Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks [*]

Dongyan Chen
Center for Advanced Computing and Communications (CACC)
Electrical and Computer Engineering Department, Duke University
Durham, NC 27708-0294
dc@ee.duke.edu

Sachin Garg
Avaya Labs Research
233 Mount Airy Rd., Basking Ridge, NJ 07920
sgarg@avaya.com

Kishor S. Trivedi[†]
Center for Advanced Computing and Communications (CACC)
Electrical and Computer Engineering Department, Duke University
Durham, NC 27708-0294
kst@ee.duke.edu

ABSTRACT

Network survivability reflects the ability of a network to continue to function during and after failures. Our purpose in this paper is to propose a quantitative approach to evaluate network survivability. We perceive the network survivability as a composite measure consisting of both network failure duration and failure impact on the network. A wireless ad-hoc networks is analyzed as an example, and the excess packet loss due to failures (ELF) is taken as the survivability performance measure. To obtain ELF, we adopt a two phase approach consisting of the steady-state availability analysis and system transient performance analysis. Assuming Markovian property for the system, this measure is obtained by solving a set of Markov models. By utilizing other analysis paradigms, our approach in this paper may also be applied to study the survivability performance of more complex systems.

Categories and Subject Descriptors

C.4 [**Performance of systems**]: Reliability, availability, and serviceability

General Terms

Performance, Reliability

Keywords

Survivability, wireless ad-hoc networks, Markov models, transient analysis, availability

1. INTRODUCTION

With the increase in complexity, scale, and speed of communication networks, network performance under failures or attacks has become a great concern in the telecommunication industry. An attack or failure may significantly reduce the capability of the communication network to efficiently deliver service to users. Some drastic effects of communication network failures have been demonstrated by several publicized network outages in recent years [19], and an increasing trend in the outage frequency was indicated in the survey by Network Reliability Steering Committee [1]. Thus the network needs to cope with failures to preserve the network service integrity under failures or attacks [4]. For this reason, objectives for network reliability are set forth for telephone networks, and quantitative metrics are standardized [21] and have been studied in several papers [12] [15].

Along with this trend, network survivability is recently drawing ever-increasing attention [29] [13]. The survivability of a network is concerned with the ability of the network to provide a defined degree of assurance that the system will continue to function during and after a natural or man-made disturbance [2]. In [9], survivability is defined as the ability of the network computing system to provide essential services in the presence of attacks and/or failures, and recover full service in a timely manner.

While these definitions of network survivability provide a good description of the concept of survivability, they do not have the mathematical precision to lead to a quantitative characterization. A variety of metrics have been used to define survivability in both voice and data networks. For voice networks, metrics like call blocking probability, call dropping probability, etc., are adopted. Along this line, framework of telephone network survivability is discussed extensively in

[*]This research was supported in part by the Air Force Office of Scientific Research under MURI Grant No. F49620-00-1-0327, and in part by DARPA and US Army Research Office under Award No. C-DAAD19 01-1-0646. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and does not necessarily reflect the view of the sponsoring agencies.

[†]This work was done while K. Trivedi was a visiting professor in the Department of Computer Science and Engineering holding the Poonam and Prabhu Goel Chair at IIT Kanpur.

MSWiM'02, September 28, 2002, Atlanta, Georgia, USA.
Copyright 2002 ACM 1-58113–610-2/02/0009 ...$5.00.

recent works, such as in [22], [25], and [31]. A sample survivability analysis is carried out in [23], where a simulative solution is carried out for the GSM network survivability. For data networks, the metric of number of disconnected nodes is used in [18] for the survivability routing problem in mobile ad hoc network (MANET), the metric of connection survivability is used in [31] to evaluate the survivable wireless ATM architecture, and the metric of connectivity efficiency is used in [20] to analyze wireless ad hoc network survivability.

With these diverse interpretations of survivability, it is not easy to uniquely quantify network survivability. As an example, we cannot say one network architecture is more survivable than another one merely because it has lower call blocking probability or higher average connectivity. Thus it is difficult to compare network survivability architectures as an architecture may be superior than another in some aspects and vice versa.

Based on these observations, we propose a unified quantitative approach to compute network survivability in this paper. We begin with the definition of survivability due to Knight and Sullivan in [14], where a four-tuple is used to describe the survivability specification. In this paper, we build a stochastic model based on this definition, and we solve the model for the probability that the system resides in preferred states.

Although the definition in [14] is amenable to a quantitative survivability characterization, it did not take into account the impact of the failure conditions, which is emphasized in T1A1.2 group's network survivability performance definition [3]. According to T1A1.2 working group's definition, the assessment of network survivability performance has two facets. First, the assessment of the frequency of occurrance of abnormal conditions, and second, the assessment of the impact of these conditions. Of these two facets, only the frequency of occurrence of abnormal conditions assessment is considered in the definition in [14].

In this paper, we propose to carry out a composite approach to evaluate the network survivability performance, where the transient overload analysis is incorporated into the failure frequency analysis. In other words, we use a composite model which captures both the system transient behavior, an important measure to evaluate failure impact on the system [26] [24], and the system steady state behavior. With this approach, both the failure frequency and the failure impact aspects are considered for a comprehensive network survivability characterization.

As an illustration of this concept, the end to end survivability performance of wireless ad hoc networks is studied. With increasing interest and emphasis on wireless and mobile networks, it is important for such networks to possess the capability to overcome failures and provide survivable services. A higher degree of survivability may be achieved by ad hoc networks due to the fact that the ad hoc network is highly decentralized and each node has its own computing facility. Compared to the wireless networks with a central controller, the failure of some nodes or links in an ad hoc network may not necessarily bring the whole network down. In our work, we apply the aforementioned techniques to quantitatively analyze the end to end survivability of this class of networks.

The organization of this paper is as follows: In Section 2 we give the definition of survivability, in Section 3 the availability analysis of wireless ad hoc network is carried out, in Section 4 we present the transient analysis of system behavior under overloads, and in Section 5 the composite survivability model is introduced. Finally, Section 7 concludes the paper.

2. DEFINITION OF SURVIVABILITY PERFORMANCE

The definition of survivability for telecommunications systems by Federal Standard 1037C is [2]:

Definition 1. *Survivability is a property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance; e.g., nuclear burst. Note: For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration.*

For information system survivability, the definition in [9] is:

Definition 2. *Survivability is the ability of the network computing system to provide essential services in the presence of attacks and/or failures, and recover full service in a timely manner.*

While these definitions provide a good description of the concept of survivability, they do not have mathematical precision to lead to a quantitative determination of survivability. It is hard to determine whether a given system is survivable, and it is difficult to compare the survivability of two systems.

For this reason, Knight and Sullivan [14] introduced a general definition of survivability for critical information systems:

Definition 3. *A survivability specification is a four-tuple,* $(\{E, R, P, M\})$ *where:*

- E *is a statement of the assumed operating environment for the system. It includes details of the various hazards to which the system might be exposed together with all of the external operating parameters. To the extent possible, it must include any anticipated changes that might occur in the environment.*

- R *is a set of specifications each of which is a complete statement of a tolerable form of service that the system must provide. This set will include one distinguished element that is the normal or preferred specification, i.e., the specification that provides the greatest value to the user and with which the system is expected to comply most of the time.*

- P *is a probability mass function across the set of specifications,* R*. A probability is associated with each member of the set* R *with the sum of these probabilities being one. The probability associated with the preferred specification defines the fraction of operating time during which the preferred specification must be operational.*

- *M is a finite-state machine denoted by the four-tuple $\{S, s_0, V, T\}$ with the following meanings:*

  - *S: A finite set of states each of which has a unique label which is one of the specifications defined in R.*
  - *s_0: $s_0 \in S$ is the initial or preferred state for the machine.*
  - *V: A finite set of customer values.*
  - *T: A state transition matrix.*

and a system is survivable if it complies with its survivability specification

By this definition, a probability is assumed to be assigned to each state, and the system survivability is determined by the probability that the system reside in the preferred states. In Section 3 we show how to compute the probability mass function P for the set of states in S.

The concept of network survivability performance is introduced by the T1A1.2 working group on network survivability performance [3]. The network survivability performance provides an assessment of how well a network supports its function under abnormal conditions. These abnormal conditions can either be introduced by failures of network elements or caused by events that generate abnormally high-traffic levels, such as congestion at certain nodes. The emphasis of network survivability performance evaluation is on the assessment of the frequency of the abnormal conditions, and the assessment of the impact of these conditions [32].

This concept can be connected with Definition 3 in that the probability of system residing in *undesirable* states is associated with the frequency and duration of the abnormal conditions. In addition to Definition 3, the transient system performance under occurrence of failures needs to be incorporated as one of the measure of network survivability performance to reflect the performance degradations of the network under abnormal conditions

To this end, the network survivability performance can thus be centered on

- the frequency of failure events;
- the duration of the outages; and
- the impact of failures on the system.

In fact, the first two items may be resolved by availability analysis following Definition 3, when the system failure mechanisms are known. The third item involves system transient analysis, where the measures of interest may be maximum overshoot, or relaxation time, or expected excess loss in overload, or the combination of two or more items [30]. The combination of the availability measure and the transient measures together determine overall system survivability.

Inspired by this observation, in subsequent sections we carry out the availability analysis and the transient analysis of wireless ad hoc networks under failures, as well as a composite model that combines both of these measures. We hope our paper provides a unified approach for network survivability performance evaluation.

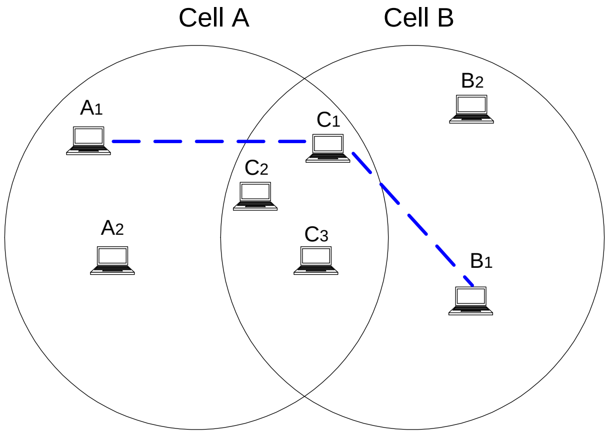

Figure 1: A simple ad hoc network with two cells

3. SYSTEM AVAILABILITY ANALYSIS

Consider a simple wireless ad hoc network shown in Figure 1, which consists of two cells, cell A and cell B. We use A_1 and A_2 to represent the mobile terminals in cell A but not in cell B, B_1 and B_2 to represent the mobile terminals in cell B but not in cell A, and we use C_1, C_2 and C_3 to represent the mobile terminals that are in the intersection area of cells A and B. It is worthwhile to point out that the notion of *cell* is used in the sense that the mobile terminals in each cell are able to communicate with each other, while mobiles in different cells cannot directly communicate with each other due to either transmission range limits or physical obstacles between the cells. In this case, C_1, C_2 and C_3 may act as *routers* for A_1 and A_2 to establish links with B_1 and B_2.

Connecting with Definition 3, the statement of the assumed system operation environment, E, is described in the above paragraph. To describe the set R, or the system tolerance for each specific environment, we need to understand the system fault model. Only with this information can we determine the fault patterns that the system is required to tolerate. With this knowledge, the finite state automata M is then converted into a continuous time Markov chain (CTMC) model. Assigning transition rates to state transitions and solving the CTMC, the probability mass function, P, is then obtained.

3.1 Fault model

Physical faults of the end to end communication connection in the ad hoc network system include [5]:

- Node faults: The node faults in an end to end connection may be caused by the unavailability of the routers, due to the mobility of terminals in the intersection region of the cells A and B. In Figure 1, if mobile station C_1 moves out of the intersection region, a router fault occurs on the path between A_1 and B_1. When this happens, the routing task between these two terminals may be switched to another mobile in the intersection region (C_2 or C_3 in our case). When no router is available, the connection between A_1 and B_1 fails.
- Power faults: Power faults are caused by the limited battery life in mobile stations. A router may be in-

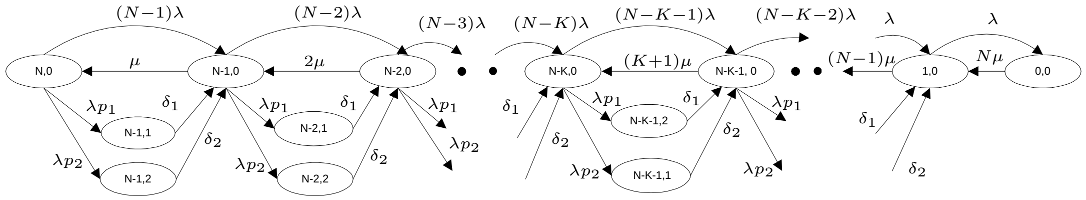

Figure 2: CTMC model for system end to end availability

capable of performing the routing task either due to insufficient power, or due to its desire to reserve energy for later use. In such cases, the terminals in A and B will need to switch to another router.

- Link faults: Link faults are introduced by either obstacles between nodes, known as the slow fading effect, or by excessive noise in the wireless link. Under the occurrence of a link fault, the communication between terminals in cells A and B may either be routed through another node, or interrupted for a while until the link recovers, depending on the nature of the fault and the service requirement of the communication task.

When a fault cannot be tolerated, a failure in the communication will occur. From the *failure domain* viewpoint, failures can be classified as *value failures*, where the value of the delivered service does not comply with the specification, and *timing failures*, where the timing of the service delivery does not comply with the specification [8] [6]. For the ad hoc network, a failure in the communication link may lead to both packet losses, which is value failure, and excessive end to end delay, which is timing failure. We call this class of failures *stopping failures*, and the ad hoc network is thus a *fail-stop* system.

3.2 Availability model

Consider the connection $A_1 \rightarrow C_1 \rightarrow B_1$ in Figure 1. If at any time, there is a node or power fault in C_1, or a link fault between A_1 and C_1, or B_1 and C_1, C_2 or C_3 will take up the routing task between A_1 and B_1 after a switching delay. In this case, C_2 and C_3 are regarded as routers for C_1. However, if faults have occurred in all three nodes, the connection between A_1 and B_1 is down until one of the three nodes is brought up again. Furthermore, due to mobility of terminals, the number of nodes in the intersection region may also vary.

When a router fault is detected by the terminal nodes, the routing task is switched to another station in the intersection area. For node or power faults, we assume the router may inform the affected terminal nodes before such faults occurs (i.e., the router has the capability to issue a warning before it runs out of power or moves out of the intersection region.). On the other hand, for link faults, it is nearly impossible for the router to issue such a warning beforehand. With a prior warning, the affected terminal nodes will have the chance to switch to another router before the current router fails; while without any warning, the affected terminal nodes will need to look for a router after the fault is detected. For this reason, we assume that the node and power faults incur a smaller switching delay than link faults. And thus in our model, we discriminate between the node and power faults from link faults by means of differences in system switching delays.

In our study, we assume the failure rate for each router is λ. When a fault occurs, the probability of this fault being a node or power fault is p_1; and the probability of this fault being a link fault is p_2. The average switching delay for node and power faults is $1/\delta_1$; and the average switching delay for link fault is $1/\delta_2$. The repair rate for either type of fault is μ.

According to Definition 3, a quantitative survivability characterization involves the construction of the finite state machine model with a complete specification of the system operating environment, and the probability mass assignment to each state in the finite state machine. We observe that this task may also be achieved by converting the FSM into a Markov chain where the state transitions are assigned transition rates. In this sense, we may construct a homogeneous continuous time Markov chain (CTMC) model for this problem, and solve for the steady-state probability that the system is up, also known as the steady-state availability.

Note that besides the CTMC approach, other paradigms may also be used to study this problem. For example, when the exponential assumptions does not hold for CTMC models, we may solve the problem either by Markov regenerative process [16] or by Markov fluid models [10]. For more complex systems where it is hard and error prone to construct the CTMC by hand, stochastic Petri nets may be applied to automatically construct and solve the underlying CTMC [7] [11]. Moreover, simulation and experimentation approaches may also be applied. In this paper, we present a simplified system model solvable by CTMC for the purpose of better illustrating the approach of quantitative survivability performance evaluation.

Thus for simplicity of presentation, we have made the following assumptions:

- All component failure events are mutually independent;
- Exponential distribution is assumed for time to occurrence of each component failure event;
- Different types of failures have the same repair rate; and
- The switching delay is small compared to the average time to router failures, so that during the switching delay no additional failure event occur.

Let $i \in I = \{0, 1, \cdots, N\}$ represent the number of available routers for the connection; and let $j \in J = \{0, 1, 2\}$ represent the type of fault ($j = 0$ represents no fault, $j = 1$ represents a node or power fault, and $j = 2$ represents a link fault). The tuple $\{(i, j), i \in I, j \in J\}$ defines a state where the connection is up (or down) with i routers available and with (or without) fault type j. The underlying stochastic process is a homogeneous CTMC with state space $I \times J$.

Figure 2 shows the CTMC model for the system end to end availability. We assume that there are a total of $N+2$ nodes in the system, and therefore there are a total of N nodes that may act as routers. State $(N, 0)$ represents the state where the connection is up, with all of the N nodes are in the intersection region, each not having failed. In this state, either the $N-1$ backup routers may fail with rate λ, and bring the system to state $(N-1, 0)$, representing that the connection is up and the number of backup routers is reduced to $N-2$, or the router in use may fail and bring the connection down. The main router fault follows the two scenarios we discussed earlier: it may fail with probability p_1 as a node or power fault, and bring the system to state $(N-1, 1)$ (representing the connection is down due to a node/power fault, with $N-1$ routers available to switch over), or it may fail with probability p_2 as a link failure, and bring the system to state $(N-1, 2)$ (representing the connection is down due to a link failure, with $N-1$ routers available to switch over). For a node/power fault, the average switching delay is $1/\delta_1$, and for a link failure, the average switching delay is $1/\delta_2$.

Let $\pi_{i,j}$ be the corresponding steady-state probability, and by solving the above mentioned Markov chain we have

$$\pi_{0,0} = \frac{1}{1 + \sum_{j=2}^{N} \frac{(N-j)!(j-1)!}{N!} \rho^j (1 + \frac{\lambda p_1}{\mu_1} + \frac{\lambda p_2}{\mu_2}) + \frac{1}{N}\rho^j} \quad (1)$$

$$\pi_{j,0} = \frac{(N-j)!(j-1)!}{N!} \rho^j \pi_{j,0} \quad (2)$$

$$\pi_{j,1} = \frac{(N-j)!(j-1)!}{N!} \rho^j \frac{\lambda p_1}{\mu_1} \pi_{j,0} \quad (3)$$

$$\pi_{j,2} = \frac{(N-j)!(j-1)!}{N!} \rho^j \frac{\lambda p_2}{\mu_2} \pi_{j,0} \quad (4)$$

where $\rho = \frac{\lambda}{\delta}$.

The measures of interest that could be obtained are:

- Steady state availability:

  The end to end connection availability, A_s, is

$$A_s = \sum_{j=1}^{N} \pi_{j,0} \quad (5)$$

- Failure frequency:

  Following the approach in [27], the failure frequency may be represented as $A_s \lambda_{eq}$, where λ_{eq} is the equivalent failure rate. To compute λ_{eq}, the states are partitioned into two classes of states, *up* states (denoted by U) and *down* states (denoted by D). Transitions from up states to down states are called *red* transitions (denoted by R) and transitions from down states to up states are called *green* transitions (denoted by G). The equivalent failure rate is then:

$$\lambda_{eq} = \sum_{t_{a,b} \in R} P(\text{system in state } a \,|\, \text{system is up}) \times q_{a,b} \quad (6)$$

$$= \frac{\sum_{j=1}^{N} \pi_{j,0} \lambda}{\sum_{j=1}^{N} \pi_{j,0}} \quad (7)$$

$$= \lambda \quad (8)$$

where $q_{a,b}$ is the (a,b)th element of the infinitesimal generation matrix of the CTMC.

The failure frequency in our CTMC model is thus

$$f_e = \lambda \sum_{j=1}^{N} \pi_{j,0}$$

Mapping our CTMC development onto the four tuple survivability definition 3, E corresponds to the system fault/error/failure analysis; R corresponds to the ability of the system to tolerate the router failures; M corresponds to the CTMC model presented in Figure 2; and whether the system could meet the constraints defined by P may be determined from the probability measures obtained by solving the CTMC in Figure 2.

4. TRANSIENT ANALYSIS OF SYSTEM BEHAVIOR UNDER FAILURES

4.1 Expected excess loss in overload (EELO)

Under communication failures, transient traffic overload is an inevitable situation. In this case, steady-state analysis fail to predict such transient phenomena, and transient analysis is desired. As some examples, Wang *et al* studied the transient behavior of ATM networks under overloads in [30], and Logothetis and Trivedi analyzed the transient analysis of the leaky bucket rate control scheme in [17].

When there is no failure, the pure performance model of the end to end connection may be cast as an $M/M/1/K$ queue as shown in Figure 3, where λ_p is the packet arrival rate, and μ_p is the channel service rate. Let $P_m(i,t)$ be the probability that the CTMC is in state i at time t, which may be found by solving the following system of differential equations:

$$\frac{dP_m(0,t)}{dt} = -\lambda_p P_m(0,t) + \mu_p P_m(1,t) \quad i = 0 \quad (9)$$

$$\frac{dP_m(i,t)}{dt} = -(\lambda_p + \mu_p) P_m(i,t) + \lambda_p P_m(i-1,t) + \mu_p P_m(i+1,t) \quad K > i \geq 1 \quad (10)$$

$$\frac{dP_m(K,t)}{dt} = -\mu_p P_m(K,t) + \lambda_p P_m(K-1,t) \quad i = K \quad (11)$$

The steady state probability, $P_m(i)$, may be obtained by letting $dP_m(i,t)/dt = 0$. Solving the set of linear equations, we have

$$P_m(i) = \rho_p^i P_m(0), \quad 0 < i \leq K \quad (12)$$

$$P_m(0) = \frac{1}{\sum_{i=0}^{K} \rho_p^i} = \begin{cases} \frac{1-\rho_p}{1-\rho_p^{K+1}}, & \rho_p \neq 1 \\ \frac{1}{K+1}, & \rho_p = 1. \end{cases} \quad (13)$$

where $\rho_p = \lambda_p / \mu_p$.

When a failure occurs, the channel is down and thus the service rate is 0. In this case, the queuing model becomes a pure birth process with a finite queue size. We use $P_n(i|k,t)$ to represent the probability that there are i packets in the buffer at time t, with k packets initially in the buffer at the

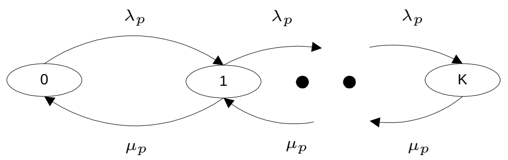

Figure 3: Performance model for the $M/M/1/K$ system

time the link fails. Then, the state transition equations are

$$P_n(i|k,t) = 0 \quad 0 \le i < k \le K \tag{14}$$

$$\frac{dP_n(i|k,t)}{dt} = \lambda_p P_n(i-1|k,t) - \lambda_p P_n(i|k,t) \qquad K > i \ge k \ge 0 \tag{15}$$

$$\frac{dP_n(K|k,t)}{dt} = \lambda_p P_n(K-1|k,t) \quad i = K \tag{16}$$

The transient solution of the above CTMC is [27]:

$$P_n(i|k,t) = \begin{cases} 0, & i < k \le K \\ \frac{(\lambda t)^{i-k}}{(i-k)!}e^{-\lambda_p t}, & K > i \ge k \\ 1 - \sum_{j=0}^{i-k} \frac{(\lambda t)^j}{j!}e^{-\lambda_p t} & i = K \end{cases} \tag{17}$$

The buffer full probability at time t, with k initial number of jobs, is thus

$$P_n(K|k,t) = 1 - \sum_{j=0}^{K-k} \frac{(\lambda t)^j}{j!}e^{-\lambda_p t}$$

Suppose the system downtime duration is t_x. Then, the expected number of lost packets in this period, with k packets initially in the buffer before the failure, is thus

$$l_r(k,t_x) = \int_0^{t_x} \lambda_p P_n(K|k,t)dt,$$

and the amount of excessive loss incurred by the failures is given by

$$L_r(k,t_x) = \int_0^{t_x} \lambda_p P_n(K|k,t)dt - \lambda_p P_m(K).$$

This measure was introduced as *expected excess loss in overload (EELO)* in [30]. In our problem, since the failure may occur at a random time, the buffer initial condition is also a random variable and need to be taken into consideration. Assuming the system has reached steady state before failure occurrence, the average excess loss is then

$$EELO(t_x) = \sum_{k=0}^{K} l_r(k,t)P_m(k) - \lambda_p P_m(K)t_x \tag{18}$$

Moreover, the switching delay t_x may also be a random variable. Suppose the probability distribution function of switching delay t_x is $P_s(t_x)$, then by unconditioning $EELO(t_x)$ with respect to t_x we get

$$EELO|_{t_x \sim P_s(t_x)} = \sum_{k=0}^{K} \int_0^{\infty} l_r(k,t_x)P_m(k)P_s'(t_x)dt_x - \int_0^{\infty} \lambda_p P_m(K)t_x P_s'(t_x)dt_x \tag{19}$$

4.2 Expected excess delay in overload (EEDO)

For real time multimedia applications, such as voice over IP, link delay is also an important measure [28]. Suppose the system downtime is a random variable t_x with probability distribution function $P_s(t_x)$. Then, the expected excess delay may be easily derived as

$$EEDO|_{t_x \sim P_s(t_x)} = \int_0^{\infty} t_x P_s'(t_x)dt_x.$$

5. HIERARCHICAL SURVIVABILITY MODEL

As discussed in Section 1, the system survivability performance involves both the system availability and the system transient response under failure conditions. To combine these two measures, we construct a hierarchical system survivability model. For this purpose, the system availability model in Figure 2 is used, and the system transient overload performance, i.e., EELO and EEDO in this paper, are assigned as cost (reward) for each system failure occurrence. The composite measures are given in (20) and (21). It is interesting to note that this measure in fact reflects the excessive packet loss rate or excessive packet delay *due to system failures* that have incurred interruption of service. For this reason, we call these measures as *excess loss due to failures (ELF)* and *excess delay due to failures (EDF)* respectively. In this sense, these measures reflect both the *duration of failures* and the *impact of failures*, as defined in [3].

$$ELF = \sum_{j=1}^{N} \big(\lambda\pi_{j,0}\big(p_1 EELO|_{t_x \sim EXP(1/\delta_1)} + p_2 EELO|_{t_x \sim EXP(1/\delta_2)}\big)\big) + \lambda\pi_{1,0}EELO|_{t_x \sim EXP(1/N\mu)} \tag{20}$$

$$\begin{aligned} EDF &= \sum_{j=1}^{N} \big(\lambda\pi_{j,0}\big(p_1 EEDO|_{t_x \sim EXP(1/\delta_1)} + p_2 EEDO|_{t_x \sim EXP(1/\delta_2)}\big)\big) + \lambda\pi_{1,0}EEDO|_{t_x \sim EXP(1/N\mu)} \\ &= \sum_{j=1}^{N} \big(\lambda\pi_{j,0}\big(\frac{p_1}{\delta_1} + \frac{p_2}{\delta_2}\big)\big) + \lambda\pi_{1,0}\frac{1}{N\mu} \end{aligned} \tag{21}$$

The EDF may be obtained directly when the system steady-state probabilities are obtained from (5). The procedure to obtain ELF involves the following steps:

- Solve the steady state system availability model by (5);
- Solve the steady state system performance model by (13);
- Solve the transient system model under failures, by (17);
- Solve the EELO by (19);
- Assign the transient performance measure, EELO, as costs in the states of the system availability model according to (20), and solve for the ELF.

We would also like to point out that although we have used analytic models (CTMC in our case) to get the system availabilty and system transient measures, other methods, such

Parameter	Meaning	Value
λ	Failure rate	0.01 per sec
$1/\mu$	Average reapir time	20 sec
p_1	Node/power failure probability	0.5
p_2	Link failure probability	0.5
$1/\delta_1$	Node/power failure switching delay	0.001 sec
$1/\delta_2$	Link failure switching delay	0.01 sec
λ_p	Packet arrival rate	100 per sec
μ_p	Packet transmission rate	200 per sec
K	Buffer size	50 packets

Table 1: Parameters for numerical evaluation

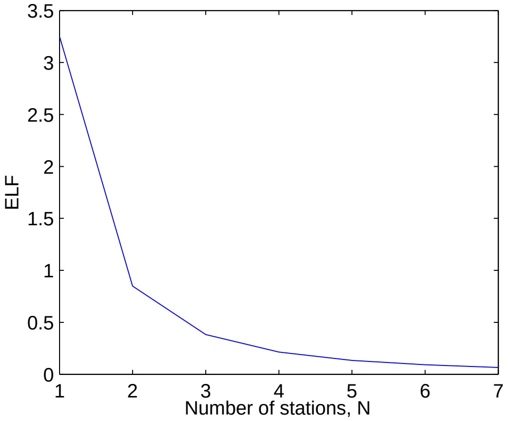

Figure 4: ELF with respect to the number of stations

as simulation or experimentation, may also be used. Simulations and experimentations are althernative approaches to analytic approaches when higher accuracy is desired, or when the assumptions made by analytic approaches do not hold. Even with these approaches, the general procedure presented here still applies.

6. NUMERICAL EXAMPLES

As a numerical example, consider the ad-hoc network shown in Figure 1. Assume that there are N intermediate nodes in the system other than the communication terminals A_1 and B_1. The other parameters are chosen as in Table 1.

Figure 4 shows the system ELF and Figure 5 shows the system EDF with respect to the number of stations. From this figure, we observe that the ELF and EDF drops fast with the number of stations, N, increased from 1 to 3. After that, the ELF and EDF drops relatively slowly with the increase in number of stations.

As another experiment, we examine the ELF with respect to the buffer size, with a station number N chosen to be 3 and 5. The result is shown in Figure 6. From Figure 6 we observe that with fewer number of stations, the ELF may be more significantly reduced by increasing the buffer size (determined from the slopes of the curves corresponding to $N = 3$, $N = 5$ and $N = 7$.

7. CONCLUSION

In this paper, we have presented a quantitative approach to evaluate the system survivability performance. We define the system survivability to be a composite measure that should include both the failure duration and the failure impact on the system. With this definition, the wireless adhoc communication system is considered, with a focus on router failures. For this system, the measure of system excess packet losses due to failures is introduced, which is a combination of the system failure duration and the packet losses during each failure. Our future research along this line includes the survivability analysis of systems with more complex structure, as well as other paradigms to obtain the survivability measures introduced in this paper.

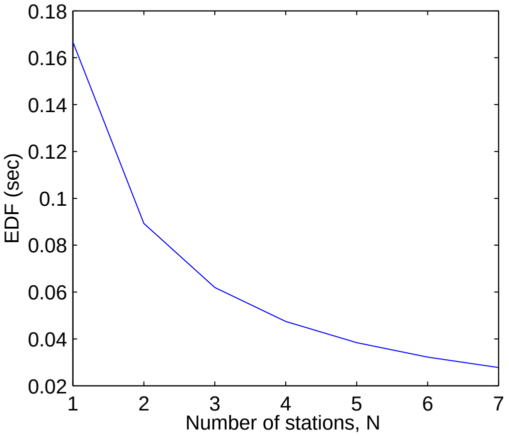

Figure 5: EDF with respect to the number of stations

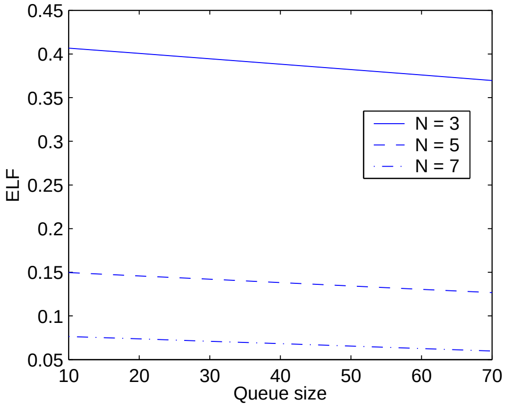

Figure 6: ELF with respect to the buffer size

8. REFERENCES

[1] Network reliability steering committee annual report 2000. http://www.atis.org/pub/nrsc/2000Rpt.pdf.

[2] U. S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunications Services, Federal Standard 1037C.

[3] T1A1.2 Working Group on Network Survivability Performance, Technical report on enhanced network survivability performance, February 2001.

[4] A. Avizienis. Design diversity - the challenge of the eighties. In *Digest of FTCS-12*, pages 44–45.

[5] D.-Y. Chen, Y. Hong, and K. S. Trivedi. Classification

of faults, errors and failures in communication systems. In *Submitted for publication.*

[6] P. F. Chimento. *System performance in a failure prone environment.* PhD thesis, Duke University, 1988.

[7] G. Ciardo, J. Muppala, and K. S. Trivedi. Spnp: stochastic petri net package. In *Proc. 3rd International Workshop on Petri Nets and Performance Models*, pages 142–151, 1989.

[8] F. Cristian, H. Aghili, R. Strong, and D. Dolev. Atomic broadcast: From simple message diffusion to Byzantine agreement. In *Proceedings of the 15th International Conference on Fault-Tolerant Computing*, Silver Spring, Maryland, 1985. IEEE Computer Society.

[9] B. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead. Survivable network systems: An emerging discipline. Technical Report CMU/SEI-97-TR-013, Software Engineering Institute, Carnegie Mellon University, November 1997.

[10] A. I. Elwalid and D. Mitra. Statistical multiplexing with loss priorities in rate-based congestion control of high-speed networks. *IEEE Transactions on Communications*, 42(11):2989–3002, November 1994.

[11] G. Horton, V. G. Kulkarni, D. M. Nicol, and K. S. Trivedi. Fluid stochastic Petri nets: Theory, applications, and solution techniques. *European Journal of Operational Research*, (105):184–201, 1998.

[12] M. Kalyanakrishnan, R. K. Iyer, and J. Patel. Reliability of Internet hosts: A case study from the end user's perspective. In *Proceedings of sixth international conference on computer communications and networks*, pages 230–246, 1997.

[13] J. Knight, K. J. Sullivan, M. C. Elder, and C. Wang. Survivability architectures: Issues and approaches. In *DARPA Information Survivability Conference and Exposition (DISCEX 2000)*, Hilton Head, SC, January 2000.

[14] J. C. Knight and K. J. Sullivan. On the definition of survivability. Technical Report CS-TR-33-00, University of Virginia, Department of Computer Science, 2000.

[15] C. Labovitz, A. Ahuja, and F. Jahanian. Experimental study of Internet stability and backbone failures. In *Proceedings of FTCS*, pages 278–285, 1999.

[16] D. Logothesis, K. S. Trivedi, and A. Puliafito. Markov regenerative models. In *Proc. Intl. Computer Performance and Dependability Symp.*, pages 134–143, Erlangen, Germany, 1995.

[17] D. Logothetis and K. S. Trivedi. Transient analysis of the leaky bucket rate control scheme under poisson and on-off sources. In *INFOCOM'94*, volume 2, pages 490–497, 1994.

[18] V. Marbukh and M. W. Subbarao. Framework for maximum survivability routing for a MANET. In *MILCOM 2000*, volume 1, pages 282–286.

[19] A. M. Noll. *Private Networks and Public Objectives*, chapter Network Security and Reliability: Emergencies in Decentralized Networks, pages 343–356. Elsevier Science, Amsterdam, The Netherlands, 1996.

[20] C. G. Omidyar, editor. *Survivability analysis of Ad Hoc wireless network architecture*, volume 1818 of *Lecture Notes in Computer Science.* Springer, 2000.

[21] B. C. Research. Reliability and quality measurements for telecommunications systems (rqms). Technical report, Bellcore, 1998.

[22] A. P. Snow, U. Varshney, and A. D. Malloy. Reliability and survivability of wireless and mobile networks. *IEEE Computer*, 33(7):49–54, 2000.

[23] D. Tipper, T. Dahlberg, H. Shin, and C. Charnsripinyo. Providing fault tolerance in wireless access networks. *IEEE Communications Magazine*, 40(1):58–64, 2002.

[24] D. Tipper, J. Hammond, S. Sharma, A. Khetan, and K. B. S. Menon. An analysis of the congestion effects of link failures in wide area networks. *IEEE Journal on Selected Areas in Communications*, 12(1), January 1994.

[25] D. Tipper, S. Ramaswamy, and T. Dahlberg. PCS network survivability. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'99)*, pages 1028–1032, New Orleans, LA, 1999.

[26] D. Tipper and M. Sundaresan. Numerical methods for modeling computer networks under non-stationary conditions. *IEEE Journal on Selected Areas in Communications*, 8(9):1682–1695, 1990.

[27] K. S. Trivedi. *Probability & Statistics with Reliability, queuing, and Computer Science Applications.* John Wiley & Sons,, second edition, 2001.

[28] M. Veeraraghavan, N. Cocker, and T. Moors. Support of voice services in IEEE 802.11 wireless LANs. In *Proceedings of INFOCOM'01*, 2001.

[29] C. Wang, J. Davidson, J. Hill, and J. Knight. Protection of software-based survivability mechanisms. In *International Conference of Dependable Systems and Networks*, Goteborg, Sweden, July 2001.

[30] C.-Y. Wang, D. Logothetis, K. S. Trivedi, and I. Viniotis. Transient behavior of ATM networks under overloads. In *Proceedings of the IEEE INFOCOM'96*, San Francisco, March 1996.

[31] Y. H. Wang, W. S. Soh, M. Y. Tsai, and H. S. Kim. Survivable wireless ATM network architecture. In *Ninth International Conference on Computer Communications and Networks*, pages 368–373, 2000.

[32] A. Zolfaghari and F. J. Kaudel. Framework for network survivability performance. *IEEE Journal on Selected Areas in Communications*, 12(1):46–51, January 1994.