Modeling and Quantifying the Survivability of Telecommunication Network Systems under Fault Propagation

Lang Xie, Poul Heegaard, Yuming Jiang

Modeling and Quantifying the Survivability of Telecommunication Network Systems under Fault Propagation

Lang Xie, Poul E. Heegaard, and Yuming Jiang

Department of Telematics,
Norwegian University of Science and Technology,
N-7491 Trondheim, Norway
{langxie,Poul.Heegaard,jiang}@item.ntnu.no

Abstract. This paper presents a generic state transition model to quantify the survivability attributes of a telecommunication network under fault propagation. This model provides a framework to characterize the network performance during the transient period that starts after the fault occurrence, in the subsequent fault propagation, and until the network fully recovers. Two distinct models are presented for physical fault and transient fault, respectively. Based on the models, the survivability quantification analysis is carried out for the system's transient behavior leading to measures like transient connectivity. Numerical results indicate that the proposed modeling and analysis approaches perform well in both cases. The results not only are helpful in estimating quantitatively the survivability of a network (design) but also provide insights on choosing among different survivable strategies.

Keywords: survivability, analytical models, fault propagation

1 Introduction

Telecommunication networks are used in diverse critical aspects of our society, including commerce, banking and life critical services. The physical infrastructures of communication systems are vulnerable to multiple correlated failures, caused by natural disasters, misconfigurations, software upgrades, latent failures, and intentional attacks. These events may cause degradations of telecommunication services for a long period. Understanding the functionality of a network in the event of disasters is provided by survivability analysis. Here, qualitative evaluation of network survivability may no longer be acceptable. Instead, we need to quantify survivability so that a network system is able to meet contracted levels of survivability.

1.1 Fault propagation

An undesired event is an event which impacts system normal operation. It triggers faults, which cause an error. When the error becomes visible outside the system boders, we have a failure, i.e., the system does not behave as specified. An excellent explanation of fault, error, failure pathology is given in [12]. The types of such events include operational mistakes, malicious attacks, and large-scale disasters.

When multiple network elements (e.g. nodes or links) go down simultaneously due to a common event, we have multiple correlated failures. Different from single random link or node failure, multiple failures are often caused by natural disasters such as hurricane, earthquake, tsunami, etc., or human-made disasters such as electromagnetic pulse (EMP) attacks and weapons of mass destruction (WMD) [8]. Correlated failures can be cascading where the initial failures are followed by other failures caused by some propagating events. Therein, a network system may be vulnerable to a time sequence of single destructive faults. It starts by an initial event on a part of network and spreads to another part of the network. The propagation continues in a cascade-like manner to other parts. This phenomena is denoted as fault propagation. As few examples: the power outages and floods caused by 2005 US hurricane Katrina resulted in approximately 8% of all customarily routed networks in Louisiana outaged [9]; in the March 2011 earthquake and tsunami in east Japan, almost 6720 wireless base stations experienced long power outage [10]. Also, some studies warn that risk of WMD attacks on telecommunication networks is rising [8].

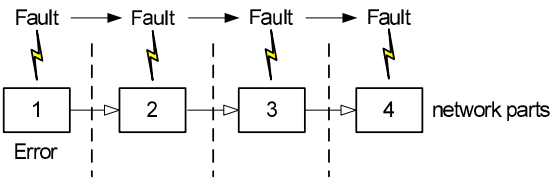


Fig. 1. Comparison of fault propagation and error propagation

Different from error propagation, fault propagation does not necessarily occur among interconnected network equipments. Since a fault may be an external event, it can occur in isolated parts of a network. The difference between fault propagation and error propagation is illustrated in Fig. 1. With the aim of developing a more realistic survivability model, fault propagating phenomena must be taken into account.

1.2 Related work

Survivability is defined as the system's ability to continuously deliver services in compliance with the given requirements in the presence of failures and other undesired events [3]. Most of the literature on network survivability quantificaiton

has been done on combating single-link or node failures [1],[2],[4]. Only a few studies have considered multiple failures. A state transition model for base station exposed to channel failures and disastrous failures was proposed in [11]. Nevertheless, this model only considers one base station without multiple or correlated base station failures. Our previous work [5] uses a continuous-time Markov chain (CTMC) to model and analyze the survivability of an infrastructure-based wireless network in the presence of disastrous failures and repairs. However, it considers only a single disaster scenario where failures are not correlated.

Very few studies have considered the quantification of network survivability against correlated failures caused by some propagating events. Therefore, there exists a critical need for appropriate quantitative, model-based evaluation techniques to address this limitation. In our previous work [6], we propose an approximative survivability model to take a disaster propagation scenario into account. To the best of our knowledge, this is the first work to quantify the survivability and the failure and repair rate tradeoffs of networks. However, such model does not distinguish the state of system before and after repair. We further relax these approximations and develop a more realistic mode in [7]. However, only a particular case of a three-subnetwork system is considered in this work.

In this paper we generalize our previous work in [7]. The resulting model turns out to be a general model that considers the fault propagation among n ($n > 0$) subnetworks. Specifically, transient failures are integrated into the proposed model. The analysis results are helpful in estimating quantitatively the survivability, in terms of certain chosen performance metrics of a network (design). Further, they provide insights on specifying the values of repair rates required to achieve a contracted service performance and availability. Our goals are providing some critical inputs for network design and operation. For example, in network deployment in coastal areas, which are vulnerable to specific disaster types like flooding as well as hurricanes, the knowledge of network survivability is useful.

The rest of the paper is organized as follows. In Section 2, we develop Markov models for a system from the survivability quantificaiton view point. Section 3 analyzes the models that may be used to find the transient probabilities leading to the computation of transient survivability measures. Numerical results of the analysis performed on the models are presented in Section 4. Finally, Section 5 gives the conclusions along with some future directions in this area.

2 Markov Model for Survivability Quantification

A network system that is survivable consists of network design and management procedures to mitigate the effects of failures on the network services. To analyze and quantify the survivability attributes of such a network system, we have to take into account the propagating behavior of a fault as well as the network system's response to the fault propagation. Therefore, we would require a composite survivability model that incorporates the behavior of both these elements.

2.1 Network View

The network can be viewed as a directed graph consisting of nodes and directed edges. A node can be a single network equipment or a subnetwork. The directed edges denote the directions of possible disaster propagation among various nodes. We suppose the number of subnetworks in the networked system is n ($n > 0$). Furthermore, we assume a disastrous event initially occurred on one subnetwork and then propagated from the affected subnetwork to another within a random time period. The process continues until no more subnetwork failures occur. Here, we mainly consider the multiple failures caused by some events such as natural disasters, intentional attacks, etc, which are among the main reasons that trigger fault propagation.

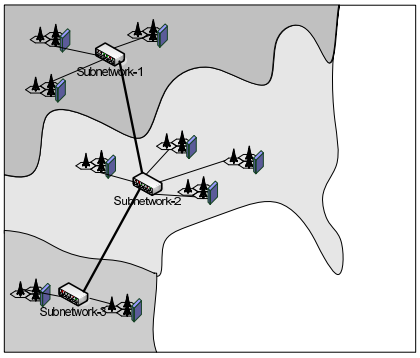


Fig. 2. Network example with three subnetworks

To illustrate the above view, we use a wireless network example. As depicted in Fig. 2, it consists of n (e.g. $n = 3$) subnetworks. The view shows the actual geographic layout of the network elements, such as cell site, radio network controller (RNC), mobile switching center (MSC) and so on. Assume a disastrous event occurs in subnetwork-1 at the beginning. Then the disastrous event propagates its effect to subnetwork-2, subnetwork-3 in successive steps. For the sake of illustration, the number of network elements in the figure does not necessarily equal to the real number. Our objective is to investigate the network performance during the transient period that starts after the disaster occurrence, in the subsequent disaster propagation and until the network fully recovers. For this, we define the (i) *undesired events* to be disastrous events, (ii) *service* to be the connections between access points and subscribers, (iii) *service requirement* to be a minimum number of access points that need to be operational for the service. It is remarked that our focus is "connectivity" and our focus is not about how to obtain the performance metric at a real network or network component. Thus we do not consider the dynamics brought by routing and traffic flows further in this paper.

We need a methodology to capture the transient variation of performance under fault propagation, as well as tractable. In what follows, we introduce a phased recovery model to quantify the survivability of network under fault propagation caused by disaster. The model is constructed stepwise, starting with only permanent hardware failures and gradually extending it to include software and transient hardware failures. The discussion here is not limited into a wireless network. We believe the methods and analysis presented can be applied to other telecommunication networks such as a public switched telephone network (PSTN), a data network, or an optical network.

2.2 Model I: Permanent hardware failures

The first model only considers failures that require manual repair, i.e., permanent hardware failures caused by the disasters (e.g. hurricanes, tornados, floods, earthquakes, and tsunamis) and environment (e.g. power outages).

A fault always tries to bring a network system into a failure state. This requires the fault to spend time and effort. In general, this time or effort is best modeled as a random variable. Once a fault is detected, the system needs to initiate appropriate recovery actions. The basic nature of this response would be to try to make the system move back to a normal state from a failure state. This movement requires time or effort on the system. As before, this time or effort is best modeled as a random variable that is described by a suitable probability distribution function. The system's response to a fault may be described by the states and transitions between these states. In order to analyze the survivability attributes of a network system, we need to consider the actions undertaken by a fault as well as the system's response to a fault. The transient period of our interest is assumed to evolve as a continuous-time stochastic process $\{X(\tau) : \tau \geq 0\}$. The state X of the n-subnetworks at any time τ can be completely described by the collection of the state of each subnetwork. That is, a n-dimensional vector

$$X(\tau) = (X_1(\tau), X_2(\tau), \cdots, X_n(\tau)), \qquad \tau \geq 0, \tag{1}$$

where for each subnetwork $X_l(\tau) = p$ (l is discrete; $l = 1, \cdots, n$) represents the state that a permanent hardware failure has occurred on the l-th subnetwork at time τ, $X_l(\tau) = o$ in the case when the l-th subnetwork works normally at time τ, and $X_l(\tau) = r$ if the l-th subnetwork has been repaired at time τ. Here, it is assumed that the service in state r restores to the same value as in normal state o.

The propagation is assumed to have 'memoryless' property: the probability of disastrous events spreading from one given subnetwork to another depends only on the current system state but not on the history of the system. The affected subnetwork can be repaired in a random period. Moreover, all the times of the disaster propagation and repair are exponentially distributed.

With the above assumptions, the transient process $X(\tau)$ can be mathematically modeled as a continuous-time Markov chain (CTMC) with state space $\Omega = \{(X_1, X_2, \cdots, X_n) : X_1, X_2, \cdots, X_n \in \{p, o, r\}\}$. The transition rate matrix of $X(\tau)$ is $\mathbf{Q}$.

In brief, the following summarizes the model:

- the state of each subnetwork at time t lies within the set $\{p, o, r\}$,
- at the initial time $t = 0$, a disastrous event hits the 1-st subnetwork, which changes the system state to $(p, o, \cdots, o)$,
- the disaster propagates from the subnetwork l (l is discrete; $l = 1, \cdots, n$) to subnetwork $l + 1$ according to Poisson processes with rate $\lambda_{p(l+1)}$,
- a disastrous event can occur on only one subnetwork at a time,
- each subnetwork has a specific repair process which is *all at once* and the repair time of subnetwork l is exponentially distributed with mean $1/\mu_{pl}$,
- subnetworks with permanent failure are not repaired before all subnetworks are affected by the disaster,
- the propagation or repair transition is determined only by the current state, not on the path until reaching the current state.

Table 1. Transition generation rules for **Q**

Condition	Q_{ab}	a→b
Propagation phases:		
$'r' \notin a \&\& 'r' \notin b, a[0] = b[0] =' p'$	λ_{p2}	$(p, o, \cdots, o) \rightarrow (p, p, o, \cdots, o)$
	$\vdots$	$\vdots$
	λ_{pn}	$(p, \cdots, p, o) \rightarrow (p, \cdots, p)$
Repair phases:		
$f(b) = f(a) + 1$, $a[i] = b[j] =' r'$, $i, j \in 1 \cdots n, j \neq i$	μ_{pj}	
*Note: 1. f is the function to return the number of 'r' in the state; 2. state $(r, \cdots, r) = (o, \cdots, o)$.		

Our previous work [7] has provided a 3-subnetwork example in Section 2.1. Here we make a further step in constructing a general model for a network with n subnetworks. We consider the transition from one certain state a to b with rate Q_{ab}, where the state is represented as a vector as the form in Eq. (1). To distinguish the states in repair phases, we use a function f to counter the number of $'r'$ in the state. Table. 1 summarises the rules in constructing the infinitesimal generation matrix of model I for a network with a general number of subnetworks n ($n > 0$; n is discrete).

2.3 Model II: Transient failures

Transient failure is a brief malfunction that often occurs at irregular and unpredictable times, which has in most systems a significant impact on the reliability

and survivability. Some examples of transient failures are electromagnetic interference and radiation, noise on a transmission line and alpha-particles passing through RAM flipping bits. The restoration after a transient failure does not require manual maintenance and repair, it is often the case that the automatic reboot fix the problem. As an important type of failure, transient failure is largely overlooked in network survivability modeling. In the following, we will integrate the impact of transient failures into the system model.

It is necessary to distinguish between permanent and transient failures. We add a new value to the state space, that is, $X_l(t) = t$ represents the state that a transient failure has occurred on the l-th subnetwork at time τ. The following summarizes the increased model assumptions:

- the state of each subnetwork at time τ lies within the set $\{p, t, o, r\}$,
- the disaster propagates from the subnetwork l (l is discrete; $l = 1, \cdots, n$) to subnetwork $l + 1$ according to Poisson processes with rate $\lambda_{p(l+1)}$,
- transient failures occur according to a Poisson process of intensity λ_t,
- the restoration of a transient failure does not require manual repair, it is assumed that the automatic reboot (with mean rate μ_t) fix the problem, which implies a shorter repair/restoration time, i.e., $\mu_t > \mu_p$,
- each subnetwork has a specific repair process which is *all at once* and the repair time of subnetwork l is exponentially distributed with mean $1/\mu_{pl}$,
- a subnetwork with a permanent failure cannot fail due to transient failures,
- a subnetwork with a transient failure can fail due to a permanent failure,
- when a subnetwork is repaired both permanent and transient failures are removed.

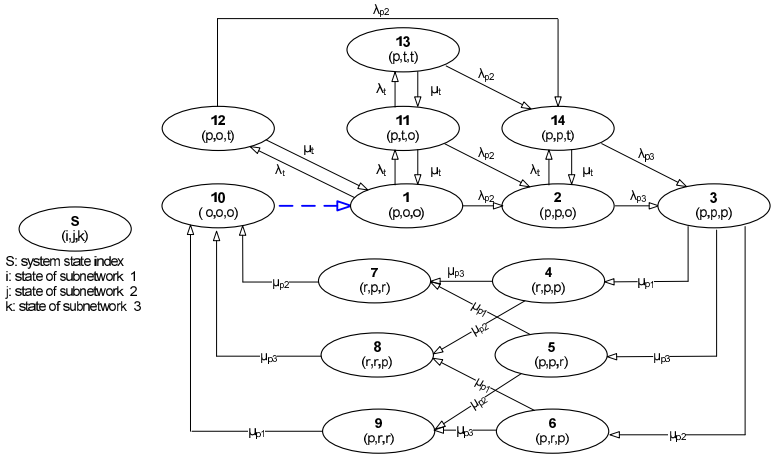


Fig. 3. A state transition diagram for model II

For the sake of illustration, we use the wireless network example in Section 2.1. The state transition model considering transient failures is presented in Fig.

3. This diagram is an extension of the model I example which has been presented in [7]. Given the initial state is (p, o, o), the CTMC may jump to state (p, p, o) if the propagation occurs with rate λ_{p2}; or it may jump to state (p, t, o) or (p, o, t) with rate λ_t due to transient failures. Time to restart to fix the transient failures is assumed to be exponentially distributed with rate μ_t. Similarily, on state (p, p, o), the CTMC may jump to state (p, p, p) if the propagation continues with rate λ_{p3}; or it may jump to state (p, p, t) with rate λ_t for transient failures. As for the other transition structures, model II is the same with model I.

On state (p, p, p), the CTMC may jump to three possible states: firstly, it may jump to state (p, p, r) if the subnetwork-3 is recovered (this occurs with rate μ_{p3}); secondly, it may jump to state (r, p, p) if the subnetwork-1 is recovered (this occurs with rate μ_{p1}); and thirdly, the CTMC may jump to state (p, r, p) if the subnetwork-2 is recovered (this occurs with rate μ_{p2}).

It should be observed that the frequency of the initial event is not considered in the survivability model because the focus is: given that an undesired event has occurred what is the nature of performance degradation just after such event until the system stabilizes again. This is indicated by the dashed line in Fig. 3.

Section 3 will discuss the use of the Markov model and transient probabilities to arrive at the transient suvivability model analysis.

3 Model Analysis

In this section we discuss and derive survivability attributes based on the Markov models presented in the previous section. It was explained earlier that to carry out the survivability quantification analysis, we need to analyze the Markov model of the system that was described by its state transition diagram. In order to compute survivability measure, we need to first compute the transient probabilities of the model states.

Let $\pi(\tau) = [\pi_{(p,o,\cdots,o)}(\tau) \cdots \pi_{(o,o,\cdots,o)}(\tau)]$ denote a row vector of transient state probabilities at time τ. In order to calculate $\pi(\tau)$, the Kolmogorov-forward equation expressed in the matrix form should be satisfied as follows:

$$\frac{d\pi(\tau)}{d\tau} = \pi(\tau)\mathbf{Q}, \tag{2}$$

where $\mathbf{Q}$ is the transition rate matrix. Then the transient state probability vector can be obtained as follows:

$$\pi(\tau) = \pi(0)e^{\mathbf{Q}\tau}, \tag{3}$$

where $e^{\mathbf{Q}\tau}$ is defined as follows:

$$e^{\mathbf{Q}\tau} = \sum_{i=0}^{\infty} \mathbf{Q}^i \frac{\tau^i}{i!}. \tag{4}$$

The simplest method to compute Eq. (4) is to truncate the summation to a large number (e.g., K), which can be expressed as follows:

$$e^{\mathbf{Q}\tau} = \sum_{i=0}^{K} \mathbf{Q}^i \frac{\tau^i}{i!}. \tag{5}$$

The other common alternative methods to obtain the transient probability vector $\pi(\tau)$ include uniformization [13], matrix exponential approach [14]. Here we take uniformization approach as the model analysis example. Let q_{ii} be the diagnoal element of $\mathbf{Q}$ and $\mathbf{I}$ be the unit matrix, then the transient state probability vector is obtained as follows:

$$\pi(\tau) = \pi(0) \sum_{i=0}^{\infty} e^{-\beta\tau} \frac{(\beta\tau)^i}{i!} \mathbf{P}^i, \tag{6}$$

where $\beta \geq max_i|q_{ii}|$ is the uniform rate parameter and $\mathbf{P} = \mathbf{I} + \mathbf{Q}/\beta$. Truncate the summation to a large number (e.g., K), the controllable error ϵ can be computed from

$$\epsilon = 1 - e^{-\beta\tau} \sum_{i=0}^{K} \frac{(\beta\tau)^i}{i!}. \tag{7}$$

Whenever the system is in state $i \in \Omega$, a reward is assigned at a rate $\Upsilon(i)$, where Υ denotes a reward function. Since Υ_i is the reward rate associated with state i, and so Υ_i can take any of the $|\Omega|$ values. The vector of reward rates associated with the state is expressed as $\mathbf{\Upsilon} = [\Upsilon_1, \Upsilon_2, ..., \Upsilon_{|\Omega|}]$. Here, the reward rate can be many types, such as economic return vector or cost vector in business continuity preparedness planning.

We currently equate survivability performance with connectivity, *the percentage of users connected successfully*. Based on the above calculated transient probabilities, the measure of interest is obtained as reward measures from the CTMC model. Then, the expected instantaneous reward rate $E[\Upsilon_{X(\tau)}]$ gives the average connectivity of the system at time t, which is expressed as follows:

$$E[\Upsilon_{X(\tau)}] = \mathbf{\Upsilon} \cdot \pi^T(\tau). \tag{8}$$

As stated in Section 2 complete description of this Markov model requires the knowledge of various model parameters. Clearly for the model to be accurate, it is important to estimate the model parameters accurately. In this paper, our focus is more on developing a methodology for analyzing quantitatively the survivability attributes of a network rather than model parameterization.

4 Numerical Example

In this section, we perform numerical experiments for the case study in Section 2.1. First, we apply and compare model I and model II in this network example for different values of fault propagation rates. Then we study the impact of differents repair rates on model II's performance.

For the parameters setting of the proposed models, we refer to the data from Japan 2011 earthquake situation report [10]. In doing so, our model parameters fall in ranges which represent the typical real system's behavior. Our experimental setup consists of three subnetworks and the disaster occurs at subnetwork-1 initially. We set the transition rates as follows: $\lambda_{p2} = \lambda_{p3} = 0.67$, $\lambda_t = 50$,

$\mu_t = 100$, $\mu_{p1} = \mu_{p2} = \mu_{p3} = 0.097$, given in units of events per day. For simplicity, the average number of users per each base station is assumed to be the same. Then the percentage of connected users is equal to the fraction of available base stations. The rewards at each model state are shown in Table 2.

Table 2. Rewards: fraction of available base stations

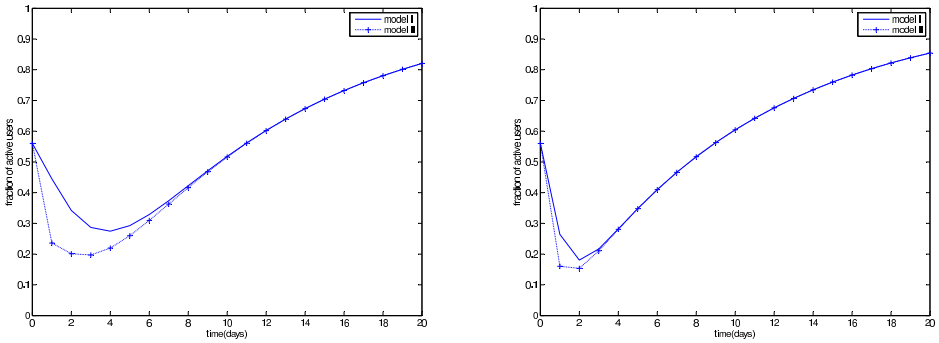
Parameter	Value	Parameter	Value
Υ_1	0.560	Υ_8	0.871
Υ_2	0.429	Υ_9	0.611
Υ_3	0.040	Υ_{10}	1.000
Υ_4	0.429	Υ_{11}	0.430
Υ_5	0.483	Υ_{12}	0.130
Υ_6	0.169	Υ_{13}	0.040
Υ_7	0.560	Υ_{14}	0.040

First, we compare model I and model II in this network example for different values of fault propagation rates. In fig. 4, when $\lambda_{p2} = \lambda_{p3} = 0.67$, there is a gap between model I and model II curves. Compared to model I, the fraction of active users in model II decreases more sharply. On the other hand, as expected, when fault propagation rates increase, i.e., $\lambda_{p2} = \lambda_{p3} = 1.8$, then model I and model II curves are close to each other. The impact of transient failure and repair is not as evident as in former case.

Then we study the impact of different repair rates on model II's performance. We vary the transient and permanent failure repair rate values, and the results are summarized in Fig. 5. Consider the scenario in which the permanent failure repair rate is low ($\mu_{p1} = \mu_{p2} = \mu_{p3} = 0.3$). In this scenario, the fraction of active users is low (roughly 0.3, 2 hours after the failure when $\mu_t = 10$). However, when the permanent failure repair rates are relatively higher ($\mu_{p1} = \mu_{p2} = \mu_{p3} = 3$), the fraction of active users sharply increases. In both figures, the effect of the transient failure repair rate is not as evident for longer observation time (after 8 hours). As shown in 5(b), the value of transient failure repair rate μ_t which makes the fraction of active users achieve 60% in two days is $\mu_t > 100$.

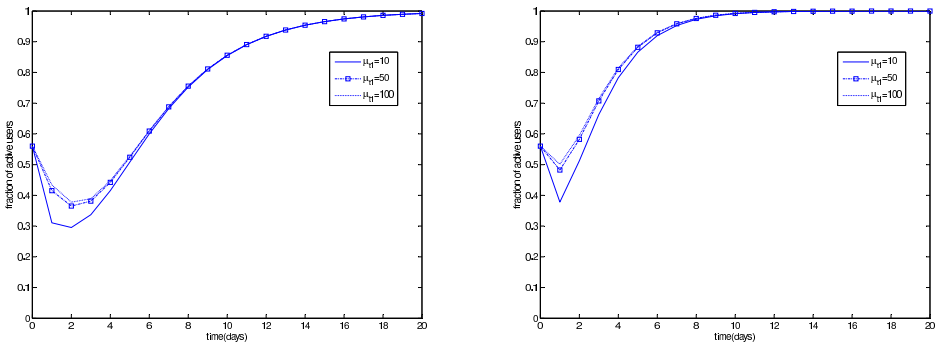
5 Conclusions and Future Work

In this paper we have presented an approach for quantitative assessment of network survivability against fault propagation. First, we considered the case where physical fault propagation is considered. Second, we considered the case in which both physical and transient fault are incorporated. The impact of different parameters, such as fault propagation rates, repair rates were studied. Users can choose different models depending on the real cases. For example, if both physical and transient faults occurred, model II is more appropriate; otherwise, model I



(a) $\lambda_{p2} = \lambda_{p3} = 0.67$ (b) $\lambda_{p2} = \lambda_{p3} = 1.8$

Fig. 4. Comparison of the fraction of connected users in model I and II for different values of fault propagation rates



(a) $\mu_{p1} = \mu_{p2} = \mu_{p3} = 0.3$ (b) $\mu_{p1} = \mu_{p2} = \mu_{p3} = 3$

Fig. 5. Impact of repair rates on the fraction of connected users in model II

is enough for the requirement. The main goal of this paper is to construct the models, rather than model parameterization.

One of the goals of our future work is to collect more real data. This information should provide us with a better understanding of the behavior exhibited by faults, help us to refine its stochastic description and lead to better estimates of the model parameters. Another goal of our future work is to consider geographic factors. We will extend the system state by adding more dimensions representing geographical characterizations.

References

1. Zolfaghari, A., Kaudel, F.J.: Framework for network survivability performance. Selected Areas in Communications, IEEE Journal on. 5, 46–51 (1994)
2. Yun, L., Mendiratta, V.B., Kishor, S.T.: Survivability analysis of telephone access network. In: IEEE 15th International Symposium on Software Reliability Engineering, pp. 367–377. IEEE Press, Bretagne (2004)
3. Heegaard, P.E., Kishor, S.T.: Network survivability modeling. Comput. Netw. 53, 1215–1234 (2009)
4. Fei, X., Wenye, W.: On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures. Dependable and Secure Computing, IEEE Transactions on. 7, 284–299 (2010)
5. Lang, X., Heegaard, P.E., Yuming, J.: Modeling and Analysis of the Survivability of an Infrastructure-Based Wireless Network. In: 18th EUNICE Conference on Information and Communications Technologies, pp. 227–238 (2012)
6. Lang, X., Heegaard, P.E., Yuming, J.: Network Survivability under Disaster Propagation: Modeling and Analysis. In: IEEE Wireless Communications and Networking Conference 2013. (2013)
7. Lang, X., Yuming, J., Heegaard, P.E.: Modelling and Analysis of the Survivability of Telecommunication Network. In: International Symposium on Performance Evaluation of Computer and Telecommunication Systems 2013. (2013)
8. Reuters: Experts Warn of Substantial Risk of WMD Attack, http://research.lifeboat.com/lugar.htm.
9. Kwasinski, A., Weaver, W.W., Chapman, P.L., Krein, P.T.: Telecommunications power plant damage assessment for Hurricane Katrina - site survey and follow-up results. IEEE Systems Journal 3 on. 3, 277–287 (2009)
10. Adachi, T., Ishiyama, Y., Asakura, Y., Nakamura, K.: The restoration of telecom power damages by the Great East Japan Earthquake. In: Proc. IEEE Telecomm. Energy Con. (INTELEC), Amsterdam, Netherlands (2011)
11. Jindal, V., Dharmaraja, S., Kishor, S.T.: Analytical survivability model for fault tolerant cellular networks supporting multiple services. In: IEEE International Symposium on Performance Evaluation of Computer and Telecommunication Systems, pp. 505–512. IEEE Press, Calgary (2006)
12. Avizienis, A., Laprie, J.C., Randell, B. and Landwehr, .C.: Basic concepts and taxonomy of dependable and secure computing. In: Dependable and Secure Computing, IEEE Transactions on . 1, pp. 11–33 (2004)
13. Jensen, A.: Markoff chains as an aid in the study of Markoff processes. In: Skand. Aktuarietiedskr on. 36, pp. 87–91. (1953)
14. Trivedi, K.S.: Probability and Statistics with Reliability, Queueing, and Computer Science Applications, 2nd Edition. (2001)