The 31st International Technical Conference on Circuits/Systems,
Computers and Communications (ITC-CSCC 2016)

Analysis of Cascading Failure Rate for Telecommunications Networks

Takuya Omura and Masahiro Hayashi
Major of Information Engineering of Graduate School, Tokyo City University
1-28-1 Tamazutsumi, Setagaya-ku, Tokyo 158-8557, Japan
E-mail: mhaya@tcu.ac.jp

Abstract: This paper proposes a new probabilistic measure of cascading failures of telecommunications networks. The key idea is that we use not availability, which is the conventional reliability measure, but the mean number of occurrences of serious cascading failures, where ‘serious’ means the impact of the cascading failure measured by the total traffic volume went below a specified value.

We performed some numerical experiments and found some interesting facts. For example, if we use the same routers with the same MTBF, then the cascading failure rate becomes smaller than if we use different routers with different MTBFs while the average of the MTBFs of the routers are the same for both cases.

Keywords-- **Cascading Failures, Telecommunications Networks, Reliability, Survival Traffic Rate**

1. Introduction

Cascading failures are failures that result in wide-area damage of telecommunications networks and are caused by successive failures of elements triggered by only a small failure of one element. In 2003, Italy experienced cascading failures caused by the interaction of Internet systems and electrical power supply networks going down [1]. In the USA in 2009 and 2012, Google’s web mail services experienced cascading failures that occurred in a single network [2][3]. Because Japan and other countries are anxious about experiencing cascading failures in the near future, many researchers have studied how to protect users from them. Almost all their approaches are based on quantitatively analyzing the impact caused by cascading failures so that it can be minimized by designing appropriate telecommunications networks. To analyze the impact, Hara et al. [4] proposed a measure called the survival traffic rate, which is defined as the percentage of the total traffic volume surviving after the occurrence of a cascading failure.

While this measure is very useful, it has the problem that it is deterministic and never considers the probability of a cascading failure occurring, even though this probability is necessary for designing telecommunications networks against such failures.

Now, we propose an improved measure, so we can probabilistically analyze cascading failures.

2. Preparation

First, we explain the mathematical, graph theoretic, and reliablility theoretic concepts and symbols used in this paper.

We used a graph consisting of nodes and links. The nodes are numbered 1, 2, …, n, and a link connects two nodes. If a link connects nodes i & j, i & j are called the end nodes of that link.

We use G to represent the graph. V is the set of all nodes in G, and E is the set of all links in G. That is $G = (V, E)$. An alternate sequence of nodes and links is called a path. If there is a path between two nodes, these nodes are connected. If any two nodes in G are connected, G is connected.

A non-negative real number is assigned to any link. This number is the length of the link. The sum of the lengths of all the links in a path is the length of this path. If the length of a path is the minimum of all paths between two specified nodes i & j, then this path is called the shortest path between i & j or more briefly the shortest path.

For any two sets X & Y, $X-Y = \{x| x\in X, x\notin Y\}$.

The MTBF (mean time between failures) is the mean time from the beginning of being repaired to the next failure. The MTTR (mean time to repair) is the mean time from the beginning of the failure to the failure being repaired. The availability is MTBF/(MTBF+MTTR) .

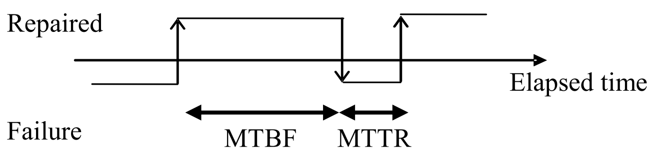

Figure 1. MTBF & MTTR.

3. Existing Research

3. 1 Model for telecommunications networks

A standard model for a telecommunications network [4] in the study of cascading failures is given as a graph satisfying the following condition.

A non-negative real number $D(i, j)$ (called a traffic demand) is assigned to any pair of nodes i & j, and the traffic volume corresponding to this assigned value is ensured between a node pair.

For this model, we define the initial state as follows.

Step 1. The shortest path $h^{i,j}$ is selected as the traffic path between any pair of nodes i & j to ensure the traffic demand between this pair of nodes.

Step 2. Let $H(k)$ be the set of all traffic paths going through node k. $f(k)$ is defined as below.

$$f(k) = \sum_{h^{i,j}\in H(k)} D(i, j)$$

($f(k)$ means the total traffic volume going through node k.)

Step 3. The node capacity c_k is assigned to each node k by $c_k = d \times f(k)$, where d is a non-negative constant value called the durability parameter.

A simple example of the initial state is shown in Figure 2.

In this initial state, we assume that $D(i, j) = 100$ for every pair of nodes and the duration parameter is 1.1. Therefore, $c_1 = c_2 = c_5 = 440$ and $c_3 = c_4 = 660$ for the initial state.

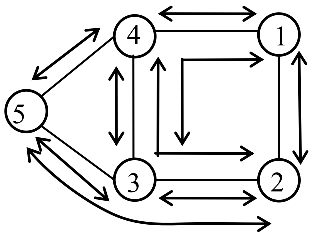

Figure 2. Initial state.

A cascading failure is caused in the initial state due to the steps described below [4].

Mechanism of cascading failure

Step 1. Let $Z = \{\phi\}$ and N be the initial state. A trigger failure is caused at one node of the initial state, and this node is put into Z.

Step 2. All traffic paths going through the nodes included in Z are deleted from N.

Step 3. All nodes in Z and all links connecting at least one node of Z are deleted from N.

Step 4. If we find a pair of nodes i & j still connected in N, but its traffic path is lost, then we search for new shortest paths beween i & j and select one of them as the new traffic path ensuring the value of $D(i, j)$.

Step 5. $f(k)$ is computed for any $k \in \{1, 2, \ldots, n\} - Z$.

Step 6. If we find $f(k) \leq c_k$ for any $k \in \{1, 2, \ldots, n\} - Z$, then the mechanism of cascading failure is terminated; otherwise all nodes satisfying $f(k) > c_k$ are put into Z.

Step 7. Go to Step 2.

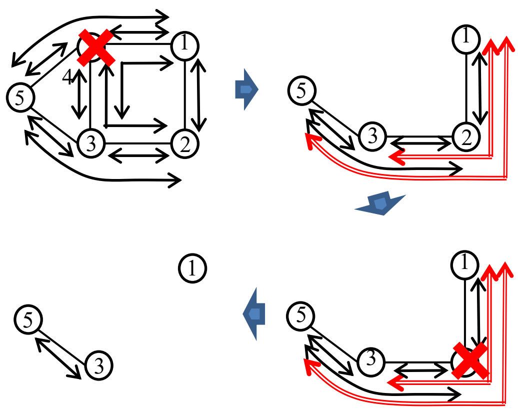
Figure 3. Example application of mechanism.

An example of an application of the above mechanism is shown in Figure 3.

A detailed explanation of the example application shown in Figure 3 is shown below.

Step 1. Let $Z = \{\phi\}$ and N be as in Figure 2. A trigger failure occurs at node 4; therefore $Z = \{4\}$.

Step 2. Six traffic paths go through node 4. Therefore, these six traffic paths are deleted fom N.

Step 3. Node 4 and all links connecting to node 4 are deleted from N.

Step 4. Node 1 & 3 and 1 & 5 are still connected, but their traffic paths are lost. Therefore, new shortest paths are assigned to these pairs of nodes (double-headed arrows in the upper right figure in Figure 3).

Step 5. $f(1) = f(5) = 300$, and $f(2) = f(3) = 500$.

Step 6. Node 2 is put into Z because $f(2) = 500 > c_2 = 440$. (lower right hand figure in Figure 3.)

Step 7. Go to Step 2.

Step 2'. Five traffic paths go through node 2. Therefore, these five traffic paths are deleted fom N.

Step 3'. Node 2 and all links connecting to node 2 are deleted from N.

Step 4'. We find the pair of nodes 3 & 5 that are still connected on N, and its traffic path is **not** lost.

Step 5'. $f(1) = 0$, and $f(3) = f(5) = 100$.

Step 6'. $f(1) = 0 \leq c_1 = 440$, $f(3) = 100 \leq c_3 = 660$, and $f(5) = 100 \leq c_5 = 440$. Therefore, this mechanism is terminated.

The lower left figure in Figure 3 is obtained by performing the above steps.

3. 2 Measure for impact of cascading failures

As a result of performing the mechanism of cascading failure, some pairs of nodes have traffic paths, and others do not. If we have a traffic path between node i & j, then it implies that traffic demand $D(i, j)$ is ensured between them; otherwise $D(i, j)$ is not ensured.

We define Pa_0 and Pa_1 as below.

$Pa_0 = \{(i, j) \mid$ pair of nodes in the initial state.$\}$

$Pa_1 = \{(i, j) \mid$ pair of nodes with a traffic path between nodes i & j after executing mechanism of a cascading failure$\}$

Hara et al. defined the survival traffic rate as below [4].

$$\text{Survival traffic rate} = \frac{\sum_{(i,j)\in Pa_1} D(i,j)}{\sum_{(i,j)\in Pa_0} D(i,j)}$$

For the example application of the mechanism shown in Figure 3, $Pa_0 = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$ and $Pa_1 = \{(3, 5)\}$. Because we assume that $D(i, j) = 100$ for every pair of nodes, as described just before Figure 2, we obtain

$$\sum_{(i,j)\in Pa_1} D(i,j) = 100, \quad \sum_{(i,j)\in Pa_0} D(i,j) = 1000.$$

Accordingly, for Figure 3,

$$\text{Survival traffic rate} = \frac{\sum_{(i,j)\in Pa_1} D(i,j)}{\sum_{(i,j)\in Pa_0} D(i,j)} = \frac{100}{1000} = 0.1.$$

This implies that the total traffic volume is reduced to 10% by the cascading failure whose trigger failure is caused at node 4.

3. 3 Problem of existing research

While the survival traffic rate is a very useful measure for evaluating the effectiveness of the countermeasures for cascading failures, we claim that this measure still has a problem because it does not consider the probabilities of cascading failures occurring.

Even when the impact of cascading failures measured by survival traffic rate is very serious, we do not need to be anxious about such cascading failures if the probability of occurrence is very low. However, when the impact of cascading failures is not serious, we need to be anxious about it if the probability of occurrence is not low.

While researchers in the traditional reliability engineering field have emphasized that such a probabilistic approach is very important to design highly reliable telecommunications networks [6], all researchers studying cascading failures do not take into account such probablistic approaches [1][4].

4. Proposal

4.1 Cascading failure rate

Now, we propose an improved measure, so we can probabilistically analyze cascading failures. The definition of this measure denoted by $Cas(\alpha)$ is as below.

$$Cas(\alpha) = \frac{1}{M},$$

where M = the mean time from the start of service to the first experience of cascading failure whose survival traffic rate goes below a threshold value α.

A conceptual view of $Cas(\alpha)$ is shown in Figure 4.

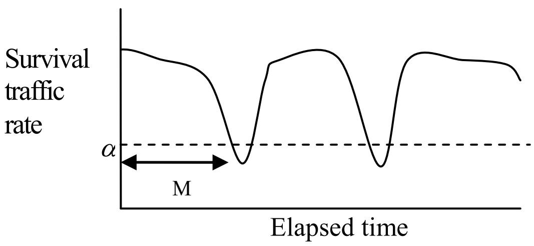

Figure 4. Conceptual view of cascading failure rate.

The key point of this measure is that we use not availability as defined in Section 2, which is the conventional reliability measure, but the mean number of occurrences of serious cascading failures, where 'serious' means the survival traffic rate went below α.occurrence is not low.

We call this improved measure the cascading failure rate. This measure is better than the availability-based one because the cascading failure rate can be estimated without repair time data (the availability-based one cannot do this because of the definition of availability given in Section 2). We emphasize that repair time data are very difficult to obtain in the case of cascading failures. Because cascading failures cause very serious situations, their repair times are different from commonly observed repair times.

We emphasize that we can only compute $Cas(\alpha)$ from the initial state information, mechanism of cascading failure, and additional information about the MTBF of each node.

4. 2 Computation method for cascading failure rate

Due to the definition of $Cas(\alpha)$, it is easy to see that the following steps compute the value of $Cas(\alpha)$.

Step 1. Let $Cas(\alpha) = 0$.
Step 2. Repeat the following substeps for each r (r = 1, 2, …, n)
  Substep 2-1. Start mechanism of cascading failure with trigger failure that occurs at node r.
  Substep 2-2. Compute the survival traffic rate.
  Substep 2-3. If the survival traffic rate < α, then
    $Cas(\alpha) = Cas(\alpha) + 1/\text{MTBF of node } r$
Step 3. Ouput $Cas(\alpha)$

For the case shown in Figure 2, the survival traffic rate = 0.6 when trigger failure occursat node 1, 2, or 5, and the survival traffic rate = 0.1 when trigger failure is caused at node 3 or 4.

Therefore, if α = 0.2 and the MTBF of each node is 100000 hours, then $Cas(\alpha)$ = 0.00001 + 0.00001 = 0.00002 (1/hours).

5. Numerical experiments

We implemented a software program to compute cascading failure rates of telecommunications networks and executed some numerical experiments.

5.1 Target models

The topology is shown in Figure 5 and has been provided by the Institure of Electoronics, Information and Communication Engineers[5]. The length of each link is determined by real map data of Japan.

For this topology, traffic demands are assigned as below.

If either i or j is 14, 16, 17, 18, 19, 23, 25, 26, 27, or 29, then $D(i, j)$ equals 10000; otherwise it equals 100.

The above assumption means that we have traffic concentrations for big cities.

Furthermore, we assume the following two patterns of MTBF of nodes (hours).

Pattern 1.

The same value of 4.57×10^6 is assigned for any node.

Pattern 2.

The values of 5.81×10^6, 4.57×10^6, and 3.81×10^6 are assigned to Areas *A, B,* and *C*, respectively, as shown in Figure 5.

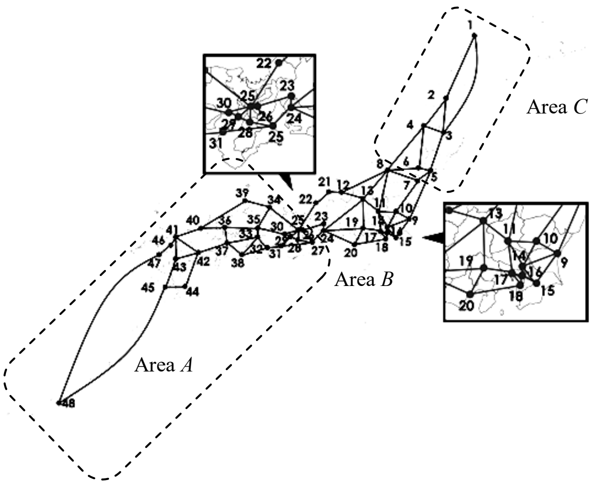

Figure 5. Topology.

We emphasize that the average of the MTBFs of the nodes is the same value in Pattern 1 & 2. These patterns mean that we use the same routers in all nodes or several different routers.

5.2 Analysis results

The analysis results for Pattern 1 are shown in Figure 6.

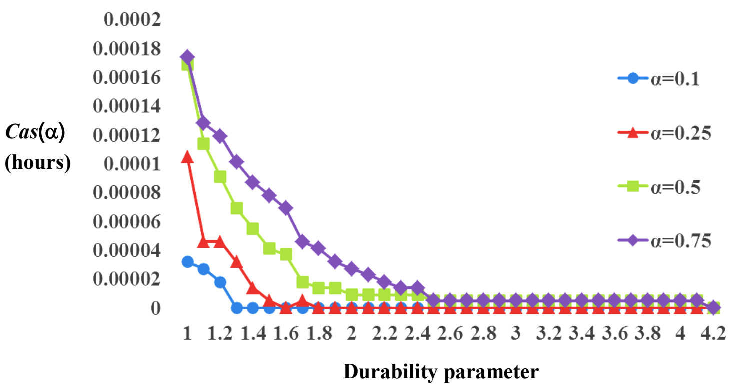

Figure 6. Analysis Results for Pattern 1.

The total computation time to obtain all data for Figure 6 is 4 minutes and 20 seconds.

Due to the analysis results for Pattern 1, if we increase the duration parameter from 1 to 1.3, the cascading failure rate ($\alpha = 0.1$) becomes almost zero. In this example, having only a small margin of capacity effectively prevents serious cascading failures. That is, by analyzing cascading failure rates, we can find effective countermeasures for cascading failures at low cost.

The analysis results for both Pattern 1 & 2 with a duration parameter of 2.0 are shown in Figure 7.

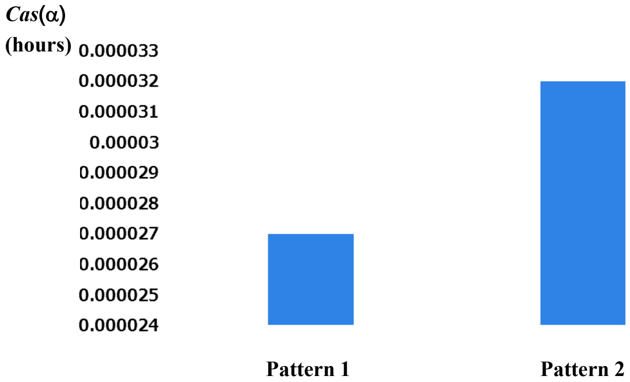

Figure 7. Analysis Results for Pattern 1 & 2.

The total computation time to obtain all data for Figure 7 is 12 seconds.

The results shown in Figure 7 indicate that the cascading failure rate becomes small if we have different values of the MTBFs of nodes even though the average of the MTBFs of nodes is the same. Therefore, we can determine that we should use different types of routers to reduce the number of occurrences of cascading failures.

6. Conclusion

This paper proposes a new measure of cascading failures of telecommunications networks. Previous measures do not consider the probabilities of occurrences of cascading failures. However, our measure considers such probabilities. The key idea is that we do not use the conventional availability-based measure because this needs repair time data, which is very difficult to obtain in the case of cascading failure.

For future work, we need to analyze the effects of actual countermeasures for cascading failures from the viewpoint of cascading failure rates and further improve the measure of cascading failure.

References

[1] S. V. Buldyrev, et al., "Catastrophic Cascade of Failures in Interdependent Networks", Nature, Vol. 464, pp. 1025–1028, 2010.

[2] http://itpro.nikkeibp.co.jp/article/NEWS/20090903/336439/ (in Japanese)

[3] http://static.googleusercontent.com/media/www.google.com/ja//appsstatus/ir/plibxfjh8whr44h.pdf

[4] Hara et al., "A Study of Evaluating the Impacts of Cascading Failures in Telecommunications Networks", APNOMS2013, 13-4, 2013.

[5] http://www.ieice.or/~pn/jp/jpnm.html

[6] W. G. Schneeweiss, *Boolean Functions with Engineering Applications and Computer Programs,* Springer–Verlag, 1989.