Scalability of Network-Failure Resilience

Guanglei Liu and Chuanyi Ji, *Senior Member*

Abstract— In this work we quantify scalability of network resilience upon failures. We characterize resilience as the percentage of lost traffic upon failures [5] and define scalability as the growth rate of the percentage of lost traffic with respect to network size, link failure probability and traffic for given failure protection schemes. We apply probabilistic graphical models to characterize statistical spatial dependence between physical-layer failures and logical network topologies for traffic flows. We then derive the scalability for large networks of different topologies.

We first focus on the scalability of resilience for regular topologies under uniform traffic with independent and dependent link failures, with and without protection. For large networks with small probabilities of failures and without protection, we show that the scalability of network resilience grows linearly with the average route length and with the effective link failure probability. For large networks with 1+1 protection, we obtain lower and upper bound of the percentage of lost traffic. We derive approximations of the scalability for arbitrary topologies, and attain close-form analytical results for ring, star, and mesh-torus topologies. We then study network resilience under random traffic with Poisson arrivals. We find that when the network is under light load (small traffic arrival rate), the network resilience is reduced to that under uniform deterministic traffic. Our scalability analysis shows explicitly how network resilience varies with different factors and provides insights for resilient network design.

***Index Terms*—network resilience, scalability, probabilistic graphical models, dependent failures, Erlang fixed point approximation.**

I. INTRODUCTION

Network resilience to failures has been a fundamental problem in networking. In the past decade, due to a dramatic increase in network complexity and scale, network failures have become a norm rather than an exception [1]. For example, failures may result from hardware/software faults, operator errors, malicious attacks, and natural disasters [2]. With current demands for high network resilience, it is imperative to understand and quantify resilience for network design and operation.

What is network resilience? Network resilience is closely related to reliability that has been defined through deterministic and probabilistic metrics [3]. Deterministic measures consider whether a network is still connected upon failures. Two basic deterministic metrics are cohesion and connectivity of the underlying graph [3] [4], which denote the minimum cardinality of an edge cut-set and a node cut-set respectively. Probabilistic metrics assume that components may fail with a certain probability, which are be further categorized as "non-traffic-based" and "traffic-based" [5].

The "non-traffic-based" approaches focus on an underlying topology and the network connectivity. A common non-traffic-based metric is the *k*-terminal reliability, which is defined as the probability that a specific set of *k* nodes can communicate with one another [6]. Non-traffic-based measures do not consider constraints resulting from the network layer, i.e., link capacity, traffic distribution, and protection schemes upon failures. Moreover, such metrics may not be meaningful for well-connected topologies, where the network connectivity remains high even after failures occur.

Traffic-based metrics considers the amount of traffic carried by a network so that the degree of service disruptions can be quantified. In particular, traffic-based measures focus on the effects of multiple factors, such as physical layer failures, network layer traffic, and failure protection operation schemes, A key open issue in non-traffic-based and traffic-based network resilience is scalability. The scalability shows how the "rate" of the resilience varies with different factors, and provides insights for resilient network design. Hence, the impact of the multiple factors to the scalability is the focus of this work.

A challenge to quantify traffic-based resilience and thus scalability is that the metrics depend on multiple factors at both the physical layer and the network layer. A cross-layer model is thus required to include all these factors. Specifically, we define resilience as the percentage of the lost traffic upon failures [5]; and the scalability as the rate of the percentage of lost traffic that varies with respect to the following factors:

- Physical topologies,
- Dependent failure at the physical layer,
- Network traffic protection schemes upon failures,
- Network layer traffic.

We then apply probabilistic graphical models to characterize statistical spatial dependence between physical layer failures and logical topologies. Expansion techniques are then used to obtain asymptotic results on the growth rate of the resilience, i,e, the scalability.

For simplicity of analysis, we first assume uniform deterministic (all-to-all) traffic at the network layer. This allows us to focus on the impacts of the first three factors on the resilience and the scalability. We show that, for large networks, small probabilities of failures and without protection, the resilience is $O(\bar{h}p_e)$, where $\bar{h}$ is the average route length that depends on a network-size and network-layer traffic (routes), and p_e is the effective link failure probability. With 1+1 protection and independent failure, the percentage of lost traffic is between $O[(\bar{h}p)^2]$ and $O[k^2(\bar{h}p)^2]$, where k is the number of nodes in the networks and p is marginal probability of link failure. With 1+1 protection and dependent failure, the percentage of lost traffic is between $O[2bp_b^2+(\bar{h}p_e)^2]$ and $O[2bp_b^2+k^2(\bar{h}p_e)^2]$, where b and p_b are parameters in the dependent failure model to be discussed in detail in Section IV.B. In addition, we obtain close-from expressions on

resilience and scalability for ring, star, and mesh-torus topologies.

For networks under stochastic traffic, we adopt Poisson traffic arrivals. To obtain analytical results on the resilience and the scalability, we employ Erlang Fixed Point Approximation (EFPA) [8]. We find that: (1) when the network is under light load, the resilience of the network is reduced to that under uniform deterministic traffic, and (2) when the network is under a high load, the percentage of lost traffic approaches its upper bound, which is the marginal probability of link failure.

The rest of the paper is organized as follows. In Section II, we discuss the related work. In Section III, we present the problem formulation. In Section IV and Section V, we consider network resilience under deterministic traffic and dynamic traffic respectively. Finally, Section VI summarizes the paper.

II. Related Work

There has been extensive research in connectivity-based network reliability metrics. The problems of computing connectivity-based metrics are generally NP-hard since the total number of possible routes between node-pairs usually grows exponentially with the size of a network. Therefore, different algorithms for evaluating *k-terminal* reliability have been proposed using heuristics, e.g. [6].

Traffic-based network reliability metrics are defined in [5] as the percentage of traffic lost due to failures. This metric is then used to study the reliability of ring networks without protection and pre-planned protection. However, the study in [5] is restricted to independent failures, ring networks, and deterministic traffic. A general framework is proposed in [2] to quantify network survivability upon failures. In addition, a composite Markov model is used to study the transient/steady state behavior of a point-to-point telecommunication link. The composite Markov model has the advantage of representing failure events, but is too complex for analysis of dependent failures at the network level. Two other frameworks are proposed in [9][10] to evaluate network survivability, where the focuses are on definitions of survivability metrics for network failures of different degree, i.e., catastrophic, major or minor.

Another closely-related research area is network design. A metric of *k-terminal* reliability is used in [3] to study topological architectures for networks under stress. The work in [3] considers the effects of physical topologies and dependent failures on reliability, but ignores the impact of network traffic and protection schemes.

One open issue in the aforementioned research is the scalability of network resilience for large networks, i.e., how the resilience varies with multiple factors from both the physical and the network layer. Hence the scalability shall be the focus of this work.

III. Problem Formulation

We begin with an example of network resilience.

A. Example

Consider an example of the NSF (National Science Foundation) network in Figure 1, which consists of 14 nodes and 21 links. For simplicity of illustration, we assume fixed routing on a set of 5 routes: $\mathbf{R} = \{r_{12}, r_{14}, r_{19}, r_{24}, r_{29}\}$, which are marked as dashed lines in Figure 1. The subscripts denote the source and destination nodes of each route. Then the active connections on each route in $\mathbf{R}$ form the network layer traffic. When the link between node 1 and node 2 fails, traffic carried by connections on routes (1,2), (1,4) and (2,9) would get lost. Hence, we can quantify network resilience as the percentage of lost connections due to physical layer failures [5].

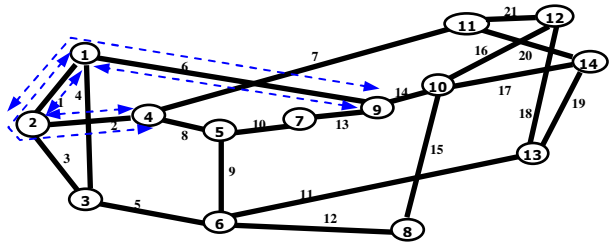

Figure 1. NSF network topology

As both the amount traffic of on each route and the link failures can be random, the interaction between the network layer traffic and physical layer failures needs to be characterized. Specifically, there remain the key question on how resilience may depend on physical topology, failure dependency, failure protection schemes, and network traffic. Next we formally define the network resilience and its scalability.

B. Problem Formulation

Let $\mathbf{G}(\mathbf{V},\mathbf{E})$ be a physical-layer topology, where $\mathbf{V}$ is a set of nodes and $\mathbf{E}$ is a set of bi-directional links. We assume fixed routing and let $\mathbf{R}$ be a set of routes used by the network for connections. The route set $\mathbf{R}$ may be determined by such factors as traffic demands and operator preference. For networks without protection, we assume that $\mathbf{R}$ consists of one link-shortest route between each pair of nodes in the network. For networks with protection, we focus on 1+1 protection and assume that $\mathbf{R}$ consists of one primary route and one link-disjoint backup route between each pair of nodes in the network.

We denote the network layer traffic as a vector $\mathbf{D} = (D_{ij} : i, j \in \mathbf{V})$, where D_{ij} is a random variable denoting the total amount of traffic carried on active connections between node i and j. In general, D_{ij} is the sum of bandwidth rates of active connections between node i and node j. Without loss of generality, we assume that each connection carries one unit of bandwidth. Then D_{ij} reduces to the total number of active connections between node i and node j.

Assume that links in $\mathbf{E}$ may fail with a certain probability. Let the status of link i be a binary random variable Z_i, where

$Z_i = 1$ if there is a failure at link i; and $Z_i = 0$ otherwise. Let the status of connections on the route between node m and n be a binary random variable S_{mn}, where S_{mn} depends on the status of the links, $S_{mn} = I(\sum_{i \in R_{mn}} Z_i)$: $I(\sum_{i \in R_{mn}} Z_i) = 1$ if $\sum_{i \in R_{mn}} Z_i > 0$; and $I(\sum_{i \in R_{mn}} Z_i) = 0$ otherwise.

For networks without protection, S_{mn}=1 if there is one or more link failures on its route; and S_{mn}=0 otherwise, i.e.,

$$P(S_{mn} = 0) = P(\sum_{i \in \mathbf{E}_{R_{mn}}} Z_i = 0), \quad (1)$$

where $\mathbf{E}_{R_{mn}}$ is the set of links traversed by route R_{mn}.

For networks with 1+1 dedicated protection, S_{mn}=1 if there are one or more link failures at both the primary route and its link-disjoint backup route ; and S_{mn}=0, otherwise, i.e.,

$$P(S_{mn} = 0) = P(\sum_{e_i \in \mathbf{E}_{R_{mn,p}}} Z_i = 0 \cup \sum_{e_i \in \mathbf{E}_{R_{mn,b}}} Z_i = 0), \quad (2)$$

where $\mathbf{E}_{R_{mn,p}}$ and $\mathbf{E}_{R_{mn,b}}$ are the set of links traversed by the primary and the backup route between node m and n respectively.

We now formally define network resilience as in [5], and then the scalability.

Definition 1: Network resilience measure k is the percentage of lost traffic due to physical link failures [5], i.e.,

$$\mathrm{k} = \frac{\mathbf{Z}}{\sum_{ij} E[D_{ij}]}, \quad (3)$$

where $\mathbf{Z} = \sum_{ij} E[D_{ij} S_{ij}]$ is the expected amount of lost traffic due to network failures.

Definition 2: Scalability of network resilience is defined as the growth rate of k with respect to the physical topology, the failure probabilities, the protection schemes, and the network layer traffic.

In this work, we focus on open-loop analysis of the network resilience and the scalability, and assume

$$\mathbf{Z} = \sum_{ij} E[D_{ij}] E[S_{ij}], \quad (4)$$

where $E[D_{ij}]$ is the expected number of active connections between node i and j; $E[S_{ij}] = P(S_{ij} = 1)$ is the probability of service unavailability for routes between node i and j. The product of expected values in (4) implies that the interaction between network layer traffic and physical layer failures is considered in an average sense. Our goal is to gain insights on impacts of multiple factors on network resilience from this relatively simple scenario.

IV. Resilience and Scalability under Uniform Deterministic Traffic

We begin with a simple network traffic model, i.e., uniform deterministic traffic, to study the effects of physical topologies, network protection schemes, and dependencies in physical layer failures. Uniform deterministic traffic means that there is one active connection on the link-shortest route between each pair of nodes in the network, i.e., $D_{ij} = 1, \forall\, i, j \in \mathbf{V}$. Thus, the resilience measures reduce to

$$\mathrm{k} = \frac{2 \sum_{i,j \in \mathbf{V}, i \neq j} E[S_{ij}]}{k(k-1)}, \quad (5)$$

where k is the number of nodes in the network and there are total $k(k-1)/2$ connections under the uniform deterministic traffic model.

A. Resilience and Scalability under Independent Failure

We first study network resilience under independent link failures. For simplicity, we assume that each link in $\mathbf{E}$ fails independently with probability p.

1) Arbitrary Physical Topology

We begin with arbitrary topologies without protection.

Lemma 1: Consider an arbitrary topology $\mathbf{G}(\mathbf{V}, \mathbf{E})$. Let p be the probability of failure of each link. Let k be the number of nodes in the network. Let $l_{\max}$ and $l_{\min}$ be the maximum and minimum route lengths in $\mathbf{R}$. Assume that there is no connection protection. Then the resilience measure is

$$\mathrm{k} = \sum_{l=l_{\min}}^{l_{\max}} \frac{2h_l}{k(k-1)} [1-(1-p)^l], \quad (6)$$

where h_l is the number of routes with l links in $\mathbf{R}$, $2h_l/k(k-1)$ is the percentage of the routes with l links, and $1-(1-p)^l$ is the probability that a connection on a route with l links is lost due to failure.

Equation (6) can be viewed as finding the expected value of function $1-(1-p)^L$ of random variable L. Since $1-(1-p)^l$ is concave in l, we can apply Jensen inequality [14] and obtain

$$\mathrm{k} \leq 1-(1-p)^{\bar{h}}, \quad (7)$$

where $\bar{h}$ is the average length of routes in $\mathbf{R}$. Then we have the following Lemma regarding the scalability of resilience:

Lemma 2: For a small probability of failure, i.e., $l_{\max} p << 1$, the resilience is

$$\mathrm{k} = \bar{h}p + o(\bar{h}p). \quad (8)$$

Next we consider 1+1 fault protection, where the traffic between two nodes is lost if there is one or more link failures at both the primary and the backup route.

Lemma 3: Let $l_{mn,1}$ and $l_{mn,2}$ be the lengths of the primary route and the backup route between nodes m and n. The resilience for networks with 1+1 connection protection is

$$\mathrm{k} = 1 - \frac{2}{k(k-1)} \sum_{m \neq n,\ m,n \in \mathbf{V}} P(S_{mn} = 0), \tag{9}$$

where $P(S_{mn} = 0) = (1-p)^{l_{mn,1}} + (1-p)^{l_{mn,2}} - (1-p)^{l_{mn,1}+l_{mn,2}}$ and means that, with 1+1 protection, the connections between node m and n is lost if there are link failures at both the primary and the backup route.

Lemma 4: For a small probability of failure, i.e., $(l_{mn,1} + l_{mn,2})^2 p^2 << 1$, $m, n \in \mathbf{V}, n \neq m$, the network resilience with 1+1 protection is

$$\mathrm{k} = \frac{2}{k(k-1)} \sum_{m,n \in \mathbf{V}, n \neq m} l_{mn,1} l_{mn,2} p^2 + o(\ ), \tag{10}$$

where $o(\ )$ is a smaller order term. Furthermore, for a large network, (10) can be simplified as

$$\mathrm{k} = \frac{2}{k^2} \sum_{m,n \in \mathbf{V}, n \neq m} l_{mn,1} l_{mn,2} p^2 + o(\ ). \tag{11}$$

The proof of Lemma 4 is based on the observation that $P(S_{mn} = 0) = 1 - l_{mn,1} l_{mn,2} p^2$ if $(l_{mn,1} + l_{mn,2})^2 p^2 << 1$. If we assume that the length of the primary and the back-up route are the same, which is reasonable for large mesh networks, (11) can be further simplified using Cauchy-Schwartz inequality as,

$$(\bar{h}p)^2 + o(\ ) \leq \mathrm{k} \leqq k^2 (\bar{h}p)^2 + o(\ ). \tag{12}$$

Comparing (12) with (8), we can find that fault protection increases the network resilience significantly and the percentage of lost traffic is reduced from $O(\bar{h}p)$ to around $O[(\bar{h}p)^2]$.

2) Regular Topologies

We now consider the resilience and the scalability of three regular topologies including ring, star, and mesh-torus for independent link failures. These are special cases of Lemma 1 and Lemma 2, where $\bar{h}$ can be obtained explicitly.

Corollary 1: For a ring network with k nodes, $k \geq 3$,

$$\mathrm{k}_{ring} = \begin{cases} 1 - \dfrac{2}{k-1}\left[\left(\dfrac{1-p}{p}\right)\left(1-(1-p)^{\frac{k-1}{2}}\right)\right], \\ \qquad\qquad \textit{if } k \textit{ odd, without protection}, \\ 1 - \dfrac{2}{k-1}\left[\left(\dfrac{1-p}{p}\right)\left(1-\left(1-\dfrac{p}{2}\right)(1-p)^{\frac{k}{2}-1}\right)\right], \\ \qquad\qquad \textit{if } k \textit{ even, without protection}, \\ 1 + (1-p)^k - \dfrac{2}{k-1}\left[\dfrac{(1-p)-(1-p)^k}{p}\right], \\ \qquad\qquad \textit{with protection}. \end{cases} \tag{13}$$

Corollary 1 can be proved using the sum of geometric series. The average route length for a ring network can be found in [11]. Thus, from Corollary 1, Lemma 2 and Lemma 4, we have the scalability of large ring networks.

Corollary 2: For large ring networks ($k >> 1$) with a small failure probability p ($kp << 1$), the resilience is,

$$\mathrm{k}_{ring} = \begin{cases} \dfrac{k}{4} p + o(kp), & \textit{without protection}, \\ \dfrac{8}{3}\left(\dfrac{k}{4} p\right)^2 + o(k^2 p^2), & \textit{with protection}. \end{cases}$$

The growth rate of the resilience is $O(kp)$ and $O(k^2 p^2)$ for ring networks with and without protection respectively. Similar approaches can be applied to star networks.

Corollary 3: For star network with k nodes, $k > 2$,

$$\mathrm{k}_{star} = p + \frac{k-2}{k}(p - p^2), \ \textit{without protection}. \tag{14}$$

Furthermore, when $k >> 1$ and $p << 1$, $\bar{h} = 2$, and

$$\mathrm{k}_{star} = 2p + o(p), \quad \textit{without protection}. \tag{15}$$

Thus, the growth rate of the percentage of lost traffic is $O(2p)$ regardless of the network size.

Next we consider the resilience of two-dimensional mesh-torus networks. Mesh-torus networks are 2-ary hypercube with edge nodes connecting to nodes on the opposite edges [12]. We can view a two-dimensional $N \times N$ mesh-torus network as a grid network with N rows and N columns. In addition, the nodes on the boundary of the grid network are connected to nodes on the opposite boundary.

For mesh-torus network of k nodes, the network diameter is $O(\sqrt{k})$ [12]. In addition, through mathematical derivation based on the sum of geometric series, we have the following Corollary:

Corollary 4: For a mesh-torus network with k nodes, and $\sqrt{k} > 3$, when $k >> 1$ and $\sqrt{k}\, p << 1$, the network resilience is

$$\mathrm{k}_{torus} = \begin{cases} \dfrac{\sqrt{k}}{2} p + o(\sqrt{k}\, p), & \textit{without protection}, \\ \dfrac{7}{24} k p^2 + o(k p^2), & \textit{with protection}. \end{cases} \tag{16}$$

The growth rate for the percentage of lost traffic are $O(\sqrt{k}\, p)$ and $O(kp^2)$ for mesh-torus networks without and with protection respectively.

3) Summaries and Discussions

The scalability of resilience of the three typical topologies under independent link failures is summarized in Table I. Specifically,

(1) When the probability of link failure (p) is small:

- Without failure protection, the resilience is determined by the average route length $\bar{h}$. Of the three topologies with the same number of nodes, the star network is the most resilient $O(2p)$ due to the shortest $\bar{h}$, whereas the ring network is the least resilience $O(kp)$ due to the longest $\bar{h}$.
- With 1+1 protection, a mesh-torus network is more resilient than a ring network $O(kp^2)$. That is because a mesh-torus network generally has shorter primary and backup routes than a ring network.
- Comparing the same topology with and without failure protection, 1+1 protection improves network resilience by an order of a magnitude as shown by the scalability results. The percentage of lost traffic due to failure decreases by a factor of $O(kp)$ and $O(\sqrt{k}\,p)$ for ring and mesh-torus networks respectively. The intuition is that the probabilities of service unavailability on the primary and backup routes are independent.

(2) When the probability of link failure (p) is large, failure protection does not significantly improve network resilience. The three topologies have similar network resilience. The reason is that both the primary and the back routes have a high probability of failure.

Table I. Scalability of Network Resilience of Ring, Star, and Mesh-Torus Network Independent Failure, Large Network **

	$p \to 0$; without protection	$p \to 1$; without protection	$p \to 0$; with protection	$p \to 1$; with protection
Ring	$O(kp)$	$1-(1-p)\frac{2}{k}$	$O(k^2p^2)$	$1-(1-p)\frac{2}{k}$
Star	$O(2p)$	$1-(1-p)\frac{2}{k}$	N/A	N/A
Mesh-Torus	$O(\sqrt{k}p)$	$1-(1-p)\frac{4}{k}$	$O(kp^2)$	$1-(1-p)\frac{4}{k}$

B. Resilience under Dependent Failure

We now study the resilience under dependent link failures.

1) Dependent Failure Models

In many scenarios, network links fail in a dependent fashion. For example, network components in a Shared Risk Link Groups (*SRLG*) in optical networks are under impacts of common risk factors such as shared conduit, shared right of way, shared switching office, and geographic proximity [17]. Conditional probabilities per *SRLG* are proposed in [17] to capture the failure dependencies. For instance, when two links L_1 and L_2 share a common conduit, each link may fail with a certain probability given the failure of the conduit.

Several dependent failure models have been proposed. For example, network failures are modeled in [15] using a birth-death process. The rate of occurrences for new failures is assumed to vary with the number of existing failures in the network, resulting in dependency among failures. A dependent failure model is presented in [3] based on Markov dependency among failures on a sequence of links. Another commonly-used model of dependent failures is given in [16] that can be represented using a bipartite graph [18][19].

In this work, we adopt the dependent failure model in [18][16]. We represent the failure model using a special type of graphical models, i.e., Bayesian Belief Network. The graphical model is probabilistically consistent, and shows the dependences among different link failures explicitly. In particular, a Bayesian Belief Network defines two types of random variables. One corresponds to the status of each network link. The other characterizes occurrences of network events that may cause one or more links to fail.

Note that most dependent link failures are among links that are incident to a common network node, as incident links share common risks of failures, e.g., sharing of network-node equipments and power. In addition, incident links are located in the same geographic areas and are subject to same abnormal events such as earthquakes and hurricanes. Thus we assume that incident links are in the same shared-risk-link group and may fail simultaneously due to a common risk.

For instance, the dependent failure model of the NSF network in Figure 1 is depicted in Figure 2. The status of each link is denoted as $Z_1, Z_2, ..., Z_{21}$. Each link may fail, i.e., $Z_i = 1$, due to two types of events. First is Event A_i that may only affect the status of *link* i, $i = 1, 2, ..., 21$. In this work, we assume that A_i occurs with probability a_i, and define random variables X_i : $X_i = 1$, if event A_i occurs; and $X_i = 0$, otherwise. Second is Event B_j that may affect the status of all the links incident at a *node* j, $j \in \mathbf{V}$. We assume B_j occurs with probability b_j, and define random variable $Y_j = 1$ if event B_j occurs; and $Y_j = 0$, otherwise.

Examples of event A_i include fiber cut or inline amplifier-failures at link i and abnormal events that only affect the geographic location of link i. a_i, which is the probability event A_i could be in the range of 10^{-4} to 10^{-8} depending on such factors as the vulnerability of the geographic location to natural disasters. Examples of events B_j include failures of the shared network equipments at the node; an abnormal event that that may affect the geographical area where the node is located such as power failure, natural disasters; and intentional/unintentional damage of the node. Event B_{i_1} occurs with probability b_{i_1}, which can be in the same range of a_i, i.e., 10^{-4} to 10^{-8} [10].

Now consider link i in the network and denote the two end nodes of link i as node i_1 and node i_2. Then the status of link i can be affected by event A_i, event B_{i_1}, and event B_{i_2}. For simplicity, we assume that the three events cause link i to fail independently of each other. Furthermore, let $p_{ai} = P(Z_i = 1 \mid X_i = 1, Y_{i_1} = 0, Y_{i_2} = 0)$, which denotes the probability that event A_i causes link i to fail given the

occurrence of event A_i and nonoccurrence of event B_{i_1} and event B_{i_2}. Let $p_{b,ii_1} = P(Z_i = 1 | X_i = 0, Y_{i_1} = 1, Y_{i_2} = 0)$, which denotes the probability that event B_{i_1} cause link i to fail given the occurrence of B_{i_1} and nonoccurrence of A_i and B_{i_2}. Similarly, we let $p_{b,ii_2} = P(Z_i = 1 | X_i = 0, Y_{i_1} = 0, Y_{i_2} = 1)$.

Conditional probabilities p_{a_i}, $p_{b,i\,i_1}$, and $p_{b,i\,i_2}$ are in the range of 0 to 1 depending on the severalty of the risk events.

Assuming that the risk events occur independently of each other, we have the following conditional probabilities for the dependent failure model in Figure 2,

$$P(Z_i = 1 | X_i, Y_{i_1}, Y_{i_2}) = 1 - (1 - p_{ai})^{X_i} (1 - p_{b,i\,i_1})^{Y_{i_1}} (1 - p_{b,i\,i_2})^{Y_{i_2}}, \quad (17)$$

$$P(Z_i = 1) = 1 - (1 - a_i p_{ai})(1 - b_{i_1} p_{b,i\,i_1})(1 - b_{i_2} p_{b,i\,i_2}), \quad (18)$$

where $1 \le i \le 21$. For simplicity of analysis, we assume that $a_i \equiv a$, $b_j \equiv b$, $p_{a\,i} \equiv p_a$, and $p_{b,ii_1} = p_{b,ii_2} \equiv p_b$ for the rest of this work. Note that node failures are characterized implicitly in our dependent model of link failures. A failure at node j is a special case of the dependent failure model that corresponds to event B_j with P_b=1.

2) Arbitrary Topology

We now quantify the network resilience and scalability with dependent failure and without failure protection.

Theorem 1: Let j be the number of links on route r_{mn}, with dependent failures and without failure protection,

$$P(S_{mn} = 0) = (1 - ap_a)^j (1 - bp_b)^2 (1 - b(2p_b - p_b^2))^{j-1}. \quad (19)$$

The proof of Theorem 1 can be found in Appendix *I*.

Consider a special case that $p_b = 1$. This means that the occurrence of event $B_i, i \in \mathbf{V}$, causes all the links incident of node i to fail. We can further simplify Equation (19) and obtain the following corollary.

Corollary 5: For small failure probabilities, i.e., $jap_a << 1$ and $jbp_b << 1$, and without failure protection,

$$k_{dep} = \bar{h} p_e + bp_b^2 + o(), \quad (20)$$

where $p_e = ap_a + 2bp_b - bp_b^2$ is denoted as effective link failure probability. In addition, for a large network ($\bar{h} >> 1$),

$$k_{dep} = \bar{h} p_e + o(), \quad (21)$$

which shows that the growth rate of the percentage of lost traffic is $O(\bar{h} p_e)$.

In the expression for p_e, ap_a is the probability that an event A cause the loss of connections on the route; $2bp_b - bp_b^2$ is the probability that an event of type B cause the loss of connections on the route. Hence $p_e = ap_a + 2bp_b - bp_b^2$ can be considered as the probability that a pair of event *A* and *B* cause the loss of connections on the route.

For comparison, when failures were assumed independent, $P(S_{mn} = 0)$ is overestimated by a factor of

$$\frac{(j-1)b}{jap_a + (j+1)b}, \quad \text{if } jap_a << 1 \text{ and } jb << 1. \quad (22)$$

In addition, the independent-failure assumption results in

$$k = \bar{h}(ap_a + 2bp_b). \quad (23)$$

Hence, the failure independent assumption overestimates the percentage of lost traffic by a factor of $\frac{(\bar{h}-1)bp_b^2}{\bar{h}p_e - bp_b^2}$. Clearly, the independent model of failures is a special case of the dependent model with $b = 0$ for all events $B_i, i \in \mathbf{V}$, which means that no event would cause two network links to fail simultaneously.

Therefore, the independent-failure assumption overestimates the percentage of lost traffic by a factor between 0 and 1. The lower limit is achieved if all the connections in the network are of link length 1. In this case, the failure independent assumption does not affect the evaluation of network resilience. The failure independent assumption overestimate the percentage of lost traffic by a factor close to 1 if $a << b$, $p_b >> 0$, and $\bar{h} >> 1$.

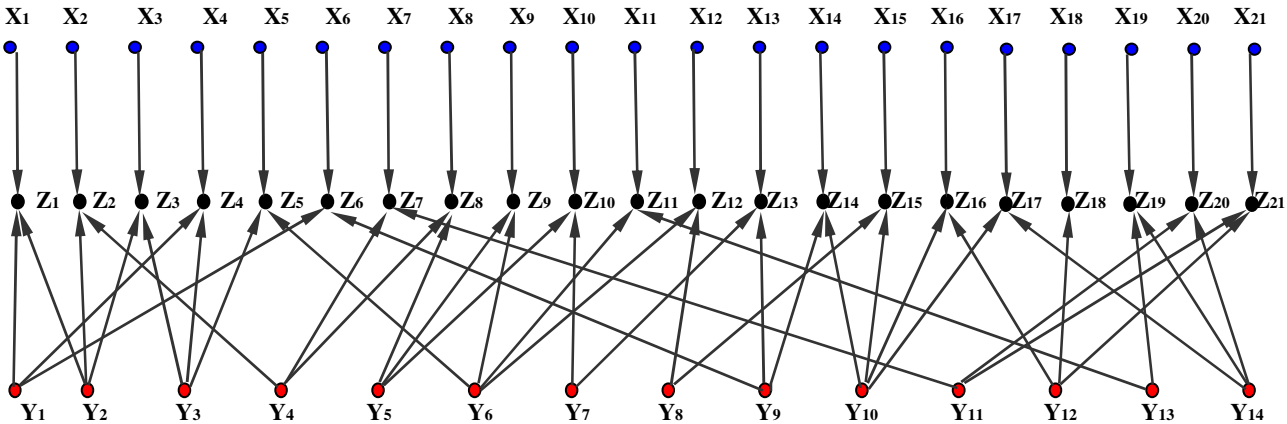

Figure 2. Bayesian Belief Network representation of dependent failure models for NSF network

The above analysis results the following corollary on resilience of network topologies.

Corollary 6: Without failure protection, for small failure probabilities, i.e., $jap_a << 1$ and $jbp_b << 1$, of all the physical topologies with the same number of nodes in the network, the fully-connected graph is the most reliable; of all the physical topologies with the same number of nodes and links in the network, the Moore graph is the most reliable.

Note that a Moore graph is a regular graph of degree *d* and diameter *h* whose number of vertices satisfies the following upper bound: $1+d\sum_{i=0}^{h-1}(d-1)^i$ [13]. Thus, for regular topologies with the same number of nodes and links, a Moore graph has the minimum average shortest route between each pair of nodes [13]. The results in Corollary 6 complement the finding in [3] which shows that the Moore graph has the best *all-terminal* reliability, when the link failure probability is low and all failures are independent.

Next, we consider network resilience and the scalability with dependent failure and with protection. Without loss of generality, we consider an active connection on the primary route between node *m* and *n* in **R** with j_1 links, while its backup route has j_2 links.

Theorem 2: When the probability of failure is small ($j_1 j_2 a^2 << 1$ and $j_1 j_2 abp_a << 1$), we have

$$P(S_{mn}=1) = 2bp_b^2 + j_1 j_2 p_e^2 + o(\ ). \qquad (24)$$

The proof of Theorem 2 is similar to that of Theorem 1 in Appendix I. Details are omitted. Similar to the derivation of (12), it can be shown that, with dependent failure and 1+1 protection, assuming that the primary route and the backup route have the same number of links,

$$2bp_b^2 + (\bar{h}p_e)^2 + o(\ ) \le \mathrm{k}_{dep} \le 2bp_b^2 + k^2(\bar{h}p_e)^2 + o(\ ), \qquad (25)$$

For comparison, with failure independent assumption, the probability that connections between nodes *m* and *n* are lost due to failures on both its primary and backup route is $j_1 j_2 p^2 + o(\ )$, where $p = ap_a + 2bp_b + o()$ is the marginal link failure probability

Thus, with fault protection, the failure independent assumption may underestimate the probability that the connection loss significantly. Specifically, when $j_1 j_2 a^2 << 1$ and $b << 1$, the failure independent assumption underestimates the probability that traffic on the route between node *m* and *n* is lost by a factor of $\frac{2bp_b^2 - j_1 j_2 (p^2 - p_e^2)}{2bp_b^2 + j_1 j_2 p_e^2}$. If $a = O(b)$, the independent assumption underestimates the percentage of lost traffic by a factor of $1 - O(bp_b)$. Furthermore, with dependent failures, failure protection helps the most when an event that may cause several links fail simultaneously occurs with a small probability, i.e., *b* is small.

3) Typical Topologies

We now consider ring, star, and mesh-torus networks with dependent failures and without protection. From Theorem 1, we have the following corollaries.

Corollary 7: For a ring network with *k* nodes, $k > 3$,

$$\mathrm{k}_{dep,ring} = \begin{cases} 1 - \frac{2(1-bp_b)^2}{(k-1)(1-2bp_b+bp_b^2)}\left[\left(\frac{1-q}{q}\right)\left(1-(1-q)^{\frac{k-1}{2}}\right)\right], & k\ odd, \\ 1 - \frac{2(1-bp_b)^2}{(k-1)(1-2bp_b+bp_b^2)}\left[\left(\frac{1-q}{q}\right)\left(1-\left(1-\frac{q}{2}\right)(1-q)^{\frac{k}{2}-1}\right)\right], & k\ even, \end{cases} \qquad (26)$$

where $q = 1-(1-ap_a)(1-2bp_b+bp_b^2)$.

For comparison, the marginal probability of link failures $p = 1-(1-ap_a)(1-2bp_b+b^2p_b^2)$. In addition, we have

Corollary 8: For small probabilities of events *A* and *B*, ($kap_a << 1$, $kbp_b << 1$), and a large network ($k >> 1$), without failure protection,

$$\mathrm{k}_{dep,ring} = \frac{k}{4}p_e + o(kp_e)\ , \qquad (27)$$

where $p_e = ap_a + 2bp_b - bp_b^2$ is from corollary 5.

This shows that the growth rate of the percentage of lost traffic for the ring network is $O(kp_e)$.

Corollary 9: For star network with *k* nodes, $k \ge 3$,

$$\mathrm{k}_{dep,star} = 1 - \frac{(1-bp_b)^2}{k(1-2bp_b+bp_b^2)}\{2(1-q)+(k-2)(1-q)^2\}, \qquad (28)$$

where $q = 1-(1-ap_a)(1-2bp_b+bp_b^2)$.

In addition, for large star network, we have:

Corollary 10: For small probabilities of event *A* and *B* ($ap_a << 1, bp_b << 1$), and a large network, i.e., $k >> 1$, without protection, the network resilience is

$$\mathrm{k}_{dep,star} = 2p_e + o(p_e)\ , \qquad (29)$$

which shows that the growth rate of the percentage of lost traffic for the star network is $O(2p_e)$.

Corollary 11: For a mesh-torus network with *k* nodes, and $\sqrt{k} > 3$, when $k >> 1$ and $\sqrt{k}\,p << 1$, $\bar{h} = \frac{\sqrt{k}}{2}$ for *k* odd, and $\bar{h} = \frac{k^{3/2}}{2(k-1)}$ for *k* even. Hence, the network resilience is

$$\mathrm{k}_{dep,torus} = \frac{\sqrt{k}}{2}p_e + o(\sqrt{k}\,p_e)\ . \qquad (30)$$

Thus, the growth rate of the percentage of lost traffic is $O(\sqrt{k}\,p_e)$ for mesh-torus networks without with protection.

Furthermore, a rule of thumb is that independent assumption overestimates the percentage of lost traffic by a factor of $\frac{(\bar{h}-1)bp_b^2}{\bar{h}p_e^2 - bp_b^2}$ for large networks, when the probability of failure is small and there is no failure protection.

Next, we consider the resilience of ring and mesh-torus networks with dependent failure and 1+1 protection.

***Corollary 12*:** For ring network with k nodes, $k > 2$, if $k^2a^2p_a^2 << 1$, and $k^2abp_ap_b << 1$,

$$\mathrm{k}_{dep,ring} = 2bp_b + \frac{k^2p_e^2}{6} + o(k^2p_e^2), \qquad (31)$$

which shows that the growth rate of the percentage of lost traffic for the ring network is $O(2b + k^2p_e^2)$.

***Corollary 13**:* For a mesh-torus network with k nodes, and $\sqrt{k} > 3$, when $k >> 1$ and $kabp_ap_b << 1$,with dependent failure and 1+1 protection, the network resilience is

$$\mathrm{k}_{dep,torus} = 2bp_b + \frac{7}{24}kp_e{}^2 + o(kp_e{}^2), \qquad (32)$$

which shows that growth rate for the percentage of lost traffic for the mesh-torus network is $O(2bp_b + kp_e{}^2)$.

4) Summary

In this section, we have adopted uniform deterministic traffic to study the effects of physical topologies, failure protection, and dependencies among physical layer failures on network resilience and the scalability. The results are as shown in Table II. For uniform deterministic traffic, we have the following findings when the probability of link failure (*p*) is small.

(1) The impact of physical topologies:

- Without protection, the network resilience is determined by the average route length. Thus, the mesh-torus network is the most reliable of the three topologies due to its smaller network diameter O($\sqrt{k}$).
- With protection, the network resilience is determined by the network diameter if the link failures are independent; and is determined by both the network diameter and the probability of occurrence for events that may cause several links to fail simultaneously, i.e., value of *b*.

(2) The impact of failure protection:

- When link failures are independent, the percentage of lost traffic generally is reduced from $O(p)$ to $O(p^2)$. Hence failure protection can imp*r*ove the network significantly.

When failures are dependent, the percentage of lost traffic increases linearly with bp_b. Hence it is important to reduce the probability of occurrence for events that may cause several links fail simultaneously.

(3) The impact of failure dependencies

- Without protection, the failure independent assumption overestimates the percentage of lost traffic roughly by a factor of $(\bar{h}-1)bp_b^2 / (\bar{h}p_e^2 - bp_b^2)$.
- With protection, the failure independent assumption underestimates the probability of lost traffic on a route by a factor of $\frac{2bp_b - j_1j_2(p^2 - p_e^2)}{2bp_b + j_1j_2p_e^2}$. The underestimation is $1 - O(b)$, if $a = O(b)$, which implies that the percentage of lost traffic derived with failure independent assumption is a magnitude smaller than the actual value.

Table II Scalability of resilience for large ring, star, and mesh-torus network; uniform deterministic traffic; small probability of link failure

	Ring	Star	Mesh-Torus
Independent failure; without protection	$O(kp)$	$2p$	$O(\sqrt{k}\,p)$
Dependent failure; without protection	$O(kp_e)$	$2p_e$	$O(\sqrt{k}\,p_e)$
Independent failure; with protection	$O(k^2p^2)$	N/A	$O(kp^2)$
Dependent failure; with protection	$2bp_b + O(k^2p_e^2)$	N/A	$2bp_b + O(kp_e^2)$

V. Resilience under Uniform Random Traffic

We now consider uniform *random* traffic to study the impact of network layer traffic on resilience. We assume that each link j in **E** has capacity C and the network uses fixed routing on a set of routes **R**. Without fault protection, **R** consists of one link-shortest route between each pair of nodes in the network. With 1+1 protection, **R** consists of two link-disjoint routes between each pair of nodes in the network, at least one of which is a link-shortest route.

For simplicity of analysis, we assume that connection requests between each pair of nodes in the network arrive as a Poisson process with rate v and each connection requires one unit of link capacity. Connection requests are blocked if there is no free capacity on the corresponding route. The holding time of each accepted connection is an independent and identically distributed (*i.i.d*) exponential random variable with unit mean. Then, it has been shown in [8] that, in the equilibrium state, the stationary distribution of the number of connections in progress in the network is

$$\pi(\mathbf{N}) = Z^{-1}\prod_{r\in\mathbf{R}}\frac{v^{N_r}}{N_r!}, \quad \mathbf{N}\in \mathrm{S}, \qquad (33)$$

where N_r is the number of connections on route r, and $\mathbf{N} = (N_r : r \in \mathbf{R})$; S is the set of vector **N** that satisfies the link capacity constraint. The stationary distribution in (33) is

intractable due to the difficulty to derive the normalization constant Z.

Erlang Fixed Point Approximation (EFPA) [8] has been shown both theoretically and empirically to be an effective approximation to the stationary distribution in (33). In particular, for the network layer model in (33), there always exist a unique fixed-point solution which is asymptotically correct [8]. Empirically, EFPA performs well especially for networks with large link capacities and/or networks with non-linear structure. Thus, we use the Erlang Fixed Point Approximation [8] to analyze the resilience.

A. *Cross-Layer Graphical Model*

The coupling of physical layer failure with network layer traffic can be represented explicitly through a cross-layer probabilistic graphical model. The graph has one additional layer to include the randomness of network traffic compared with that in Figure 2. We assume N_r large so that $N_r \sim \sqrt{2\pi} N_r^{N_r+0.5} e^{-N_r}$ due to Stirling formula [14]. Then

$$\pi(\mathbf{N}) = W^{-1} \exp\{\sum_{r\in R} N_r (1 + \ln v - \ln N_r)\}, \quad \mathbf{N} \in \mathrm{S.},$$

where W is the normalization constant.

Using the Gibbs distribution for network-layer traffic [8] and combining network layer traffic with the physical layer failures, the cross-layer graphical model can be obtained. Figure 3 depicts an example of the graphical representation for the NSF network in Figure 1 with only 5 routes in **R**. In Figure 3, the upper part of the representation correspond to the network layer model, where all the network routes that share a common link at the physical layer form a fully-connected graph (clique). The lower part of the representation represents the physical layer dependent failures. The network layer model characterizes the number of active connections on each route. Meanwhile, the physical layer model describes the status of each link. Combining the two layers, we can obtain the information on the number of connections lost on each route due to failures. Detailed explanations of cross-layer model representations can be found in [21].

The impact of network layer traffic is on $E[D_{ij}]$'s as in

$$\mathbf{Z} = \sum_{ij} E[D_{ij}]E[S_{ij}], \tag{34}$$

$$\mathrm{k} = \frac{\sum_{ij} E[D_{ij}]E[S_{ij}]}{\sum_{ij} E[D_{ij}]}, \tag{35}$$

where $E[D_{ij}]$ is the expected number of active connections between nodes i and j. $E[S_{ij}]$'s remain the same as those for deterministic traffic, hence it suffices to evaluate $E[D_{ij}]$'s.

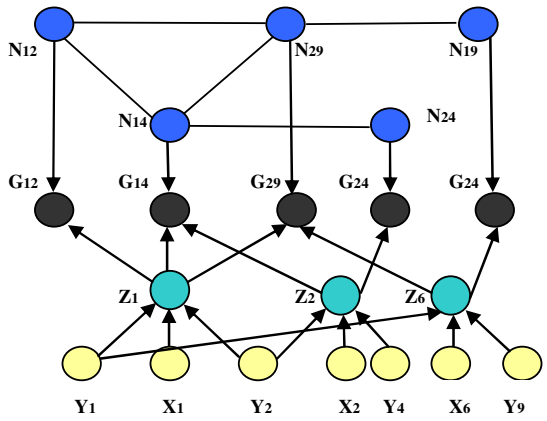

Figure 3. Cross-Layer Graphical Representation of the NSF Network with 5 routes in Figure 1; *Nij* denotes the number of active connections on route *ij*; *Gij* denotes the number of connections lost on route *ij* due to failures.

B. *Independent Failure and Without Protection*

We first focus on the resilience of Ring and Star topologies with independent failure and without protection.

1) *Ring Topologies*

Lemma 5*:* For a k - node ring network, $k \geq 3$,

$$E[D_{ij}] = v(1 - B_{ring})^{d_{ij}}, \tag{36}$$

where d_{ij} is the number of links traversed by route R_{ij}; B_{ring} is the link blocking probability obtained from the fixed point equations using EFPA,

$$B_{ring} = Erlang(\rho_{ring}, C) = \frac{\rho_{ring}^C}{C!} \Big/ (\sum_{i=0}^{C} \frac{\rho_{ring}^i}{i!}), \tag{37}$$

$$\rho_{ring} = \begin{cases} \dfrac{v\{1 - \frac{k+1}{2}(1-B_{ring})^{\frac{k-1}{2}} + \frac{k-1}{2}(1-B_{ring})^{\frac{k+1}{2}}\}}{B_{ring}^2}, & k \text{ odd}, \\ \dfrac{v\{1 - \frac{k}{2}(1-0.5B_{ring}^2)(1-B_{ring})^{\frac{k}{2}-1} + (\frac{k}{2}-1)(1-B_{ring})^{\frac{k}{2}}\}}{B_{ring}^2}, & k \text{ even}. \end{cases} \tag{38}$$

Theorem 3*:* Combining $E[D_{ij}]$ and $E[S_{ij}]$, we have

$$\mathbf{Z}_{ring} = \begin{cases} kv\{\dfrac{(1-B_{ring})p - (1-B_{ring})^{\frac{k+1}{2}}(B_{ring} + p - B_{ring}p - B_{ring}(1-p)^{\frac{k+1}{2}})}{B_{ring}(B_{ring} + p - B_{ring}p)}\} & k \text{ odd}, \\ kv\{\dfrac{(1-B_{ring})p - (1-B_{ring})^{\frac{k}{2}}(B_{ring} + p - B_{ring}p - B_{ring}(1-p)^{\frac{k}{2}})}{B_{ring}(B_{ring} + p - B_{ring}p)}\} & \\ \quad + 0.5kv(1-B_{ring})^{\frac{k}{2}}(1-(1-p)^{\frac{k}{2}}), & k \text{ even}, \end{cases} \tag{39}$$

$$\mathrm{k}_{ring} = \begin{cases} 1-\dfrac{B_{ring}\{(1-B_{ring})(1-p)-(1-B_{ring})^{\frac{k+1}{2}}(1-p)^{\frac{k+1}{2}}\}}{(B_{ring}+p-B_{ring}p)\{(1-B_{ring})-(1-B_{ring})^{\frac{k+1}{2}}\}}, \\ \qquad k \text{ odd}, \\ 1-\dfrac{B_{ring}\{(1-B_{ring})(1-p)-(1-B_{ring})^{\frac{k}{2}}(1-p)^{\frac{k}{2}}(1-0.5(B_{ring}+p-B_{ring}p))\}}{(B_{ring}+p-B_{ring}p)\{(1-B_{ring})-(1-B_{ring})^{\frac{k}{2}}(1-0.5B_{ring})\}}, \\ \qquad k \text{ even}, \end{cases} \tag{40}$$

where k_{ring} denotes the average percentage of lost traffic due to failures in the ring network. Theorem 3 can be obtained using the sum of series. Details are omitted here.

Corollary 14: When the probability of link failures is small ($kp << 1$),

$$\mathrm{k}_{ring} = \begin{cases} p\times\dfrac{1-(1-B_{ring})^{\frac{k-1}{2}}(1+\dfrac{k-1}{2}B_{ring})}{(B_{ring}+p-B_{ring}p)(1-(1-B_{ring})^{\frac{k-1}{2}})}, \ k \ odd \\ p\times\dfrac{1-(1-B_{ring})^{\frac{k}{2}-1}\{1+(\dfrac{k}{2}-1)B_{ring}+0.25kB_{ring}(B_{ring}+p-B_{ring}p)\}}{(B_{ring}+p-B_{ring}p)(1-(1-B_{ring})^{\frac{k}{2}-1}(1-0.5B_{ring}))} \\ \qquad , \ k \ even. \end{cases} \tag{41}$$

To obtain insights, we consider a special case of light load.

Corollary 15: When the load is light, i.e., the blocking probability is small ($kB_{ring} << 1$), Equation (41) can be simplified as

$$\mathrm{k}_{ring} = \frac{k}{4}p + o(p) + o(B_{ring}) . \tag{42}$$

This reduces to the case for the deterministic traffic.

For the heavy load i.e., $\rho >> C$, we have the following:

Theorem 4*:* For a k - node ring network with independent failure and without failure protection, under heavy load, ($v >> 1$)

$$B_{ring} = 1-\frac{C-1}{v+1}, \tag{43}$$

$$\mathbf{Z}_{ring} = k(C-1)p + o(\frac{C^2 p}{v}), \tag{44}$$

$$\mathrm{k}_{ring} = p + o() . \tag{45}$$

The proof of Theorem 4 can be found in *Appendix II*. Equation (43) shows that, under heavy load, the link blocking probability under EFPA approaches 1. Thus almost all the active connections are of link length 1. Therefore, the expected number of lost connections due to failures approaches $k(C-1)p$ and the expected percentage of lost connections due to failures approaches p.

Next we consider the resilience of the ring network with independent failure and 1+1 failure protection. Now the capacity needs to be allocated to both the primary and the backup route. For a ring network, each connection request always requires capacity from k links regardless of the source and destination. This means that we can use Corollary 1 and 2 to evaluate the resilience of the ring network.

Theorem 5: For a ring network with k nodes, and 1+1 protection,

$$\mathbf{Z} = kv(1-B_{ring,p})[1+(1-p)^k - \frac{2}{k-1}(\frac{(1-p)-(1-p)^k}{p})], \tag{46}$$

where $B_{ring,p} = Elrang(\dfrac{k(k-1)}{2}v, C)$.

$$\mathrm{k}_{ring} = 1+(1-p)^k - \frac{2}{k-1}\frac{(1-p)-(1-p)^k}{p}. \tag{47}$$

It can be observed that (47) has the same form (13). Thus, under the uniform random network model, the resilience and thus the scalability of the ring network with protection have the same forms as those under the uniform deterministic traffic, because the expected number of connections between each pair of nodes remains the same.

2) Star Topologies

We now consider the resilience of star networks with independent failures and without failure protection.

Lemma 6: For star network with k nodes, $k > 2$,

$$E[D_{ij}] = v(1-B_{star})^{d_{ij}} , \tag{48}$$

where d_{ij} is the number of links traversed by route R_{ij} ; B_{star} is the link blocking probability of the star network obtained from the EFPA, and

$$B_{star} = Erlang(\rho_{star}, C) = \frac{\rho_{star}^C}{C!}(\sum_{i=0}^{C}\frac{\rho_3^i}{i!}), \tag{49}$$

$$\rho_{star} = v(k-1-(k-2)B_{star}). \tag{50}$$

Theorem 6: For the star network,

$$\mathbf{Z}_{star} = v(k-1)(1-B_{star})\{p+0.5(k-2)(1-B_{ring})(2p-p^2)\}, \tag{51}$$

$$\mathrm{k}_{star} = \frac{p+0.5(k-2)(1-B_{ring})(2p-p^2)}{1+0.5(k-2)(1-B_{ring})}. \tag{52}$$

Corollary 16: When the probability of link failure is small ($p << 1$),

$$\mathbf{Z}_{star} = (k-1)vp(1-B_{star})(1+(k-2)(1-B_{ring})) + o( ), \tag{53}$$

$$\mathrm{k}_{star} = \frac{1+(k-2)(1-B_{ring})}{1+0.5(k-2)(1-B_{ring})}p + o(p). \tag{54}$$

In addition, when k is large ($k >> 1$),

$$\mathrm{k}_{star} = \frac{1+k(1-B_{ring})}{1+0.5k(1-B_{ring})}p + o(). \tag{55}$$

Furthermore, when the non-blocking probability $1-B_{ring}=O(1)$, $\mathrm{k}_{star}=2p+o(\,)$.

Thus, for a large star network with a small probability of link failure and a moderate blocking probability, the scalability of the resilience is of the same order as that for uniform deterministic traffic. Next we consider the case that the network blocking probability is large.

Theorem 7: For a k - node star network with independent link failure and without failure protection, under heavy load, $(v>>1)$,

$$\mathbf{Z}_{star}=(k-1)Cp+o(\frac{C^2p}{v}), \tag{56}$$

$$\mathrm{k}_{star}=p+o(\,). \tag{57}$$

The proof of Theorem 7 is similar to that of Theorem 4 and details are omitted here. Equations (56) and (57) show that, under heavy load, the expected number of lost connections due to failures approaches $(k-1)Cp$ and the expected percentage of lost connections due to failures approaches p for the star network with uniform random traffic. It can be observed, under high load, the percentage of lost traffic due to failure is twice of that under light load. The reason is that under high load, most of the active connections in the network are on the routes with only one link; whereas under light traffic, there are almost the same number of active connections on each route due to the uniform connection arrival rate.

C. Dependent Failure

We now focus on the network resilience with dependent failure and without failure protection. Here, $E[S_{ij}]$'s can be obtained from (20), and $E[D_{ij}]$'s can be obtained from Subsection V.B.

1) Arbitrary Topologies

Let $l_{ij}\ \forall\, i,j\in\mathbf{V}$ be the length of the route between node i and j. For small failure probability $l_{ij}p<<1,\forall\, i,j\in\mathbf{V}$ and without failure protection, we have from Corollary 5 that

$$E[S_{ij}]=l_{ij}p_e+bp_b^2, \tag{58}$$

$$\mathbf{Z}_{dep}=\sum_{ij}[l_{ij}p_e+bp_b^2]E[D_{ij}], \tag{59}$$

$$\mathrm{k}_{dep}=\frac{\sum_{ij}[l_{ij}p_e+bp_b^2]E[D_{ij}]}{\sum_{ij}E[D_{ij}]}, \tag{60}$$

Furthermore, when there is 1+1 failure protection with small failure probabilities ($l_{ij,1}l_{ij,2}a^2p_a^2<<1$, $l_{ij,1}l_{ij,2}abp_ap_b<<1$),

$$\mathbf{Z}_{dep}=\sum_{ij}\{2bp_b+l_{ij,1}l_{ij,2}p_e^2\}E[D_{ij}], \tag{61}$$

$$\mathrm{k}_{dep}=\frac{\mathbf{Z}_{dep}}{\sum_{ij}E[D_{ij}]}. \tag{62}$$

2) Numerical Results

We now study the network resilience with dependent failures and without protection using numerical approach. Our goals are to verify and assess our scalability results in real networks of mesh topology. We consider the percentage of lost traffic due to failures for three networks: a 14 node ring network, the 14 node NSF network and a random-graph topology [20].

Figure 4 depicts the percentage of lost traffic vs. the connection arrival rate for the 14 node ring and NSF networks. The numerical results are obtained using Erlang-Fixed Point Approximation. Each network link is assumed to have capacity 20. The following parameters are used for dependent failure model: event A_i occurs with probability $a=10^{-4}$; the occurrence of event A_i cause link i to fail with probability $p_a=0.5$; event B_i occurs with probability $b=10^{-4}$; the occurrence of event B_i cause all the links incident on node i fail with probability $p_b=1.0$. The corresponding marginal probability of link failure is $p=2.5\times10^{-4}$. This set of model parameters corresponds to a high probability of link failure.

Figure 5 depicts the percentage of lost traffic vs. the connection arrival rate for the same two networks. Each network link is assumed to have capacity 20. A different set of parameters are used for dependent failure model: event A_i occurs with probability $a=10^{-6}$; the occurrence of event A_i cause link i to fail with probability $p_a=0.5$; event B_i occurs with probability $b=10^{-6}$; the occurrence of event B_i cause all the links incident on node i fail with probability $p_b=1.0$. The corresponding marginal probability of link failure is $p=2.5\times10^{-6}$. This set of failure model parameters corresponds to a small probability of link failure.

It can be found that the failure independent assumption overestimates the percentage of lost traffic due to failures for both networks. Furthermore, the magnitude of the overestimation is smaller when the network is under smaller load, i.e., with smaller connection arrival rate. Specifically, the percentage of overestimation is 39.5% for the ring network from Figure 3 and Figure 4. Using the rule of thumb, we can obtain that the overestimation is around 41.6% for 14-node ring networks under light load as its average route length is 3.77. The percentage of overestimation is 26.8% for the NSF network from Figure 3 and Figure 4. Based on the rule of thumb, we can find that the overestimation is around 26.9% as its average route length is 2.13. Thus, our rule of thumb in (58) to (60) is accurate.

The magnitude of over-estimation approaches 0 when the network is under extreme high load. The reason is, when the network is under extremely highly load, most of the connections in the network are of link length 1 due to the high link blocking probability. In that case, the failure independent assumption does not overestimate the percentage of lost traffic. In addition, it can be observed that, as the network load increases, the percentage of lost traffic in both networks

approaches p (the marginal probability of link failure), which confirms Theorem 1.

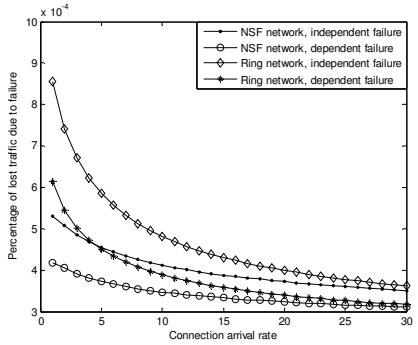

Figure 4. Percentage of lost traffic vs. connection arrival rate; 14-node ring and NSF networks; $a = 10^{-4}, p_a = 0.5, b = 10^{-4}, p_b = 1, C = 20.$

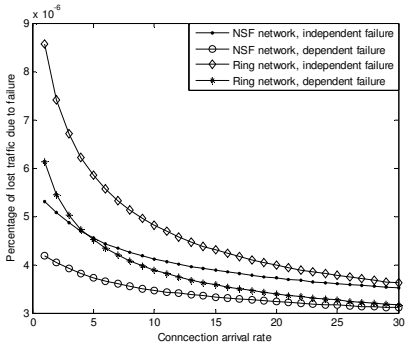

Figure 5. Percentage of lost traffic vs. connection arrival rate; 14-node ring and NSF networks; $a = 10^{-6}, p_a = 0.5, b = 10^{-6}, p_b = 1.0, C = 20.$

Figure 6 depicts the percentage of lost traffic vs. network diameter for a 200-node random graph with no protection. To focus on the effect of network diameter, we assume a uniform deterministic traffic model in Figure 6, which is equivalent to the uniform random traffic model under light load. To generate a random graph with a specific network diameter, we randomly assign a link between each pair of nodes with a fixed probability p_r, with a smaller p_r corresponds to a larger network diameter. As p_r decreases, the random graph may become disconnected. Thus, in order to maintain the connectivity of the random graph, the largest network diameter used in our study of the random graph is around 3.5. It can be observed that the rule of thumb discussed in Section IV is accurate in finding the network resilience. The error of the approximation is less than 1% of the exact value, with the large approximation errors correspond to large network diameters. In addition, the percentage of lost traffic in the random graph grows linearly with the network diameter ($\bar{h}$) as discussed in Corollary 5.

Figure 7 depicts the percentage of lost traffic vs. the link failure probability p for a 200-node random graph network with network diameter $\bar{h} = 2.104$. We can find that: (1) with independent failure, the percentage of lost traffic increases linearly with p, where $p = ap_a + 2bp_b + o(.)$; (2) with dependent failure, the percentage of lost traffic increase linearly with both p and p_e, due to the fact that the ratio between p and p_e remains a constant in Figure 6 and $p_e = ap_a + 2bp_b - bp_b^2$; and (3) the failure independent assumption overestimates the percentage of lost traffic by a factor of $\frac{(\bar{h}-1)bp_b^2}{\bar{h}p_e^2 - bp_b^2}$, which is 25.9% in this case. In Figure 6, the approximation methods also provide accurate estimation of the resilience, with the error less than 4% of the exact value, with the largest estimation error occurs at $p = 0.025$.

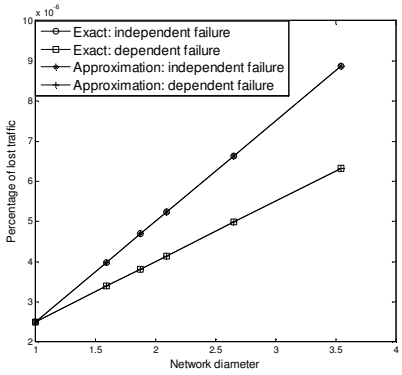

Figure 6. Percentage of lost traffic vs. Network diameter; 200-node random graph; $a = 10^{-6}, p_a = 0.5, b = 10^{-6}, p_b = 1.0.$

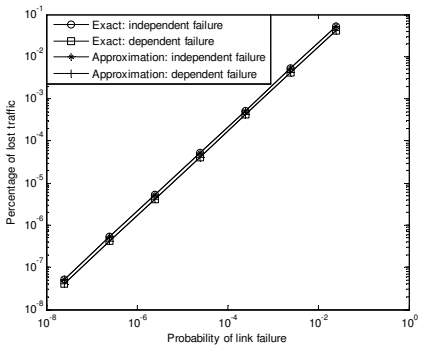

Figure 7. Percentage of lost traffic vs. Probability of link failure p; 200-node random graph; $\bar{h} = 2.104, a = b, p_a = 0.5, p_b = 1.0.$

VI. Conclusions

In this work, we have defined and investigated the scalability of network resilience in terms of multiple factors as physical topologies, failure probabilities, protection schemes, and network traffic. For large networks, with small probabilities of failures, uniform traffic, and without protection, we have proved that the scalability of network resilience are $O(\bar{h}p_e)$, where $\bar{h}$ is the average route length that depends on a physical topology and network traffic, and p_e is defined as the effective link failure probability. When all-to-all traffic is considered, $\bar{h}$ reduces to the physical network diameter. p_e is determined by failure probabilities, failure dependency, and protection schemes. When link failures are independent and 1+1 protection is used, p_e is generally reduced from $O(p)$ to

$O(p^2)$. When failures are dependent, p_e increases linearly with bp_b.

We have also considered initially random network traffic with Poisson arrivals to further investigate the effect of routes on the resilience and its scalability. We have found that: (1) when the network is under light load, the resilience of the network reduced to that under uniform deterministic traffic, and (2) when the network is under high load so that most of the active connections are on short routes, the percentage of lost traffic approaches its upper bound *p*, which is the marginal probability for link failure. More realistic traffic models can be incorporated for further studies of traffic and failures.

In view of methodology, three steps have been used in our derivation of the scalability results. First is a measure of resilience (metric) which is a function of network-wide quantities such as physical topology, traffic, failure probabilities and dependencies, and a protection scheme. Second is a definition of scalability as the "rate" of the resilience metric with respect to the multiple factors. Third is an application of probabilistic graphical models that illuminate the dependencies across physical- and network-layers, as well as expansions which attend the growth rate for large networks.

Three main assumptions have been used in our methods: (1) Fixed routing, (2) asymptotic analysis for large networks, and (3) standard topologies used for analysis and testing. The first two assumptions result in the simple expression $O(\bar{h}p_e)$ but do not consider how dynamic network control responds to failures. The third assumption allows derivations of network diameter $\bar{h}$, but has not considered a class of recently studied topologies that exhibit a strong component of network design [23]. Hence future studies may be carried out to extend resilience and scalability to dynamic networks with practical topologies.

In view of practical utility, our investigation represents an initial step in understanding how network resilience varies with multiple factors from both the physical and the network layer. Our results show that it is imperative to reduce network diameter (average minimum-hop distance) and the effective link failure probability. In addition, to decrease effective link failure probability and improve the efficiency of failure protection, it is important to reduce the occurrence of events that may cause several links to fail simultaneously. As these findings are intuitive, the scalability (rate) quantifies the intuition and shows how much each factor affects the resilience. These findings are especially meaningful for resilient design of circuit-switched networks, long-haul optical networks with flow switching, and Generalized MPLS networks, where network traffic usually can be modeled with a Poisson traffic model. However, Poisson traffic models often fail to characterize the burstiness and self-similarity of packet-switched networks such as the Internet traffic [22]. Hence, more sophisticated traffic models are needed so that a better understanding can be obtained on service disruptions upon failures.

Finally, as 1+1 protection is studied in our analysis, other schemes, e.g. 1+N protection and dynamic restoration [7] can be future directions of study. Another interesting topic is to consider how link failure probability may vary depending on the load in the network, where cross-layer graphical models as discussed in Section V. A can be potentially applied [21].

APPENDIX I
Proof of Theorem 1

Proof: Consider a route between node *m* and *n* with *j* links. We index the nodes along the route as node 0, 1, 2, …, *j* and denote the status of links on the route as $Z_{1,mn}, Z_{2,mn}, ,..., Z_{j,mn}$. Furthermore, we denote type A and B events affecting route r_{mn} as $X_{1,mn}, X_{2,mn},..., X_{j,mn}$, and $Y_{0,mn}, Y_{1,mn}, Y_{2,mn},..., Y_{j,mn}$, where the subscripts mn are omitted in the rest of *Appendix I*. The proof of Theorem 1 is obtained by considering all possible combinations of events that may not cause the connection mn to be lost when there is no failure protection.

$$P(S_{mn}=0) = \sum_{X_1,...,X_j,Y_0,...,Y_j} P(S_{mn}=0 \mid X_1,...,X_j,Y_0,...,Y_j)P(X_1,...,X_j,Y_0,...,Y_j) \tag{63}$$

Since $P(S_{mn}=0) = P(Z_1=0, Z_2=0,..., Z_j=0)$, it follows that

$$P(S_{mn}=0 \mid X_1,...,X_j,Y_0,Y_1...,Y_j) = (1-p_b)^{Y_0}(1-P_b)^{Y_j}\prod_{i=1}^{j}(1-p_a)^{X_i}\prod_{l=1}^{j-1}(1-p_b)^{2Y_l}. \tag{64}$$

As events $A_1, A_2,..., A_j$, and $B_0, B_1, B_2,..., B_j$ are independent, we have

$$P(X_1, X_2,..., X_j, Y_0, Y_1...,Y_j) = \prod_{i=1}^{j}P(X_i)\prod_{l=0}^{j}P(Y_l). \tag{65}$$

Thus, from (64) and (65),

$$P(S_{mn}=0) = \prod_{i=1}^{j}\{\sum_{X_i}(1-p_a)^{X_i}P(X_i)\} \times \prod_{l=1}^{j-1}\{\sum_{Y_l}(1-p_b)^{2Y_l}P(Y_l)\}\sum_{Y_0}(1-P_b)^{Y_0}P(Y_0)\sum_{Y_j}(1-P_b)^{Y_j}P(Y_j). \tag{66}$$

Since $P(X_i=1)=a$ and $P(X_i=0)=1-a$;
$P(Y_l=1)=b$ and $P(Y_l=0)=1-b$, from (66),

$$P(S_{mn}=0) = (1-ap_a)^j(1-bP_b)^2(1-b(2p_b-P_b^2))^{j-1}. \tag{67}$$

APPENDIX II
PROOF OF THEOREM 3

Proof:

Since $B_{ring} = Erlang(\rho_{ring}, C) = \frac{\rho_{ring}^C}{C!}(\sum_{i=0}^{C}\frac{\rho_{ring}^i}{i!})$, it follows from [8] that,

$$\rho_{ring}(1-B_{ring}) < C < \rho_{ring}(1-B_{ring}) + \frac{1}{B_{ring}}. \tag{68}$$

Thus,

$$C = \begin{cases} \sum_{j=1}^{\frac{k-1}{2}} jv(1-B_{ring})^j + \frac{1}{B_{ring}}, & k\ odd, \\ \sum_{j=1}^{\frac{k}{2}-1} jv(1-B_{ring})^j + \frac{v}{4}(1-B_{ring})^{\frac{k}{2}} + \frac{1}{B_{ring}}, & k\ \ even. \end{cases} \quad (69)$$

Therefore, as $v \to \infty$,

$$B_{ring} = 1 - \frac{C-1}{v+1};$$

$$\mathbf{Z}_{ring} = k(C-1)p + o(\frac{C^2 p}{v});$$

$$\mathrm{k}_{ring} = p.$$

ACKNOWLEDGMENT

The authors would like to acknowledge helpful discussions with S. Jeon, Z. Chen, R. Narasimha, S. Erjongmanee, with A. Walid on definition of scalability, and with W. Willinger on network topologies. The authors would like to thank the anonymous reviewers for helpful comments and the associate editor for coordinating reviews. This work was supported in part by NSF ECS 0300605 and ECS 990857.

REFERENCES

[1] "Report of the National Science Foundation Workshop on Fundamental Research in Networking," Apr. 24-25, 2003, Virginia.

[2] Y. Liu and K. S. Trivedi, "A general framework for network survivability quantification," 12th GI/ITG Conference on Measuring, Modeling, and Evaluation of Computer and Communication Systems, Sep. 2004.

[3] G. Weichenberg, V. Chan, and M. Médard, "High-reliability architectures for networks under stress," *IEEE Journal on Selected Areas in Communications*, Vol. 22, pp. 1830-1845, 2005.

[4] F. Harary, Graph Theory, Addison Wesley Publishing Company, new education edition, Jan. 1995.

[5] J.J. Shi and J. P. Fonseka, "Analysis and design of survivable telecommunications networks," *IEE proceeding of communication*, Vol. 144, No. 5, pp. 322-330, Oct. 1997.

[6] T. P. Ng, "K-terminal reliability of hierarchical networks," *IEEE Transactions on Reliability*, Vol. 40, No. 2, pp 218-225, June 1991.

[7] J. Zhang and B. Mukheriee, "A review of fault management in WDM mesh networks: basic concepts and research challenges," *IEEE Network*, Vol.: 18, No. 2, pp 41-48, Mar.-Apr. 2004.

[8] F. Kelly, "Loss Networks," *Annals of Applied Probability*, Vol. 1, No. 3, pp. 319-378, 1991.

[9] A. Zolfaghari and F. J. Kaudel, "Framework for network survivability performance," *IEEE Journal on Selected Areas in Communications*, Vol. 12, No. 1, pp. 46-51, Jan. 1994.

[10] S. C. Liew and K. W. Lu, "A framework for characterizing disaster-based network survivability," Vol. 12, No. 1, pp. 52-58, Jan. 1994.

[11] V. Tamilraj and S. Subramaniam, "A comparison of optical network topologies," *Proceeding of Allerton Conference on Communications, Control, and Computing*, pp. 1337-46, Oct. 2003.

[12] Behrooz Parhami, "Introduction to parallel processing: algorithms and architectures," Plenum Press, 1999.

[13] K. Sivarajan and R. Ramaswami, "Lightwave networks based on de Bruijin graphs," *IEEE/ACM Transactions on Networking*, Vol. 2, pp. 70-79, Feb. 1994.

[14] William Feller, An Introduction to Probability Theory and Its Applications, John Wiley & Sons, 3rd edition.

[15] J. D. Spragins, "Dependent Failures in Data Communication Systems," *IEEE Transactions on Communications*, Vol. 25, Dec. 1977.

[16] K. V. Le and V. O. Li, "Modeling and Analysis of Systems with Multimode Components and Dependent Failures," *IEEE Transactions on Reliability*, Vol. 38, No. 1, pp. 68-75, Apr. 1989.

[17] D. Papadimitriou, F. Poppe, J. Jones, S. Venkatachalam, S. Dharanikota, R. Jain, R. Hartani, and D. Griffith, "Inference of shared risk link groups," Optical Internetworking Forum (OIF) contribution oif2001-066.

[18] S. Kandula, D. Katnabi, and J. Vasseur, "Shrink, a tool for failure diagnosis in IP networks," *Proceedings of ACM Minenet*, 2005.

[19] R. R. Kompella, J. Yates, A. Greenberg, and A. C. Snoeren, "IP fault localization via risk modeling," Proceedings of the 2nd ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI), Boston, MA, May 2005.

[20] P. Erdos and A. Renyi, "On the evolution of random graphs," in *Publ. Math. Inst. Hung. Acad. Sci.*, vol. 5, pp. 17-61, 1960.

[21] G. Liu and C. Ji, "Resilience of all-optical network architectures under in-band crosstalk attacks: a probabilistic graphical model approach, " *IEEE Journal on Selected Areas in Communications*, Vol. 25, No. 4, pp. 2-17, Apr. 2007.

[22] V. Paxson and S. Floyd, "Wide-area traffic: the failure of Poisson modeling," *IEEE/ACM Transactions on Networking*, Vol. 3, No. 3, pp. 226-244, June 1995.

[23] L. Li, D. Alderson, W. Willinger, and J. Doyle, "A first-principles approach to understanding the internet's router-level topology," *ACM SIGCOMM Computer Communication Review*, 34(4):3–14, 2004.

Guanglei Liu (S'02) received the B.E. degree in electrical engineering from Tianjin University, Tianjin, China, in 1998, the M.S. degree in electrical engineering from Rensselaer Polytechnic Institute (RPI), Troy, NY, in 2001, and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology, Atlanta in May 2007. Currently, he is an Associate Professor in Computer Science at Roane State Community College, TN. His main research interest is management and control of communication networks, especially optical networks.

Chuanyi Ji (S'85-M'91) received the B.S. (Honors) degree from Tsinghua University, Beijing, China, in 1983, the M.S. degree from the University of Pennsylvania, Philadelphia, in 1986, and the Ph.D. degree from the California Institute of Technology, Pasadena, in 1992, all in electrical engineering. She is an Associate Professor in the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta. She was on the faculty at Rensselaer Polytechnic Institute, Troy, NY, from 1991 to 2001. She spent her sabbatical at Bell Laboratories, Lucent Technologies, in 1999, and was a visiting faculty at the Massachusetts Institute of Technology, Cambridge, in Fall 2000. Her research lies in network management and security, large-scale network measurements, learning algorithms and learning theory, statistics and information theory. She received an NSF Career Award in 1995, and an Early Career Award from Rensselaer Polytechnic Institute in 2000.