a set of all edges between X and Y, and d_j be a index set of $e_{i,j}$ i.e.,

$$d_j = \{i | e_{i,j} \in E\}. \quad (3)$$

Then, we define the conditional probabilities of an observations-data j for failure status given X as follows.

$$P(y_j = 1|X) = \frac{1}{C_j} \left(\frac{\sum_{i \in d_j} x_i}{|d_j|} - \alpha \right), \quad (4)$$

where the value C_j is a normalizing constant and α is a small constant value. This means if all equipment nodes x_i that have causal relations with y_j have a normal status (or failure status), the observation-data node y_j might be a normal status (or failure status). If some nodes of x_i have a normal status and the others have a failure status, the probability of a normal status for y_j is the ratio of normal statuses of x_i to failure statuses of x_i. As we stated in Section I, the edges and corresponding conditional probabilities are determined in advance.

The prior probabilities represent degree of to which equipment tends to be normal or failure. We set the prior probabilities to equipment nodes as follows.

$$P(x_i = 0) = 1 - \beta, \quad P(x_i = 1) = \beta,$$

where β is a small constant value.

Finally, when the observation-data nodes Y are given, the problem of obtaining the maximum a posteriori (MAP) p and finding the failed equipment nodes $\tilde{X}$ is below.

$$p = \max_X P(X|Y) = \max_X \frac{P(Y|X) P(X)}{P(Y)} \quad (5)$$

$$\tilde{X} = \arg\max_X P(X|Y) = \arg\max_X \frac{P(Y|X)P(X)}{P(Y)}, \quad (6)$$

under the condition that each x_i flips independently and the number of $x_i = 1$ is under κ, where $\kappa < n$ is the maximum number of pieces of simultaneous failed equipment.

III. Proposed Method

In this section, we explain our proposed method. The overview of our proposed method is illustrated in Fig. 1. The first process involves creating a causal model using topology data, history of failure data, traffic data, alerts, and so on in the same way as Shrink and creating an extended causal model by adding two modification maps to adapt to rare failures. This process is done off-line. The second process involves collecting and inputting observation data from the network and executing the inference algorithm to estimate failed equipment by using Shrink, if there is a failure. The third process is to determine whether the failure is typical or rare. If it is typical, our method outputs the estimated failed equipment and MAP by using Shrink. If it is rare, our method starts an extended inference algorithm in the fourth process. Finally, in the fifth process, we obtain the estimated failed equipment and MAP. In the following subsection, we explain our extended causal model, failure type estimation, extended inference algorithm, and scalability.

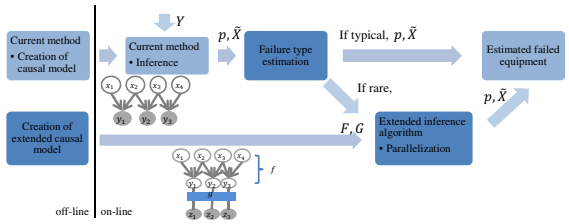

Fig. 1. Overview of our proposed method

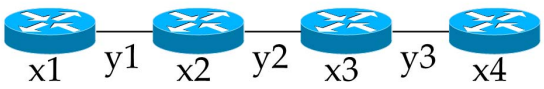

Fig. 2. Example of network

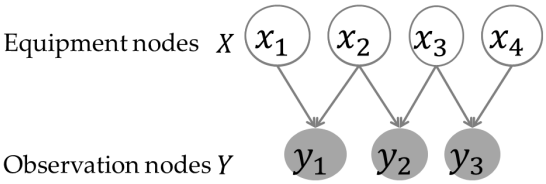

Fig. 3. Example of causal model with Shrink

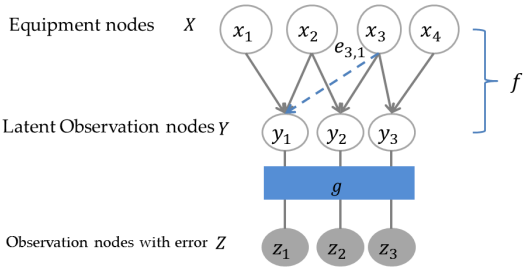

Fig. 4. Example of causal model with our proposed method

A. Extended Causal Model

We developed a causal model for finding failed equipment on the basis of a BN by combining two maps to adapt to the two rare-failure features. Consider the example network illustrated in Fig. 2. The causal models of an example network by the current method (Shrink) and our method are shown in Fig. 3 and Fig. 4, respectively. Unlike the causal model of Shrink, the model of our method has modification maps f and g, and other nodes Z that are converted from Y by a map g. We describe f, g and Z below.

First, we consider adapting the current causal model to unexpected causal relations in a BN. An unexpected causal relation can be seen as a modification (addition and deletion) of an edge and a change of the corresponding conditional probability in the BN. When a rare failure occurs in equipment i, if observation-data node y_j unconnected to x_i is affected, we regard the unexpected causal relation as an addition of a new edge from x_i to y_j.

Mathematically, we can formulate the modification as the map f that changes an edge set E to another edge set $f(E)$. The map f represents a collection of additions of new edges or deletions of existing edges. Since all pairs of edges between equipment nodes and observation nodes can be added or deleted, the number of maps f is 2^{nm}. Here we define GED (f) as the number of additions and deletions between E and $f(E)$. In other words, GED (f) is the Graph edit distance between E and $f(E)$ [11]. For instance, in Fig. 3, the original causal relation is represented as a edge set $E = \{e_{1,1}, e_{2,1}, e_{2,2}, e_{3,2}, e_{3,3}, e_{4,3}\}$. If we modify E by adding a new edge $e_{3,1}$ from x_3 to y_1, the modification map is given as $f(E) = \{e_{1,1}, e_{2,1}, e_{2,2}, e_{3,1}, e_{3,2}, e_{3,3}, e_{4,3}\}$. Since we only add a new edge, GED $(f) = 1$. In accordance with the modification of edge set E, the conditional probability also changes, and we define it as P_f. We use GED (f) to limit the number of modification because if we can modify the edges arbitrarily, solution is unreliable. Then we describe how to use GED (f) and how to find the correct modification of f in Subsection III-C.

Second, we consider g and Z for observation errors. For instance, if a rare failure occurs and there is an observation error, some alerts do not generate. This leads some observation-data nodes in the BN to have normal statuses when they should have failure statuses. To modify the observation error, we include the map that inverts the status value of observation-data nodes.

To include the observation modification map in our model, we divide the observation-data nodes Y into observation-data nodes Z with error and latent observation-data nodes Y with no error and add a map g that modifies the status from observation-data nodes with error Z, to observation-data nodes with no error Y, where we cannot observe data in practice. Then the map g represents removing the observation error in observation-data status Z. This leads to correct estimation of failed equipment. Let $g = (g_1, \ldots, g_m)$ and g_j be a signal of whether the status of each z_j is inverted or not. We calculate y as follows,

$$y_j = \begin{cases} z_j & (g_j = 0) \\ 1 - z_j & (g_j = 1) \end{cases}, \tag{7}$$

where $Z = (z_1, \ldots, z_m)$. For instance, assume that there are three observed data elements, $Z = (z_1 = 1, z_2 = 0, z_3 = 0)$, and there is an observation error in z_3. The correct value of this observation data is 1. We remove this observation error by using the observation-error modification map $g = (g_1 = 0, g_2 = 0, g_3 = 1)$.

$$g(Z) = (y_1 = 1, y_2 = 0, y_3 = 1). \tag{8}$$

By using g, we can obtain correct observation data, $y_3 = 1$. Since all pairs of observation node y_j can be inverted or not, the number of maps g is 2^m. Here we define HD (g) as the

number of the inverted nodes in Y. In other words, $\mathrm{HD}(g)$ is the Hamming distance. Similar to f, we describe how to find the correct modification of g in Subsection III-C. Since both modifications f and g are independent operation, we simultaneously modify edges and observation statuses by f and g. Let M be a set of each f and g, i.e., $M = \{f, g\}$.

Finally, for given $(f, g) \in M$, the equations that we have to solve to obtain the MAP $\tilde{p}$ and find failed equipment $\tilde{X}$, are as follows.

$$\tilde{p} = \max_X P_f\left(X|g(Z)\right) = \max_X \frac{P_f\left(Y|X\right)P\left(X\right)}{P\left(Y\right)} \tag{9}$$

$$\begin{aligned} \tilde{X} &= \arg\max_X P_f\left(X|g(Z)\right) \\ &= \arg\max_X P_f\left(Y|X\right)P\left(X\right), \end{aligned} \tag{10}$$

under the condition that each x_i flips independently and the number of $x_i = 1$ is under κ.

B. Failure Type Estimation

In order to avoid unnecessary model modification, this process determines whether the type of failure is typical or rare, since rare failures seldom happen. If there are unexpected causal relations or observation errors, this should lead to MAP p reducing significantly since the BN by Shrink cannot adapt to rare-failure features. Therefore we focus on MAP. Hence our failure type estimation algorithm decides whether a failure is typical or rare by using a local outlier filter (LoF [12]). By using MAP of a typical failure with T samples $(p_1, \ldots, p_T)$, our failure type estimation algorithm calculates the score of p by the LoF,

$$\mathrm{score}_p = \mathrm{LoF}(p_1, \ldots, p_T, p). \tag{11}$$

If that score is under the criterion value ρ set before starting the inference algorithm, we determine the failure is rare and our inference algorithm start modification. If not, we determine the failure is typical and stop inference.

C. Extended Inference Algorithm

Our extended inference algorithm calculates the MAP iteratively by solving Eq. (9) using the constructed set of f and g to obtain the MAP $\tilde{p}$. In other words, our algorithm tries every pattern of modification of the extended causal model.

We summarize our proposed method in Algorithm 1. The basic policy of our method is to be $\tilde{p}, \tilde{X}$ as a solution to the problem of finding the failed equipment using f and g. If the $\tilde{p}$ is larger than $\tilde{p}_{max}$, our algorithm is set $\tilde{p}$ as a new $\tilde{p}_{max}$. Our algorithm executes these steps iteratively. However, if f and g change the causal relation or observation status significantly, the output reliability of our method will decrease since this means that our inference algorithm ignores causal relations which is set in advance based on topology and observation data. In other words, if f and g change the causal relation or observation status significantly, we need $\tilde{p}$ to greatly increase compared with p. Therefore we set a criterion value τ and accept the solution of Equations (9) and (10) only when $\tilde{p}$ satisfies the following inequation.

$$\frac{\tilde{p}}{p} > \tau \times \left(\mathrm{GED}\left(f\right) + \mathrm{HD}\left(g\right)\right). \tag{12}$$

Finally, we show $\tilde{p}_{max}$ and corresponding $\tilde{X}$ to operators.

D. Scalability

Since our inference algorithm modifies causal relations and observation data, the number of times of solving Eq. (10), is $\#M$. Our causal model can treat any unexpected causal relation. However in this paper, it is assumed that at most one unexpected causal relation occurs between restricted nodes in our model. The way of the restriction describes below: Given failed equipment nodes by Shrink, we pick equipment nodes and observation-data nodes within three-hop distance in our extended model. Then, a causal-relation modification map adds or deletes edges only between the above nodes. Also, it is assumed that one observation error occurs in an observation-data node which is restricted above. With this restriction, the number of modification maps, f and g is decreased because in the typical communication network the causal model is sparse and the number of nodes within three-hop distance is much smaller than nm. On the other hand, even a few unexpected causal relations make finding failed equipment much more difficult for operators and previous methods.

No modifications need any information of the other modifications, so we can completely parallelize each modification without any specific technique. In Algorithm 1, we parallelize our algorithm in lines:8–13.

IV. Experiments

In this section, we discuss our numerical experiments on the proposed method and Shrink [4]. In these experiments, equipment nodes represent the status of network equipment. Observation-data nodes represent the link status. The method of constructing a causal relation is that if equipment i is connected to a link j in topology, it adds an edge between x_i and y_j the same as Shrink. We set $\alpha = 0.05$, $\beta = 0.2$, $\tau = 1.2$, and $\kappa = 6$. For metrics, we define precision and recall below. If failed equipment has a failure status in the output $\tilde{X}$, the methods succeed in finding failed equipment.

$$\mathrm{Recall} = \frac{\#\left(\text{Estimated as failure status in failed equipment}\right)}{\#\left(\text{All pieces of correct failed equipment}\right)}. \tag{13}$$

Precision is defined as the ratio of the number of correct status estimations to all status estimations.

$$\mathrm{Precision} = \frac{\#\left(\text{Correct status estimation of equipment}\right)}{\#\left(\text{All status estimation of equipment}\right)}. \tag{14}$$

A. Data sets

The failure data of typical and rare failures we used, were artificial failures through simulations topology (Experiment I, III and IV) and an actual network failure (Experiment Ⅱ).

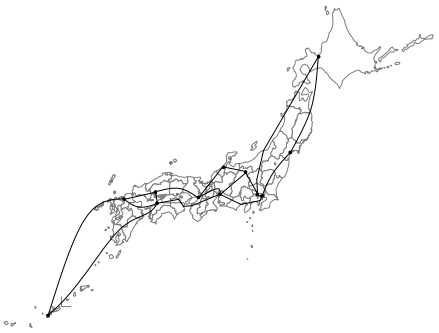

Fig. 5. Network topology of experiment I

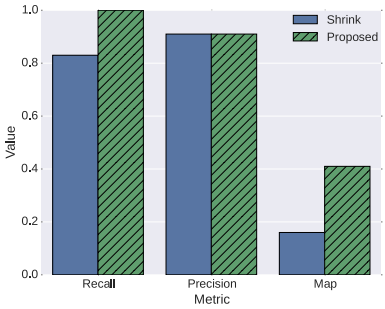

Fig. 6. Experiment I for rare failures

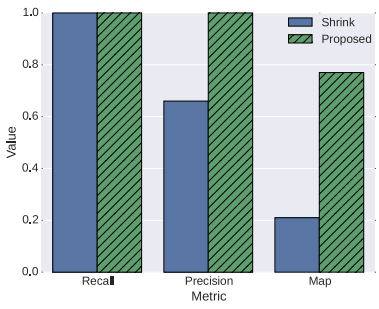

Fig. 7. Experiment I I for rare failures

Algorithm 1 Inference Algorithm

Require: $Y, M, \tau, \alpha, \beta$
Ensure: p, X
$\tilde{p}_{max} = 0$
$p = \max_X P(X|Y)$
$\text{score}_p = \text{LoF}(p)$
if $\text{score}_p > \rho$ **then**
  $X = \arg\max_X P(X|Y)$
  break.
end if
for all $(f, g) \in M$ **do**
  $\tilde{p} = \max_X P_f(X|g(Z))$
  if $\tilde{p} > \tilde{p}_{max}$ **then**
    $\tilde{p}_{max} = \tilde{p}$
    $\tilde{X} = \arg\max_X P_f(X|g(Z))$
  end if
end for
if $\frac{\tilde{p}_{max}}{p} > \tau \times (\text{GED}(f) + \text{HD}(g))$ **then**
  $p = \tilde{p}_{max}$
  $X = \tilde{X}$
else
  $X = \arg\max_X P(X|Y)$
end if

The simulation topology for Experiment I, III and IV illustrated in Fig. 5 is a photonic network model of Japan [13] that has 12 routers and 17 links. We created typical and rare failures at each piece of equipment. For typical failures, we assumed that if equipment i failed, the observation-data j connected to equipment i would be affected. We also set only one piece of equipment to fail. Since there are 12 equipment nodes in the topology, Experiment III includes data of 12 typical failures. For rare failures in Experiment I, III and IV, we assumed that when a piece of equipment failed, not only observation data connected to the failed equipment but also some observation data connected to the equipment next to the failed equipment would be affected. Similar to typical failures, they include data of 12 rare failures We created this rare failure on basis of the rare failure in Experiment Ⅱ.

The topology of the actual network failure for Experiment Ⅱ is shown in Fig. 2. This topology is a simple and small network, but it is a good example to determine whether both methods work for actual rare failures. The actual failed equipment node in this failure is x_2, and observation-data nodes are affected at not only y_1, y_2, which we can expect, but also y_3, which we can not expect. The reason that y_3 was affected is a compound event. When the equipment 2 failed, the specific packets arriving at equipment 3 generated link alerts for not only link 1 and link 2, but also link 3. This is rare failure occurred in equipment 2 but the observation data unconnected to equipment 2 were also were affected. This made it difficult for operators.

B. Experiment I : Simulation data

The results for both methods are shown in Fig. 6. Since rare failures have unexpected causal relations, an observation data status that is unconnected to a failed equipment node in the causal model is affected and turns to a failure status. Consequently, the recall of Shrink reduced to 0.83. Even if Shrink could find failed equipment, its MAP was 0.16, which means its results were less reliable for rare failures than for typical failures. The precision of the Shrink was 0.91.

The recall of our proposed method was 1.0, which means it can correctly estimate all failed equipment. Its average MAP was 0.41. From this result, we can see our proposed method handles rare failures features. The precision of our proposed method was 0.91, which is the same as that of Shrink.

C. Experiment Ⅱ : Actual rare failure data

We executed our method for an actual rare failure. We summarize the results for both methods in Fig. 7. The recall of Shrink is 1.0, so it found actual failed equipment, but it also estimated x_3 to be failed equipment. Thus, its precision decreased to 0.66. Its MAP was 0.21.

Our proposed method finds actual failed equipment and correctly estimated x_3 to be normal. Thus, its precision was 1.0, which was better than that of Shrink, and its recall was 1.0, which was the same as that of Shrink. Since its MAP was 0.77, which was larger than that of Shrink, we can trust the estimation of our proposed method more than that of Shrink.

D. Experiment III : Failure Type Estimation

Figure 8 illustrated MAPs of typical and rare failures. Since MAPs of both failure types are very different, we can estimate whether a failure is typical or rare. This is because in rare failures, there are affected observation data unconnected to failed equipment. This is a very simple simulation, but we

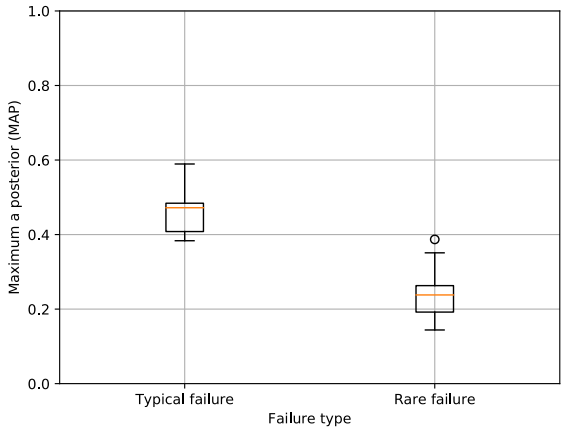

Fig. 8. Distribution of MAP for each failure type

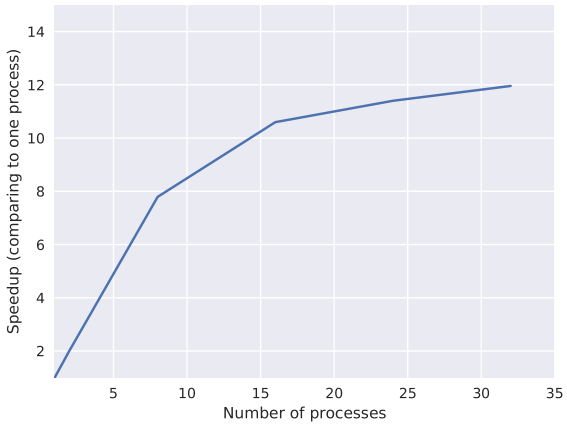

Fig. 9. Performance of parallelization

can see that it works for estimating failure type. Therefore, we can omit unnecessary modification processes and reduce computation time.

E. Experiment IV : Scalability

We parallelize our inference algorithm by Python and a multiprocessing module, and executed 10 times for rare failures with the same conditions as Experiment I. The central processing unit (CPU) we used was Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz, which has 6 cores and 12 threads. Since our inference algorithm modifies causal relations and observation data, it takes about 80 seconds with 1 process while Shrink takes about 2 seconds. Figure 9 shows the performance of parallelization. The number of processes was set to 1, 2, 4, 8, 16, 24 and 32. Since the CPU has 12 threads, the best performance is 12 times faster than computation time with 1 process. In Fig. 9, the performance linearly increase for 2, 4 and 8 processes , and is about 12 times faster for 24 and 32 processes. For more than 8 processes, parallelization effect decreases since the ratio of finding the correct f, g to the total computation time decreases and other parts became dominant in the total computation time.

V. Conclusion

We developed a root-cause diagnosis method consisting of an extended causal model and an extended inference algorithm that can find failed equipment. It is time-consuming for network operators to find rare-failure equipment because of two features of rare failures; unexpected causal relations and observation errors. Current methods can not find such failures, so we developed a method that modifies the causal relations observation data while executing our inference algorithm. As a result, our method can find both rare and typical failures and experiments show that our method finds actual rare-failure equipment.

In future work, we plan to evaluate our method with real rare failures and logs in a large scale network. Also, since modification maps are costly to infer, we will consider a more effective way to construct maps.

References

[1] Y. Matsuo, Y. Nakano, A. Watanabe, K. Watanabe, K. Ishibashi, and R. Kawahara, "ROOT CAUSE ANALYSIS FOR UNKNOWN FAILURES," *Proceedings of 2017 IEICE General Conference,B-7-35*, 2017(in Japanese).

[2] "HP intelligent management center https://www.hpe.com/jp/ja/networking/management.html," 2016.05.25.

[3] "IBM tivoli netcool/omnlbus http://www-03.ibm.com/software/products/ja/ibmtivolinetcoolomnibus," 2016.05.25.

[4] S. Kandula, D. Katabi, and J.-p. Vasseur, "Shrink: A tool for failure diagnosis in IP networks," *Proceedings of the 2005 ACM SIGCOMM workshop on Mining network data*, pp. 173–178, 2005. [Online]. Available: http://portal.acm.org/citation.cfm?id=1080178

[5] R. Kompella, J. Yates, A. Greenberg, and A. Snoeren, "IP Fault Localization via Risk Modeling," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 4, pp. 1–14, 2010.

[6] H. Yan, L. Breslau, Z. Ge, D. Massey, D. Pei, and J. Yates, "G-RCA: A Generic Root Cause Analysis Platform for Service Quality Management in Large IP Networks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 6, pp. 1734–1747, 2012.

[7] S. Kandula, R. Mahajan, P. Verkaik, S. Agarwal, J. Padhye, and P. Bahl, "Detailed diagnosis in enterprise networks," *Applications, Technologies, Architectures, and Protocols for Computer Communication*, vol. 39, no. 4, pp. 243–254, 2009. [Online]. Available: http://portal.acm.org/citation.cfm?id=1592597

[8] P. Bahl, R. Chandra, A. Greenberg, S. Kandula, D. a. Maltz, and M. Zhang, "Towards highly reliable enterprise network services via inference of multi-level dependencies," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, p. 13, 2007.

[9] R. N. Mysore, R. Mahajan, A. Vahdat, and G. Varghese, "Gestalt: Fast, Unified Fault Localization for Networked Systems," *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, pp. 255–267, 2014. [Online]. Available: https://www.usenix.org/conference/atc14/technical-sessions/presentation/mysore

[10] L. Bennacer, Y. Amirat, A. Chibani, A. Mellouk, and L. Ciavaglia, "Self-diagnosis technique for virtual private networks combining bayesian networks and case-based reasoning," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 1, pp. 354–366, 2015.

[11] X. Gao, B. Xiao, D. Tao, and X. Li, "A survey of graph edit distance," *Pattern Analysis and Applications*, vol. 13, no. 1, pp. 113–129, 2010.

[12] H. Victoria J. and A. d Jim, "A Survey of Outlier Detection Methodologies," *Artificial Intelligence Review*, vol. 22, pp. 85–126, 2004.

[13] S. Arakawa, T. Sakano, Y. Tsukishima, H. Hasegawa, T. Tsuritani, Y. Hirota, and H. Tode, "Topological Characteristic of Japan Photonic Network Model," *IEICE Technical Report*, pp. 7–12, 2013.