MANAGEMENT AND CONTROL OF SCALABLE AND RESILIENT NEXT-GENERATION OPTICAL NETWORKS

A Thesis
Presented to
The Academic Faculty

by

Guanglei Liu

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

School of Electrical and Computer Engineering
Georgia Institute of Technology
May 2007

MANAGEMENT AND CONTROL OF SCALABLE AND RESILIENT NEXT-GENERATION OPTICAL NETWORKS

Approved by:

Dr. Chuanyi Ji, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Gee-Kung Chang
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Steven W. McLaughlin
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Stephen E. Ralph
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Ellen W. Zegura
College of Computing
Georgia Institute of Technology

Date Approved: January 4, 2007

This dissertation is dedicated to my family.
Thank you for your love, encouragement, and support.

ACKNOWLEDGEMENTS

I would like to thank my advisor, Professor Chuanyi Ji, for her guidance and support from the very early stage of this research. She has been a great source of motivation for me since I started my graduate study. She helped me identify promising research topics and led me into the field of graphical models. She provided me with unflinching encouragement and support in various ways. I am very grateful to her for her care and advice for my professional developement.

I also would like to thank members of my thesis committee, Professor Gee-Kung Chang, Professor Steven W. McLaughlin, Professor Stephen E. Ralph and Professor Ellen W. Zegura. Thanks for their commitment to help me improve my thesis despite their busy schedule and other engagements. I have greatly benefited from their constructive suggestions from different perspectives.

I am very thankful for my colleagues at the Lab of Communication Networks and Machine Learning: Zesheng Chen, Sung-Eok Jeon, Rajesh Narasimha, Supaporn Erjongmanee, Dr. Guang Cheng, Dr. Sung-Ho Huang, and Dr. Minsu Kim. I thank them for helpful discussions, and for their friendship and support. I am fortunate to be part of this wonderful group.

Finally, I would like to express my deepest appreciation to my family: my late father and my mother, whose vision and wisdom have inspired me in life; my brothers for their unconditional support; and Ning, whose love and support has encouraged me all the way. This thesis is dedicated to them.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

In this thesis, we focus on two important research problems in next generation optical networks with wavelength-division multiplexing (WDM) circuit switching (flow switching) technologies: (1) scalability of network management and control, and (2) resilience/reliability of networks upon faults and attacks. Our main technical approaches are decision theory and probabilistic graphical models.

As optical networks grow in size and complexity, there is a need for inter-domain light-path assessment using partial management information. Therefore, to understand scalable network management of flow switching, we investigate the scalability of network management information for inter-domain light-path assessment. Using the framework of decision theory and probabilistic graphical models, we formulate the light-path assessment as a decision problem. We show that partial information available can indeed provide the desired performance, i.e., a small percentage of erroneous decisions can be traded off to achieve a large saving in the amount of management information.

A second consequence of the large network size and great network complexity is that: networks face an increasingly adverse environment with more frequent faults and malicious attacks. To understand network resilience under malicious attacks, we study the resilience of all-optical networks under in-band crosstalk attacks using probabilistic graphical models. Graphical models provide an explicit view of the spatial dependencies and interactions between the physical layer and the network layer, as well as computationally efficient approaches, e.g., sum-product algorithm, for studying network resilience. Based on the proposed cross-layer model of attack propagation, we investigate

key factors that affect the resilience of the network under in-band cross-talk attacks from both the physical layer and the network layer. In addition, we obtain analytical results on network resilience for typical topologies including ring, star, and mesh-torus networks.

To understand network performance upon failures, we systematically investigate traffic-based network reliability. We first adopt a uniform deterministic traffic at the network layer. This allows us to focus on the impacts of network topology, failure dependency, and failure protection on network reliability, and to obtain analytical results on the network reliabilities of typical network topologies. We then apply a random network layer traffic model with Poisson arrivals to further investigate the effect of network layer traffic distributions on network reliability. We study the interaction between the network reliability and the connection arrival rate, and obtain asymptotic results of network reliability metrics with respect to arrival rate for typical network topologies under heavy load regime.

The main contributions of this thesis include: (1) fundamental understandings of scalable management and resilience of next-generation optical networks with WDM flow switching; and (2) the innovative application of probabilistic graphical models, an emerging approach in machine learning, to the research of communication networks.

CHAPTER 1

INTRODUCTION

1.1 Motivation

Despite the seemingly abundant investments in optical fibers by network carriers, the deployment of optical networks is still at its infancy. To better exploit the capabilities of optical technologies for high-bandwidth communication, there is a need for next generation optical networks, which ideally could provide high-speed network access and bandwidth-on-demand at reduced costs. One promising technique to achieve the goal is wavelength-division multiplexing (WDM) circuit switching (flow switching), where optical circuits, i.e., light-paths, are dynamically established at a short time scale (~10's ms) [1][2]. Such a fast provisioning of light-paths would use the available network resources efficiently by adjusting to the rapidly changing needs of end users, thus reduce the cost. In addition, it could serve as a platform for new services and applications. In such a paradigm of next generation optical networks, two problems in networking community appear to be rather challenging: (1) scalability of network management and control, and (2) resilience of networks under faults and attacks.

A scalable network management system should have the property that its complexity grows gracefully with the size of the networks whereas provides efficient control. As optical networks grow in size and complexity, a light-path may traverse multiple network domains with each domain consists of hundreds of network nodes. Thus it creates the need for inter-domain light-path assessment using partial management information.

As the network grows in scale, it faces an increasingly adverse environment and network faults and malicious attacks are more frequent. For instance, the Internet Infrastructure has a large scale and is accessed by hundreds of millions of users with different interests. It constantly faces the threat of component failures, human operational errors, spreading of software virus, and malicious attacks [3]. Because of the high-bandwidth supported by optical networks, a small period of service disruption may result in huge amount of data loss. Therefore, it is important to have a good understanding of the resilience/reliability of optical networks under faults and attacks when optical networks are still at early stage of implementation. Hence, the objective of this research is to contribute to fundamental understanding of scalable and resilient next-generation optical networks using WDM circuit switching technologies.

1.2 Problem Description

In this thesis, to understand scalable network management and control of WDM flow switching, we investigate the scalability of network management information for inter-domain light-path assessment. A framework based on probabilistic graphical models is proposed to study whether it is feasible to use partial management information to achieve a desired performance for inter-domain light-path assessment.

To understand network resilience under malicious attacks, we study the resilience of all-optical networks under in-band crosstalk attacks. Crosstalk attack propagation depends on both optical devices at the physical layer and wavelength usage at the network layer. This motivates us to apply probabilistic graphical models to model attack propagation. Graphical models provide an explicit view of the spatial dependencies and interactions between the physical layer and the network layer, as well as computationally

efficient approaches, e.g., sum-product algorithm, for studying network resilience. Based on the cross-layer model of attack propagation, we investigate key factors that affect the resilience of the network under in-band cross-talk attacks from both the physical layer and the network layer.

To understand network performance upon failure events, we systematically investigate traffic-based network reliability. We first adopt a uniform deterministic traffic at the network layer, which allows us to focus on the impacts of network topology, failure dependency, and failure protection on network reliability and to obtain analytical results on the network reliabilities of ring, star and mesh-torus networks. We then apply a random network layer traffic model with Poisson arrivals to further investigate the effect of network layer traffic distributions on network reliability. We study the interaction between the network reliability and the connection arrival rate, and obtain asymptotic results of network reliability metrics with respect to arrival rate for typical network topologies under heavy load regime.

1.3 Thesis Outline

The thesis is organized as follows. In Chapter 2, we pose light-path assessment as a decision problem, and define the performance as the Bayes probability of an erroneous decision. We then characterize the scalability of management information as its growth rate with respect to the total resources of the network to achieve a desired performance. Scalability is achieved if the management information needed is only a negligible fraction of the total network resources. Specifically, we consider one type of partial information that grows only logarithmically with the number of wavelengths supported per link. We derive an upper bound for the Bayes error in terms of the blocking probability when a

new call is presented at the entrance of the network. We evaluate the upper bound using both independent and dependent models of wavelength usage for intra- and inter-domain calls. Our study shows that there exists a "threshold effect": The Bayes error decreases to zero exponentially with respect to the load when the load is either below or above a threshold value; and is non-negligible when the load is in a small duration around the threshold. This suggests that the partial information considered can indeed provide the desired performance, and a small percentage of erroneous decisions can be traded off to achieve a large saving in the amount of management information.

In Chapter 3, we use probabilistic graphical models to study the resilience of all-optical networks under in-band crosstalk attacks. At the network layer, we use an undirected probabilistic graph to represent the probability distribution of active connections in the network. The cross-layer model is obtained by combining the physical- and the network-layer models into a factor graph representation. Graphical models provide an explicit representation of interactions between the physical- and the network layer. Furthermore, graphical models facilitate derivations of analytical results on resilience with respect to physical-layer vulnerability, physical topology, and network load. Specifically, we derive bounds on the network resilience for regular topologies. We show that for ring, star, and mesh-torus networks with link-shortest path routing and all-to-all traffic, the average network resilience loss grows linearly with respect to the network load when the network load is small, and grows polynomially with respect to the probability of attack propagation from node to node along the attacker's route. In addition, numerical results suggest that the sum-product algorithm based on the factor

graph representation can be used for computationally efficient evaluation of network resilience for irregular/large topologies.

In Chapter 4, we systematically investigate different factors that affect traffic-based network reliability. We first assume a uniform deterministic traffic at the network layer, which allows us to focus on the impacts of the first three factors on network reliability. We then adopt a random network layer traffic model with Poisson arrivals to further investigate the effect of network layer traffic distributions on network reliability. To obtain analytical results on network reliability, we apply the approach of Erlang Fixed Point Approximation (EFPA). To represent the dependencies among network failures and physical layer failures, we make use of probabilistic graphical models, which provides graphical representation of the dependencies and a potential numerical approach for evaluation of network reliability when the network layer traffic is random.

In Chapter 5, we conclude the thesis with a discussion about the contribution of this work and directions for future research.

CHAPTER 2

SCALABILITY OF NETWORK MANAGEMENT INFORMATION FOR INTER-DOMAIN LIGHT-PATH ASSESSMENT

2.1 Introduction of Chapter 2

Dynamically assessing the quality of light-paths is important to many applications in wavelength-routed optical networks such as on-demand light-path provisioning, protection and restoration. As the light-path quality is a complex measure [4], this work considers a simple quality, which is the wavelength availability on a candidate light-path. The assessment then boils down to determine availability of wavelengths for incoming call requests based on given management information.

Complete or partial network management information can be used to assess the wavelength availability on a light-path. Complete information corresponds to the detailed states of wavelength usage, i.e. "which wavelengths are used at which links of a network", when there are no wavelength converters in the network. Wavelength converters can reduce state information due to their ability to relax the wavelength continuity constraint. However, it is expected that wavelength converters remain expensive and are thus used mostly on the boundaries of sub-networks [5]. Therefore, generally complete state information involves the detailed wavelength occupancy within a subnet. Partial information includes aggregated load and topology information at each subnet, and local states, e.g., the total number of wavelengths used at wavelength converters.

Providing state information is a basic functionality of network management. Traditional network management systems intend to obtain as complete state information

as possible [6]. But future IP-WDM networks may have hundreds of links with each link supporting hundreds of wavelengths [7]. This would result in a huge amount of state information for networks without wavelength converters. For instance, let H be the number of links within each subnet, F be the number of wavelengths supported per link at each subnet, and L be the number of subnets. The total amount of information about wavelength usage is in the order of FHL. When $F = 200$, $H = 250$ and $L = 10$, the number of states is about half a million. Storing and updating even a fraction of such a large number of states may result in an undesirably large amount of management traffic. Therefore, it would be prohibitive to manage a large network using complete state information.

Using partial management information is also a requirement of multi-vendor services. A light-path may traverse multiple administrative domains (sub-networks) run by different service providers. A service provider may prefer to exchange only minimal information to other network domains rather than share the complete state information of its own. In fact, it has been the experience today in the Internet that network managers of different administrative domains are extremely reluctant to and rarely share detailed network state information of their subnets with others. Therefore, inter-domain subnets are like unknown network clouds to a service provider [8]. Light-path assessment may have to use partial information on network clouds since it is infeasible to obtain complete management information across domain boundaries.

Therefore, a fundamental issue in light-path assessment is what performance can possibly be achieved given the partial information. Specifically, the related questions are: (1) what is the best performance of light-path assessments with the partial information?

(2) What is the trade-off between the performance and the amount of management information maintained for light-path assessments?

We formulate the light-path assessment as a decision problem, and define the performance as the probability of an erroneous assessment. An error occurs when an assessment decision differs from the ground truth (in terms of availability of wavelengths on a given path). The value of the error probability measures the deviation from the optimal performance (with zero error) when the complete information is available, and thus quantifies the sufficiency/insufficiency of the partial management information.

With a large amount of management information, a good performance, i.e., a small error probability, could be achieved but at the cost of management complexity such as signaling and memory overhead. With a small amount of management information, the performance may degrade but with a gain of management simplicity. Thus a trade-off can be made between the performance and the network management information.

The amount of management information needed varies with respect to the size, and the resource of the network. The size can be characterized by the number of links in a subnet and the number of subnets. The resource corresponds to the total number of wavelengths, which is related to the number of users (flows) supportable by a network. Future optical networks may have hundreds of links, each of which supports hundreds of wavelengths. Therefore, the growth rate with respect to those parameters is an important measure of the amount of management information used. In particular, a desirable growth rate should be slower than that of the total resource to be managed in a network.

Combining the performance and the growth rate, we define the scalability of network management information for light-path assessment. Assuming that a given performance

is satisfied, i.e., a small probability of error can be achieved; we consider the needed management information as scalable, if it grows at a slower rate than the total network resource; and as non-scalable, otherwise. Therefore, the scalability requires that the amount of information used is only a negligible fraction of the total wavelength resources within the network. Hence scalability/non-scalability provides a systematic way to investigate the tradeoff between performance and the management information.

In this work, we study one type of "strongly'' scalable management information, which is only logarithmic ($O(\log F)$) in the number of wavelength supported per link in the network. We investigate a simple network of bus topology to study the scalability of the partial management information. Wavelength converters are only located at the boundaries of, but not within, each subnet. The partial information we consider includes (a) aggregated information on network load and topology within subnets, and (b) local state information at wavelength converters. The aggregated information serves as model parameters of wavelength usage, and the local information corresponds to random states or observations obtained locally at domain boundaries. For a bus topology with F available wavelengths at each link and L subnets, the total amount of the partial information is $O(L \log F)$. This is indeed much less than the total amount of resources availabe in the network (FHL). Therefore, the partial information will introduce much less management complexity than complete information.

To evaluate the achievable performance using the partial information, we consider the Bayes decision rule. The Bayes rule results in the best performance achievable given the partial information, which is the Bayes probability of error. We show that the Bayes error is bounded by $\min\{P_b, 1-P_b\}$, where P_b is the blocking probability of a light-path. This

links the Bayes error with P_b, a metric commonly used for WDM networks [9][10][11]. The (Bayes) probability of error can then be investigated through the blocking probability based on different traffic models. We first adopt an independent model that corresponds to local calls. We then extend the independent model to a dependent model to include inter-domain calls. One important characteristic of the best performance using the partial information is a "threshold effect'', i.e., there exists a threshold for the load. When the load is close to the threshold value, the blocking probability makes a sharp transition from 0 to 1. The corresponding probability of error remains close to zero for most of the load conditions. This suggests that the partial information could provide desirable performance for light-path assessment. Hence the partial information is scalable and a small loss in performance may be traded off with a large saving in network management information.

The rest of Chapter 2 is organized as follows. Section 2.2 summarizes the prior work. Section 2.3 provides the problem formulation. Section 2.4 presents Bayes decision theory, and an upper bound of the best performance (the Bayes error) that can be achieved given the partial information. Sections 2.5 and 2.6 investigate the best performance using an independent model and a dependent model respectively. Simulation results are presented in section 2.7. Section 2.8 concludes Chapter 2.

2.2 Related Work

Various schemes have been proposed for managing IP-WDM networks based on different amount of management information. Complete state information has been used to establish connections [12]. This approach, as discussed earlier, may not be feasible for dynamically setting up inter-domain connections for large networks. In contrast to using

complete information, another method is to manage sub-networks as separate entities [13]. The corresponding performance (i.e., the correctness of an assessment) can be poor due to lack of information. An intermediate approach is to use partial information-exchange among network domains [14]. The idea of using partial information is also investigated in other related research problems such as network survivability [15][16][17], and wavelength routing [18]. However, these works have a different focus, which is mostly on developing approaches to manage networks using partial information. They motivate this work to investigate the scalability of management information.

Probing methods have been proposed to obtain information from network clouds [20]. Probing, however, is intrusive, and may be impractical for inter-domain light-path assessment because of security reasons.

Wavelength converters (optical or electronic) have been considered in designing WDM networks to improve wavelength utilization [21]. Sparsely-allocated wavelength converters are found to be sufficient to achieve a desired utilization gain sometimes [22]. The use of wavelength converters has also been conjectured to result in simplified network management systems due to their ability to reduce the state information [21]. This motivates us to consider a natural network architecture where wavelength converters are located at the boundaries of subnets (administrative domains).

There have also been a lot of standardization activities for next-generation optical transport networks. Specifically, ITU presents under the framework of Automatic Switched Optical Network (ASON); while the IETF adopts the GMPLS paradigm. The OIF also provides important inputs to the standardization process [19]. The GMPLS standardization activities are very much driven by the requirement of ASON and can be

regarded as one candidate set of protocols for ASON. The problem of light-path assessment can be considered as call admission control specified under the ASON framework, where it has been widely agreed that what information should be exchanged among network controllers and the scalability of management information is one of the major issues.

Prior investigations in other related areas are also beneficial to this research. In particular, inaccurate or aggregated information has been investigated in the context of *QoS* routing for IP networks [23]. Commonly used aggregated information is topology aggregation [24][25] that can be regarded as a summarized characterization of a subnet. Local information is considered in [26] for *QoS* routing in IP networks. However, the main focus of aforementioned work is on managing existing (IP) rather than IP-WDM networks.

Therefore, the tradeoff between performance and the amount of management information has not been investigated quantitatively. In our prior work [27][28], we formulated the problem of network management information for light-path assessment based on independent and dependent models of wavelength usage. This work extends the prior work to a more comprehensive setting. We formally define the scalability of management information for light-path assessment, and use both analysis and simulations to investigate the scalability of the information.

2.3 Problem Formulation

2.3.1 Network Architecture

We consider assessing wavelength availability for an end-to-end call request from source border node *S* to destination border node *D* as shown in Figure 2.1. Wavelength

converters are located at the boundaries of one-dimensional subnets, and there are L subnets on a given path. Here for simplicity, we assume that border nodes with wavelength converters connect two adjacent network domains. Each subnet has H hops and each link supports F wavelengths. Such network architecture, although simple, captures the important characteristic of multi-domain network topologies.

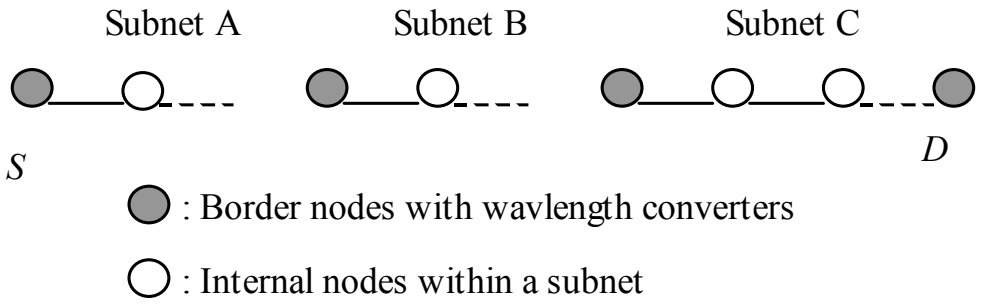

Figure 2.1 Network architecture

2.3.2 Partial Management Information

The partial information we consider consists of aggregated information and local states. The aggregated information characterizes the average behavior of each network domain so that detailed network states within each subnet do not need to be exchanged across domains. The aggregated information is denoted as $A = (A_1, A_2, ..., A_L)$, where A_i is the aggregated information on subnet i and $A_i = (F_i, H_i, \rho_i, \pi_i)$. F_i and H_i are the number of wavelengths per link and the number of links at subnet i respectively. ρ_i is the probability that a wavelength is used on a link in domain i, which is the load information aggregated over all detailed states about wavelength usage within the subnet. π_i is a parameter related to wavelength usage. For example, π_i could be the parameter that

characterizes how wavelengths at each link are used, i.e., the percentage of occupied wavelengths used for inter-domain connections. For simplicity of analysis, we assume that each subnet has the same aggregated information. Then we have $A_i = (F, H, \rho, \pi)$ for all i.

In practice, the aggregated information can be estimated through measurements, which may deviate from true parameters, and thus introduce additional information loss. For simplicity, we consider aggregated parameters as accurate. These parameters may also change with time but at a much larger time scale than the connection dynamics, and could thus be regarded as nearly static.

The local information corresponds to the number of wavelengths used at the first hop of each subnet, which is readily available at the wavelength converters. Specifically, the local information corresponding to observations (states) at the wavelength converters is given as $X = (N_1, N_2, ..., N_L)$, where N_i is the number of wavelengths used at the ith wavelength converters, i.e., the number of wavelengths used at the first link of domain i. Such local information is changing with setup and teardown of connections, and can thus be considered as random variables.

The local information is informative due to the wavelength continuity constraint within a subnet. For instance, if nearly all wavelengths are used at the first hop of a subnet, we can infer that the load is high and there may not be any wavelength available within the subnet to support an additional end-end call. Likewise, the aggregated information is informative since it characterizes the average load in a subnet. But the aggregated and local information is incomplete in determining network states, resulting in possibly erroneous wavelength assessments.

2.3.3 Decision Problem and Performance

We pose the light-path assessment as a decision problem. A decision variable ω is defined as follows: $\omega = 1$ if there is one end-to-end wavelength continuous path across subnets for the connection request; and $\omega = 0$ otherwise. The problem of light-path assessment is to decide on ω given the partial information. Then the performance of light-path assessment can be defined as the probability of erroneous decisions.

Definition 2.1 *The probability of error* P_e *is defined as the probability that the assessment decision is different from the ground truth (in terms of availability of wavelengths on a given path).*

Let D be the decision region on the management information X for $\omega = 1;$ and $\bar{D}$ be the decision region for $\omega = 0.$ In other word, if the observation X falls in D or $\bar{D},$ the decision should be $\omega = 1$ or $\omega = 0$ respectively. We then have the probability of error

$$P_e = P(X \in D,\ \omega = 0) + P(X \in \bar{D},\ \omega = 1). \tag{2.1}$$

P_e characterizes the average performance given the partial information. The validity of such a performance measure can be understood through Figure 2.2. When the complete information is available, no error is made in assessing wavelength availability, and the performance is the best (i.e., zero error). When no information is available, decisions can only be made based on random guessing, and the performance is the worst (i.e., 50% error). P_e measures the deviation from the optimal performance (zero error) when the complete information is available, and quantifies the sufficiency/insufficiency of the management information available. A question is whether it is possible to use partial management information at the cost of a small number of incorrect decisions.

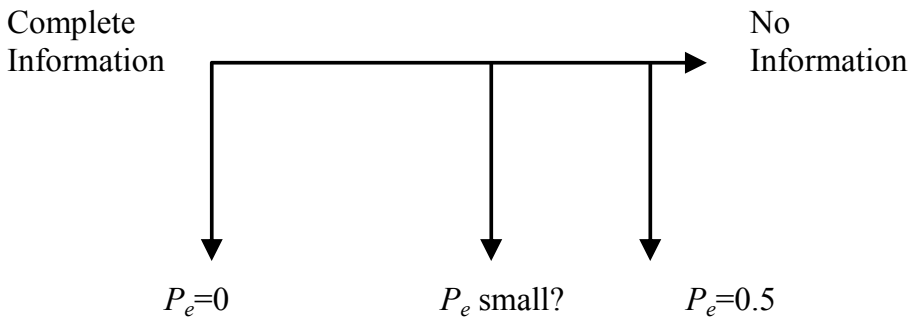

Figure 2.2 Performance vs. management information

2.3.4 Scalability of Management Information

We investigate this problem in the context of scalable network management information. Intuitively, there are two important aspects of the scalability: The amount of management information should be sufficiently large to satisfy a given performance, i.e., a small probability of error. Meanwhile, the amount of management information should be small enough to keep network management simple. For instance, it is preferred that the management information needed is just a negligible fraction of the total network resource, e.g. the total number of wavelengths supported in the network. Since the resource varies with respect to the size of a network and the number of wavelengths supported per link, it would be meaningful to characterize the amount of management information required as its growth rate with respect to those quantities. Combining the performance and the growth rate, we formally define the scalability of management information as follows.

Definition 2.2 *Let Q_P be the amount of management information used for light-path assessment. Let Q_R be the total amount of wavelength resources within the network. If Q_P grows at a slower rate than Q_R with respect to the number of wavelengths per link*

(F) and the size (HL) of a network, and the corresponding performance of light-path assessment is acceptable under most load conditions, the network management information is scalable; and non-scalable otherwise.

This definition essentially means that asymptotically (for large networks with many links and wavelengths each link), the scalable management information is a negligible fraction of the total network resource. That is, $Q_P / Q_R = o(1)$ when F and HL are large.

Consider the network shown in Figure 2.1. The number of bits is used to quantify the management information. The detailed states within each subnet are "which wavelengths are used at which link". The total number of possible (binary) states is 2^{FH} for each subnet, and 2^{FHL} for L subnets. Therefore, complete information satisfies

$$Q_P(complete) = Q_R = FHL. \tag{2.2}$$

Clearly, it is non-scalable to use complete management information according to Definition 2 even though it will always result in zero probability of error.

The partial management information considered in this work satisfies

$$Q_P(partial) = L\log(F) + Q_A, \tag{2.3}$$

where Q_A is the number of bits needed to store the aggregated information, which is indexed with A. Q_A is generally small, and changes slowly with time. $\log(F)$ is the total number of bits needed to characterize local states at one subnet. Then the amount of partial information is in the order of $\log(F)$, which is much less than that of the complete management information, especially when the number of wavelengths is large. Such partial information can be maintained easily even for a large network.

2.4 Optimal Performance Using Bayes Rule

We now evaluate the best performance of the partial management information to see whether it can provide the desired performance.

2.4.1 Bayes Error

With partial management information, assessment schemes based on Bayes decision rule [29] achieve the best performance. Given a set of local states $X = (N_1, N_2, ..., N_L)$, the Bayes rule is to decide

$$\begin{cases} \omega = 1, \ \textit{if} \ \ P(\omega = 1 \mid X = x)) \geq P(\omega = 0 \mid X = x), \\ \omega = 0, \ \textit{otherwise}, \end{cases}$$

where $P(\omega = 1 \mid X = x)$ and $P(\omega = 0 \mid X = x)$ is *a posteriori* probability given observation $X = x$. The equality $P(\omega = 1 \mid X = x) = P(\omega = 0 \mid X = x)$ corresponds to the decision boundary, which divides the space (X) into two regions, D to decide $\omega = 1$ and $\overline{D}$ to decide $\omega = 0$. The Bayes error is the average probability of error as given in (2.1).

2.4.2 Centralized Light-path Assessment

Such a Bayes rule essentially corresponds to an optimal centralized assessment scheme. Imagine a fictitious central manager, collecting partial information from all subnets. At a relatively larger time-scale than the flow dynamics, the central manager could poll the aggregated information from each subnet. The central manager then could collect the local observation X at a smaller time scale, and perform the Bayes rule to assess wavelength availability.

This centralized scheme is only conceptual, and used in this work for analysis rather than a practical solution. Centralized assessment may not be feasible for large optical

networks because each subnet could belong to different administrative entities. Thus a distributed light-path assessment scheme may be a necessity. However, distributed assessment schemes result in further information loss due to decentralization. Therefore there is a need to understand the best performance achievable using the partial information. Such best performance would then serve as a basis for assessing the performance of sub-optimal yet practical schemes.

2.4.3 Bayes Error and Blocking Probability

Although the Bayes error characterizes the optimal performance, it is difficult to evaluate because the decision regions and the corresponding probabilities are hard to obtain. Therefore, we derive an upper bound for the Bayes error. Our goal is to relate such a bound with a commonly used network measure such as blocking probability. Such a relation may provide intuition on how error decisions are related to the load (ρ) and wavelength per link (F) of each subnet. For clarity, we describe the blocking probability based on [9].

Definition 2.3 *The blocking probability P_b is defined as the probability that there does not exist a wavelength continuous path in each network domain to support an end-to-end inter-domain connection*.

A relation between the Bayes error P_e and the blocking probability P_b can then be derived.

Theorem 2.1 $0 \le P_e \le \min\{P_b, (1-P_b)\}$.

The proof of the theorem is given in *Appendix A*. Intuitively, the upper bound $\min\{P_b,(1-P_b)\}$ can be understood as follows. Consider the following decision rule: If the blocking probability of the network is $P_b > 1/2$, one can reject all connection requests. If $P_b < 1/2$, one can simply accept all connection requests. This decision rule will have $P_e = \min\{P_b,(1-P_b)\}$. Since Bayes rule uses local observation X as the additional information for light-path assessment in an optimal fashion; a better performance should be achieved. That is, the Bayes error should be bounded by $\min\{P_b,(1-P_b)\}$. The upper bound shows that the probability of error is small if the blocking probability is close to 1 or 0.

This theorem suggests an analytically feasible way to estimate the Bayes error, which is through the blocking probability. In addition, the bound is independent of a specific model of the blocking probability. The analysis can then be conducted using different models.

2.5 Independent Model

2.5.1 Independent Model

We first assume independent wavelength usage on different network links and among wavelengths. Such an assumption is equivalent to that all connections within the network are local calls as shown in Figure 2.3. Then the corresponding aggregated information is $A = (\rho, F, H, L),$ where ρ is the probability that wavelength is used on one link. The local observation is $X = (N_1, N_2, ..., N_L)$ as defined in Section 2.3. Due to the independent assumption, all the N_i's are independent random variables.

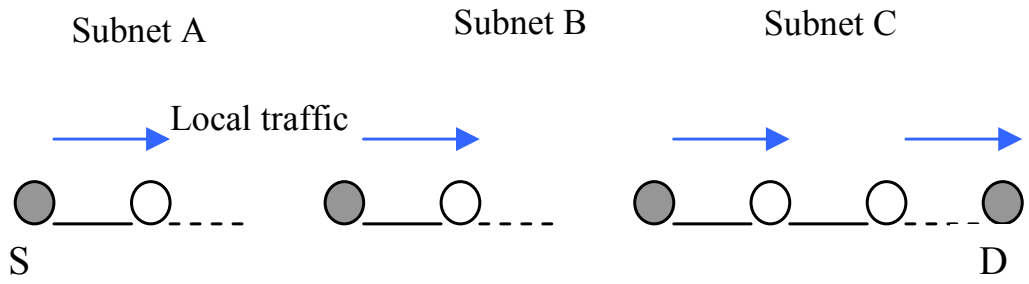

Figure 2.3 Local calls in independent Model

2.5.2 Bayes Error

Under the independent model, the *a posteriori* probability is

$$f(X) = P(\omega = 1 \mid X = (N_1, N_2, ..., N_L))$$

$$= \prod_{i=1}^{L} (1 - (1 - (1 - \rho)^{H-1})^{(F-N_i)}), \tag{2.4}$$

where $i = 1, 2, ..., L.$ This expression means that if N_i wavelengths are used at the first hop of subnet *i*, one only needs to decide whether there is a wavelength continuous path at the next $H-1$ hops from $F - N_i$ candidate wavelengths. Then $1-(1-(1-\rho)^{H-1})^{(F-N_i)}$ is the probability that there is a wavelength continuous path at the *i*th subnet given N_i, and the product is the probability that the connection request for an end-to-end call to be supported. The Bayes error is:

$$P_e = P(f(X) \geq 0.5, \omega = 0) + P(f(X) < 0.5, \omega = 1). \tag{2.5}$$

Equation (2.5) does not have a close form; and we turn to evaluate the upper bound of P_e using the blocking probability of the independent model.

2.5.3 Numerical Analysis

Under the independent assumption, the probability that there is one end-to-end wavelength continuous path can be obtained using a model in [9]:

$$P_{ai} = (1-(1-(1-\rho)^H)^F)^L, \tag{2.6}$$

where the sub-index *ai* means acceptation of a request based on independent model. Therefore, the corresponding blocking probability for an end-to-end call is,

$$P_{bi} = 1-(1-(1-(1-\rho)^H)^F)^L. \tag{2.7}$$

Figure 2.4 plots the blocking probability (P_{bi}), vs. the load (ρ) for $F =$ 10, 40, 120, $H = 5$, $L = 3$. One observation is that there is a threshold effect on P_{bi}. When ρ is below the threshold value (e.g. about at $\rho = 0.6$ for $F = 120$), P_{bi} remains close to 0. When ρ is around the threshold value, P_{bi} increases to 1 rapidly with respect to ρ. With a larger *F*, the value of the threshold increases, and the transition of P_{bi} from 0 to 1 gets sharper.

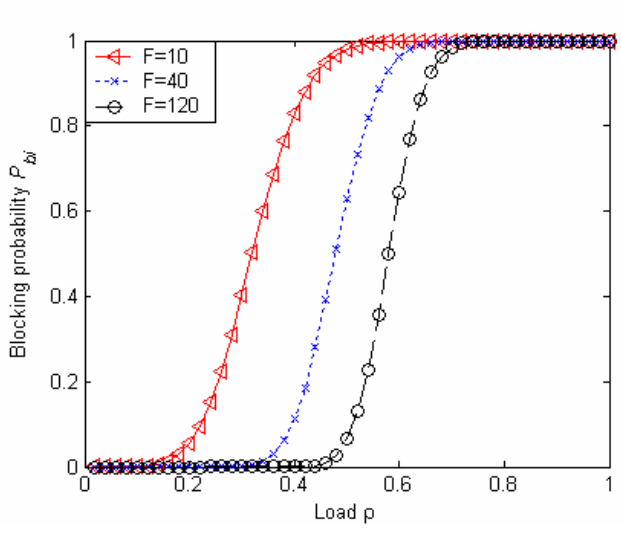

Figure 2.4 Load (ρ) vs. blocking probability (P_{bi}): *F=10, 40, 120, H=5, L=3*

This shows that under most load conditions, we either have a small or a large blocking probability, both of which result in a small probability of error. Therefore, based on Theorem 1, we can conclude that under most load conditions the probability of error for light-path assessment using partial information is small under independent model. Figure 2.5 confirms this by plotting the upper bound of P_e for $F = 10,\ 40,\ 120,\ H = 5,\ L = 3$. We can see that when the load is close to the threshold, the value of P_e increases to the maximum value exponentially; and P_e is small otherwise.

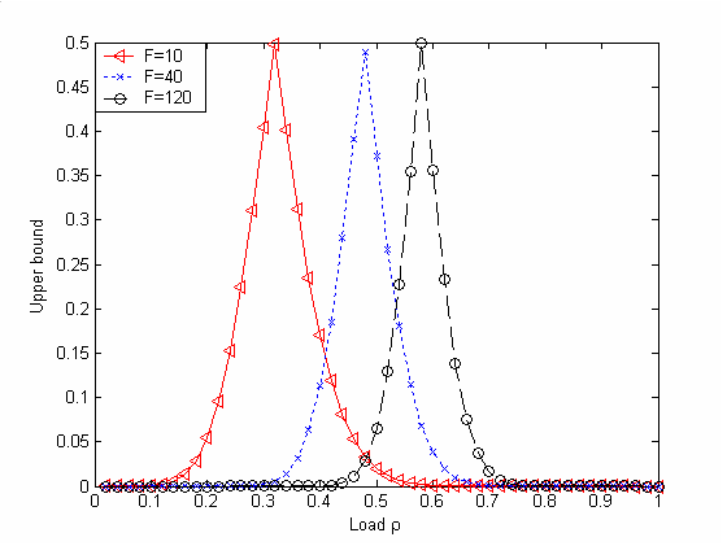

Figure 2.5 Load (ρ) vs. upper bound of P_e : *F=10, 40, 120, H=5, L=3*

2.5.4 Special cases

To quantify the decay rate of the upper bound for large F, we consider special cases of low and high load, which correspond to two parts of P_{bi} below and above the threshold. We can find that:

(*i*) When the load is light, i.e., $F >> \dfrac{1}{(1-\rho)^H}$,

$$0 \le P_e \le 2L[1-(1-\rho)^H]^F. \quad (2.8)$$

(*ii*)When the load is heavy, i.e., $F << \frac{1}{(1-\rho)^H}$,

$$0 \le P_e \le 2L(1-\rho)^{FH}. \quad (2.9)$$

These results suggest that the performance trade-off is a small probability of error that decreases exponentially with respect to the number of wavelengths per link (F) under low and high network load.

2.6 Dependent Model

The above independent model fails to capture the inter-domain calls, which extend beyond one subnet. In future optical networks, a significant percentage of the traffic may be inter-domain flows passing through subnets. Therefore, it is important to take the load correlation among subnets into consideration when estimating the performance. In this section, we investigate the probability of error by considering both intra- and inter-domain calls.

2.6.1 Dependent Model

Dependent models in a bus have been investigated in [9][10][11]. However, the study in [9] is restricted to having wavelength converters installed at each node, while the network architecture as shown in Figure 2.1 is with sparsely-allocated wavelength converters. More accurate dependent models for the blocking probability on such a topology can be found in [10][11]. However, both models are complex. Here we extend the dependent model in [9] to obtain a relatively accurate and tractable dependent model for analyzing the probability of error.

To capture the dependence on traffic flows among subnets, we assume that there are two types of calls supported by the network. One corresponds to local calls as assumed in the independent model. The other type of calls corresponds to inter-domain calls (Figure 2.6). Generally, inter-domain calls can originate and/or terminate anywhere at a network. But for simplicity of analysis, we impose the following assumptions:

(*i*) The inter-domain calls originate and exit only at edge wavelength converters.

(*ii*) If a wavelength is not used for an inter-domain call in one subnet, it is used for inter-domain call in the next subnet with probability P_n.

(*iii*) If a wavelength is used for one inter-domain call in one subnet, this inter-domain call will exit the current subnet with probability P_l, and will continue to the next subnet with probability $1 - P_l$.

(*iv*) If a wavelength is used for an inter-domain call in one subnet and is released at the edge OXC of this subnet, it is used for inter-domain calls with probability P_n in the next subnet.

(*v*) If an inter-domain call continues to the next subnet, it will use the same wavelength.

(*vi*) In each subnet, a wavelength is used for a local call in a link with probability ρ_1, and used for an inter-domain call with probability ρ_2. The probability that a wavelength is used for either a local or an inter-domain call is $\rho = \rho_1 + \rho_2$.

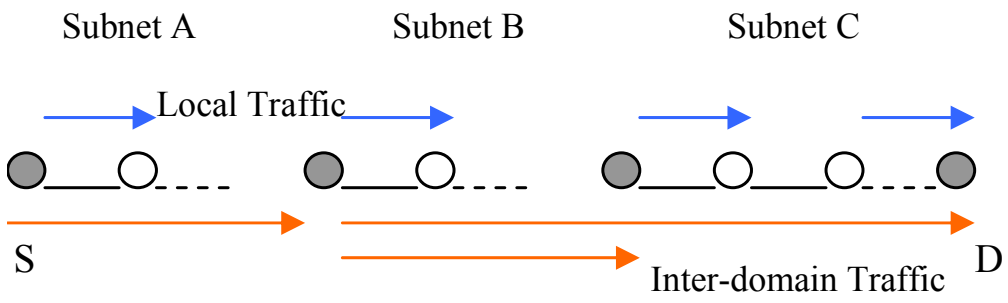

Figure 2.6 Inter-domain calls and local calls

The dependent model captures the link load correlation across subnets due to inter-domain calls, and is thus more accurate than the independent model. We are aware that it is limited to assume that the inter-domain calls can only enter or exit at the domain boundaries. However, such a model provides understanding of how inter-domain calls contribute to the performance and management information trade-off.

2.6.2 Bayes Error

We begin evaluating the performance by considering the probability of error. Again, we assume that all subnets have identical aggregated information. Under the dependent model, the aggregated information A is $A = (\rho_1,\ \rho_2,\ P_l,\ F,\ H,\ L)$. Local information is the same as that used for independent model, which is $X = (N_1, N_2, ..., N_L)$. Then the *a posteriori* probability used in Bayes rule is:

$$f(X) = P(\omega = 1 \mid X = (N_1, N_2, ..., N_L))$$

$$= \prod_{k=1}^{L} (1 - (1 - (1 - \rho_c)^{H-1})^{(F-N_i)}), \qquad (2.10)$$

Where $\rho_c = \rho_1/(1-\rho_2)$. ρ_c is defined as the probability that a wavelength is used for local calls given that it is not used for inter-domain calls. Such a posterior probability has a similar form to that of the independent case in (2.4).

The probability of error thus is the same as in (2.5). But due to inter-domain calls, the local observations (N_i's) at wavelength converters are now dependent random variables. Therefore, the Bayes error is difficult to derive, we turn to study the upper bound based on the blocking probability P_b.

2.6.3 Blocking Probability

To derive the blocking probability under the dependent model, we define $\alpha = \rho_2/\rho$, which characterizes the percentage of occupied wavelengths used for inter-domain calls. Then the independent model is just one special case of the dependent model with $\alpha = 0 (\rho_2 = 0)$. From assumptions in Section 2.6.1, we have,

(*i*) P (wavelength w_j is used for inter-domain call in subnet i| w_j is not used for inter-domain call in subnet i-1) = P_n,

(*ii*) P (wavelength w_j is used for inter-domain call in subnet i| w_j is used for inter-domain in subnet i-1) = $P_n P_l + (1 - P_l)$. Therefore,

$$\rho_2 = (1-\rho_2)P_n + \rho_2[P_n P_l + (1-P_l)]. \tag{2.11}$$

It follows that

$$P_n = \frac{\rho_2 P_l}{1-\rho_2(1-P_l)}. \tag{2.12}$$

Define $I_i = 1$ if there is one wavelength continuous path within subnet i; and $I_i = 0$, otherwise. Then a decision that there are wavelengths available for an end-to-end call

($\omega = 1$) is equivalent to $I_i = 1$ for all *i*. Let M_i be the number of inter-domain connections in subnet *i*. Then the blocking probability under the dependent model can be expressed as:

$$P_{bd} = 1 - \sum_{M_1, M_2, \ldots M_L} \{P(I_1 = 1, I_2 = 1, \ldots, I_L = 1 \mid M_1, M_2, \ldots, M_L) P(M_1, M_2, \ldots, M_L)\}$$
$$= 1 - \sum_{M_1, M_2, \ldots M_L} \{P(I_1 = 1 \mid M_1) P(M_1) P(I_2 = 1 \mid M_2) P(M_2 \mid M_1) \cdots P(I_L = 1 \mid M_L) P(M_L \mid M_{L-1})\}, \quad (2.13)$$

where $P(I_i = 1 \mid M_i) = 1 - [1 - (1 - \rho_c)^H]^{(F - M_i)}$.

Let M_{1i} be the number of inter-domain calls in the *i*th subnet that continue to the next subnet. We have

$$P(M_i = m_i \mid M_{i-1} = m_{i-1}) = \sum_{M_{1i-1}=0}^{\min\{m_i, m_{i-1}\}} P(M_i \mid M_{1i-1}) P(M_{1i-1} \mid M_{i-1}), \quad (2.14)$$

where

$$P(M_{1i-1} = m \mid M_{i-1} = k) = \binom{k}{m} P_l^{(k-m)} (1 - P_l)^m, \qquad \text{for } 0 \le m \le k \le F, \quad (2.15)$$

and

$$P(M_i = h \mid M_{1i-1} = m) = \binom{F-m}{h-m} P_n^{(h-m)} (1 - P_n)^{(F-h)}, \qquad \text{for } 0 \le m \le h \le F. \quad (2.16)$$

From (2.13) - (2.16), P_{bd} can be computed efficiently using the forward part of the forward-backward algorithm [30].

2.6.4 Numerical Analysis

The blocking probability does not have a close-form expression either, but can be evaluated numerically. Figure 2.7 plots P_{bd} vs. ρ for $F = 120$, $H = 5$, $L = 3$, $\alpha = 0,\ 0.6,\ 0.9,\ P_l = 0.2$. It could be found that ρ has a similar "threshold effect"

on the value of P_{bd} to that in the independent model. In addition, the threshold is increasing with α, which is defined as the percentage of working wavelengths used for inter-domain calls. This, intuitively, is because of the fact that the dependence of wavelength usage introduced by inter-domain calls reduces the blocking probability for a given load ρ. When $\alpha = 0$, the dependent model is reduced to the independent model, and the threshold has the lowest value.

Figure 2.8 plots P_{bd} vs. ρ for $F = 20,\ 40,\ 120$, $H = 5$, $L = 3$, $\alpha = 0.6$, $P_l = 0.2$. We can find that the threshold is increasing with the number of wavelengths F. This is due to the fact that the more wavelengths, the smaller the blocking probability for a given load. The sharpness of the transition also increases with respect to F, suggesting an asymptotic behavior of the blocking probability for a large F.

Figure 2.9 plots the upper bound for the probability of error from Figure 2.7 using Theorem 1. It shows that the value of P_e is small under most load conditions.

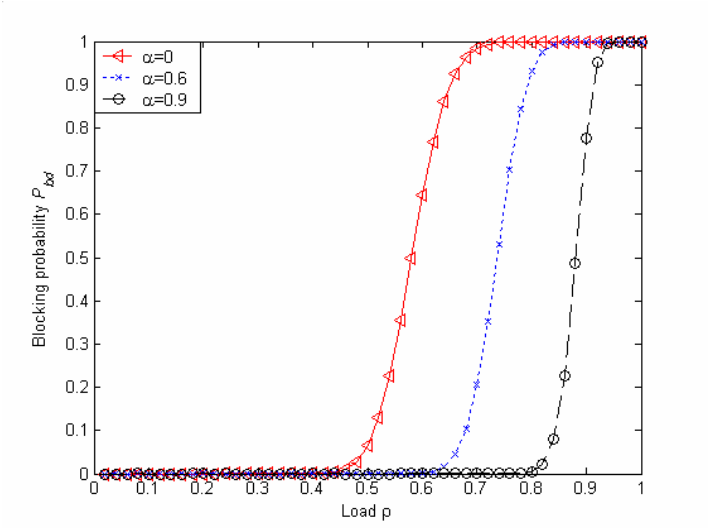

Figure 2.7 Load (ρ) vs. blocking probability (P_{bd}): F=120, H=5, L=3, $\alpha = 0, 0.6, 0.9$, $P_l = 0.2$

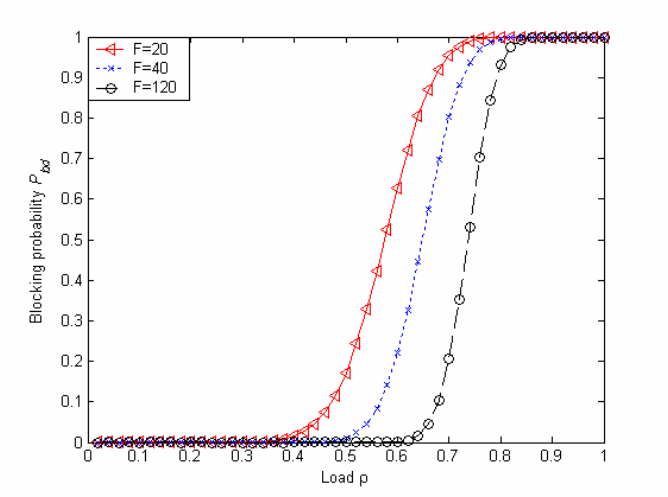

Figure 2.8 Load (ρ) vs. blocking Probability (P_{bd}): F=20, 40, 120, H=5, L=3, $\alpha = 0.6$, $P_l = 0.2$

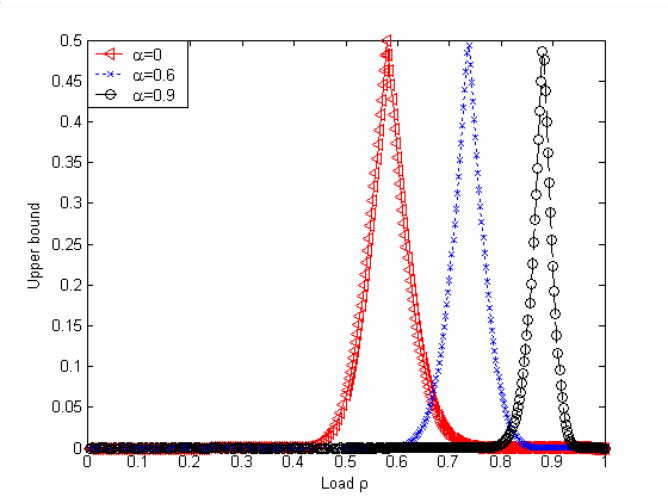

Figure 2.9 Load (ρ) vs. upper bound of P_e : F=120, H=5, L=3, $\alpha = 0, 0.6, 0.9$, $P_l = 0.2$

2.6.5 Special Cases

A question rises why the threshold effect persists for both independent and dependent models. We investigate this question by considering special cases when the number of wavelengths is large, and all the sub-networks are weakly-connected (P_l is large). Under these conditions, analytical form of the blocking probability can be derived.

2.6.5.1 Gaussian Approximation

An important step to obtain a close form expression for the blocking probability is to approximate the joint probability of the local states (N_i's) at wavelength converters. When the number of wavelengths F is large (and L is small), local states at wavelength converters, $X = (N_1, N_2, \cdots, N_L)$, are joint Gaussian random variables with probability $1 - O(\frac{L}{\sqrt{F}})$ [31]. Such a Gaussian distribution can be completely characterized by the means, variances, and covariance of N_i's. Specifically, all N_i's are random variables with the same mean μ and variance σ^2, where

$$\mu = F\rho, \tag{2.17}$$

and

$$\sigma^2 = F\rho(1-\rho). \tag{2.18}$$

The covariance C_{ij} between N_i and N_j for $i \neq j$ characterizes the dependence between two subnets, where

$$C_{ij} = E[N_i N_j] - \mu^2. \tag{2.19}$$

Such dependence can be further characterized through partitioning N_i and N_j into different components,

$$N_i = N_{ii} + M_i, \tag{2.20}$$

and

$$N_j = N_{jj} + M_j, \tag{2.21}$$

where

N_{ii} is the number of wavelengths occupied by local calls at the first hop of the *i-th* subnet;

N_{jj} is the number of wavelengths occupied by local calls at the first hop of the *j-th* subnet;

M_i is the number of wavelengths in the *i-th* subnet occupied by inter-domain calls;

M_j is the number of wavelengths in the *j-th* subnet occupied by inter-domain calls.

Define ρ_g as the correlation coefficient between N_i and N_{i+1}. Then N_i and N_{i+1} have a bivariate normal distribution: $P(N_i, N_{i+1}) \sim Normal(\mu, \mu, \sigma^2, \sigma^2, \rho_g)$. Since $N_1, N_2, ..., N_L$ form a Gaussian Markov Chain, the joint probability distribution of $X = (N_1, N_2, ..., N_L)$ is

$$P(N_1, N_2, ..., N_L) \sim Normal(\underline{\mu}, \Sigma), \tag{2.22}$$

where

$$P(N_1, N_2, \ldots, N_L) = \frac{1}{(2\pi)^{L/2} |\Sigma|^{1/2}} e^{\frac{-(X-\underline{\mu})\Sigma^{-1}(X-\underline{\mu})^T}{2}}, \tag{2.23}$$

$$\underline{\mu} = \left[F\rho, F\rho, ..., F\rho\right]_{1\times L}, \tag{2.24}$$

and

$$\Sigma^{-1} = \begin{bmatrix} a_{11} & a_{12} & 0 & \cdots & 0 & 0 \\ a_{12} & a_{22} & a_{23} & \cdots & 0 & 0 \\ 0 & a_{32} & a_{33} & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & a_{L-1\,L-1} & a_{L-1\,L} \\ 0 & 0 & 0 & \cdots & a_{L\,L-1} & a_{L\,L} \end{bmatrix}_{L\times L}, \tag{2.25}$$

with

$$a_{ii} = \begin{cases} \dfrac{1}{(1-\rho_g{}^2)\sigma^2}, & for\ i = 1\ or\ i = L, \\ \dfrac{1+\rho_g{}^2}{(1-\rho_g{}^2)\sigma^2}, & otherwise, \end{cases}$$

and

$$a_{ij} = -\frac{\rho_g}{(1-\rho_g{}^2)\sigma^2}, \quad for\ i \neq j.$$

It can be shown that

$$\rho_g = \frac{(\rho_2 - P_n)(1-\rho)}{\rho(1-\rho_2)} = (\frac{1-\rho}{\rho})(\frac{\rho\alpha - P_n}{1-\rho\alpha}), \tag{2.26}$$

for all $i = 1, 2, ..., L-1$. (Detailed derivations can be found in *Appendix B*). Two observations can be made here:

(*i*) ρ_g is monotonically decreasing when P_n is increasing. Specifically, when $\rho_2 = P_n$, all the inter-domain calls supported by a network domain exit at the current network domain ($\rho_g = 0$). When $P_n = 0$, all the inter-domain calls are end-to-end connections traversing all the network domains ($\rho_g = \frac{1-\rho}{1-\rho\alpha}\alpha$). Note that we always have $0 \le P_n \le \rho_2$.

(*ii*) ρ_g is monotonically increasing with respect to α. where α is the percentage of inter-domain calls. For instance, when $\alpha = 0$, i.e., all the calls supported by the network are local calls, we have $\rho_g = 0$. When $\alpha = 1$, i.e., all the calls are inter-domain calls, we have $\rho_g = 1 - \frac{P_n}{\rho}$.

2.6.5.2 Weakly-Connected Sub-Networks

When $\rho_g = 0$, all sub-networks are completely decoupled, i.e., each inter-domain call lasts for one subnet ($P_l = 1$). The non-blocking probability of decoupled subnets is

$$P_{ad}^* = \left\{1 - [1 - (1-\rho)(1-\rho_c)^{H-1}]^F\right\}^L, \tag{2.27}$$

where ρ_c is the probability that a wavelength is used for local calls given that it is not used for inter-domain calls, $\rho_c = \rho_1/(1-\rho_2)$. For the non-blocking probability of the independent model, we have in (2.6),

$$P_{ai} = \left\{1 - [1 - (1-\rho)^H]^F\right\}^L.$$

Equation (2.27) bears a similar form to (2.6), and thus it can be shown that there exists a threshold effect in the blocking probability for decoupled subnets similar to that for the independent model.

Of particular interest is when all the sub-networks are weakly connected. When ρ_g is small, all sub-networks are weakly-connected, i.e., a small percentage of the calls are inter-domain calls (α is small), and/or inter-domain calls exit at current subnet with a large probability (P_l is large). For weakly connected sub-networks, we obtain the following theorem through Taylor Expansion:

Theorem 2.2 *For weakly-connected sub-networks, i.e., α is small and/or P_l is large, the non-blocking probability of the dependent model can be expressed as*

$$P_{ad} = P_{ad}^*(1+\eta) + o(\rho_g), \tag{2.28}$$

where P_{ad}^* is the non-blocking probability of the decoupled subnets as given in (2.27), and η is proportional to ρ_g (see Appendix C for details).

It can be found that:

(*i*) When $P_l = 1$, all inter-domain calls last one subnet. Hence all the sub-networks are decoupled, and we have $\eta = 0,\ P_{ad} = P_{ad}^*$.

(*ii*) When P_l is large (e.g., $P_l \geq 0.8$), a small percentage of the inter-domain calls last more than one subnets. Hence the sub-networks are weakly-connected and $P_{ad} \approx P_{ad}^*(1+\eta)$. The non-blocking probability is just that of the decoupled sub-networks plus a small perturbation. Thus we can expect a threshold effect occurs under the weakly-connected sub-networks. The analysis here further explains why the threshold effect persists for both independent and dependent model.

2.7 Simulation Results

For more realistic scenarios with dynamic call arrivals and departures, the Bayesian approach we use would be applicable conceptually. However, the exact *a posterior* probability would be rather complex. Hence, a question is whether or not the static model we use could result in a good approximation. In this section, we investigate this issue through simulation of light-path assessment for dynamic call patterns. Of particular interest is the performance of the analytical bound on P_e, which is derived using the static model in a dynamic setting.

2.7.1 Simulation Setup

We simulate light-path assessment in a network of bus topology with three network domains. Each network domain is assumed to have 5 hops. Connection requests are assumed to obey a Poisson Process with unit exponential holding time. Define λ_l as the arrival rate of connection requests for local calls at each link, and λ_{ij} as the arrival rate of

connection requests for inter-domain calls from domain *i* to domain *j*. Note that the connections between two border nodes of domain *i* are considered as inter-domain calls from domain *i* to domain *i*. Let the total arrival rate to the network be λ, then $\lambda = 15\lambda_l + \sum_{i=1}^{3}\sum_{j=i}^{3}\lambda_{ij}$. Furthermore, following the assumptions in Section 2.6.1, we have

$$\alpha = \frac{\sum_{i=1}^{3}\sum_{j=i}^{3} 5(j-i+1)\lambda_{ij}}{15\lambda_l + \sum_{i=1}^{3}\sum_{j=i}^{3} 5(j-i+1)\lambda_{ij}}, \tag{2.29}$$

$$P_l = \frac{\sum_{i=1}^{m}\lambda_{im}}{\sum_{i=1}^{m}\sum_{j=m}^{3}\lambda_{ij}}, \quad for\ m = 1, 2, \tag{2.30}$$

and

$$\sum_{i=1}^{m}\sum_{j=m}^{3}\lambda_{ij} \equiv const \overset{def}{=} \lambda_{\Delta},\ for\ m = 1, 2, 3. \tag{2.31}$$

λ_{Δ} can be considered as the total arrival rate for inter-domain connections at each network domain. Solving (27-29), we can obtain the arrival rates for connection requests with different sources and destinations as follows:

$$\begin{aligned} &\lambda_l = \frac{(1-\alpha)}{\alpha}\lambda_{\Delta}, \\ &\lambda_{11} = \lambda_{\Delta}P_l,\ \lambda_{12} = \lambda_{\Delta}P_l(1-P_l),\ \lambda_{13} = \lambda_{\Delta}(1-P_l)^2, \\ &\lambda_{22} = \lambda_{\Delta}P_l^2,\ \lambda_{23} = \lambda_{\Delta}P_l(1-P_l), \\ &\lambda_{33} = \lambda_{\Delta}P_l, \end{aligned} \tag{2.32}$$

where $\lambda_{\Delta} = \frac{\lambda\alpha}{15-(14-2P_l)\alpha}$.

For a specific network load ρ, we adjust the total traffic arrival rate to the network λ to be either high or low, so that the probability that a wavelength is used in the network remains approximately ρ.

The simulator is based on discrete event simulation. For each simulation, 10 runs are performed where each run consists of 100,000 end-to-end connection requests. Four decisions may result from light-path assessment using the partial information discussed previously: (i) correct acceptation (*CA*), (ii) incorrect acceptation (*IA*), (iii) correct rejection (*CR*), and (iv) incorrect rejection (*IR*). The probability of error is obtained as the percentage of *IA* and *IR* out of all the decisions.

2.7.2 Simulation Results

Figure 2.10 depicts the probability of error for light-path assessment using aggregated information with $F = 40$, $\alpha = 0.6$, and $P_l = 0.2$. The reason for choosing these parameters are: (1) more wavelengths would be used for inter-domain calls than for local calls; (2) a large percentage of inter-domain calls supported by one network domain would be calls passing through that domain.

The simulation result confirms the threshold effect that is predicted by the analytical model and shows the good performance of the analytical bound. We can find that, using Bayesian approach based on only aggregated information and the static model, P_e is neglible under most load conditions; and P_e increases to its peak exponentially when the load is close to the threshold. Furthermore, the static model predicts the threshold of the load accurately. For Figure 2.10, $\rho_{threshold} \approx 0.65$.

Figure 2.11 shows the simulation results for $F = 80$, $\alpha = 0.6$, and $P_l = 0.2$. It also confirms that the Bayesian approach could give us a small P_e except when the load is in a small region close to the threshold. When the load is close to the threshold ($\rho_{threshold} \approx 0.71$ for Figure 2.11), P_e increases to its peak exponentially. Because of its static nature, the dependent model used in simulation cannot capture the instantaneous blocking probability of the network carrying dynamic traffic with 100% accuracy. Therefore, the probability of error exceeds 0.5 when the load is at the threshold. However, simulation results confirm that it is possible to achieve a probability of error close to 0 using only aggregated information under most load conditions.

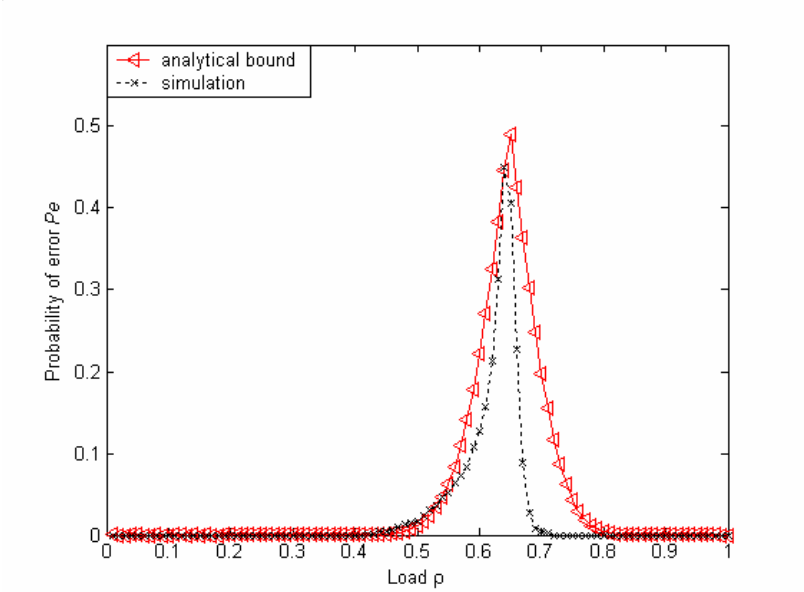

Figure 2.10 Analytical bound and simulated P_e : *F=40*, *H*=5, *L=3*, $\alpha = 0.6$, $P_l = 0.2$

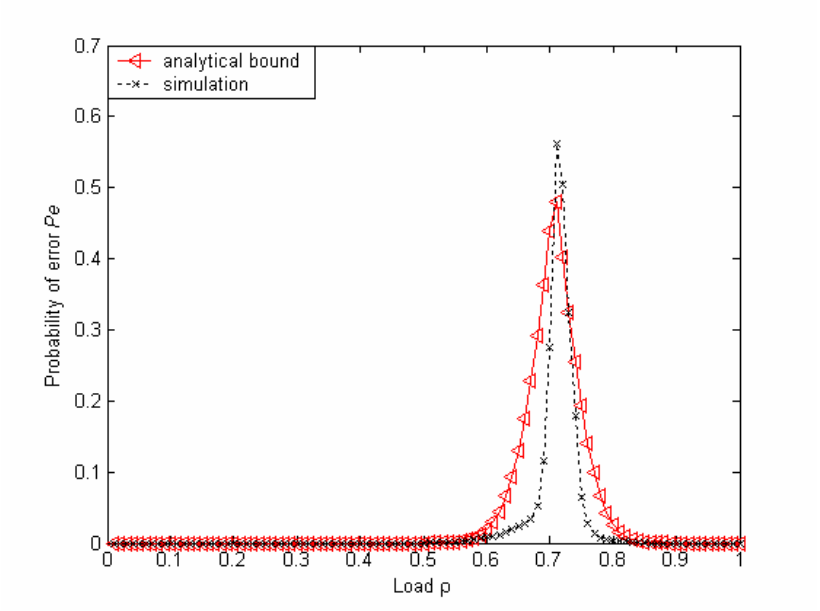

Figure 2.11 Analytical bound and simulated P_e : $F=80$, $H=5$, $L=3$, $\alpha = 0.6$, $P_l = 0.2$

2.8 Summary of Chapter 2

In this Chapter, we have investigated network management information for light-path assessment across administrative domains (subnets). Our focus has been on studying the scalability of management information, which includes aggregated information of each subnet, and local information from wavelength converters on network boundaries.

We have formulated the problem based on decision theory, and defined the performance of using partial management information through the Bayes probability of error. A bound in terms of blocking probability is derived to estimate such a performance. We then defined the scalability of management information as the growth rate with respect to network size and resource when a desired performance is achieved.

A scalable case has been studied where the partial management information grows only logarithmically with the number of wavelengths per link. Our study reveals that when the number of wavelengths is large, the resulting Bayes error is negligibly small for

most of the network load conditions. Therefore, a small loss in performance (the Bayes error) may be traded off with a large saving in network management information. In other words, the abundant network resource, which is the large number of wavelengths in future WDM networks, may make it possible to reduce the amount of network management information while achieving a good performance.

CHAPTER 3

RESILIENCE OF ALL-OPTICAL NETWORKS UNDER IN-BAND CROSSTALK ATTACKS: A GRAPHICAL MODEL APPROACH

3.1 Introduction of Chapter 3

All-optical network (AON) has been considered as a promising technology for next-generation optical networks. However, AONs are susceptible to malicious attacks as the signals remain in optical domain within the network and are difficult to be monitored closely [32]. Due to the high data rate supported by AONs, even attacks of a short duration can result in a large amount of data loss. Hence, security of AONs upon attacks has become an important issue, where an open question is how to incorporate security against attacks in the design and engineering of AON architectures. Investigations of this question are important as AONs are still at an early stage of implementation and ground-up developments of secure all-optical networks are possible [32]. The goal of this work is to study how network architecture impacts resilience in the context of in-band crosstalk attacks in AONs.

Crosstalk attacks were first studied in [32]. Crosstalk in AONs is caused by signal leakage among different inputs at non-ideal network devices, e.g. optical switches. The most detrimental type of crosstalk is in-band crosstalk, where the crosstalk element is within the same wavelength as the signal [34]. In-band crosstalk attacks can happen at fiber links or network nodes. In this work, we consider the case where an attacker gains legitimate access to a network node and inserts a flow with strong signal power into the

network [33][34]. Due to the crosstalk effects of wavelength switches, a small fraction of the signal from the attack channel may leak into other normal channels in the shared switching plane. The leakage superimposed onto normal channels may exceed a predetermined threshold for a quality of service requirement, such that those channels are considered to be affected by the attack at network nodes.

AONs are susceptible to crosstalk attacks. Major applications of AONs include metropolitan area networks (MANs) and wide area networks (WANs), but MANs and WANs are not 100% secure. As AON grows in span and functionality, it has the potential to provide services to a wider set of applications in the future, e.g. analog services, novel applications that require optical interfaces. Therefore, there is an increasing demand for access of the AON from outside parties, i.e., partners and customers of service providers may also have limited management access to the network, which poses an increasing threat to optical network security [35]. A wider set of users and the increasingly open platform of optical networks entail a higher risk of user misue of the network, which is evidenced by the security threats such as denial-of-service attack and worm attack in the current Internet [34]. The Internet Infrastructure has a large scale and is accessed by hundreds of millions of users with different interests. Therefore, it constantly faces the threat of human operational errors, spreading of software virus, and malicious attacks [3]. It is expected that the risk of crosstalk attacks could be higher when the AON higher when the AON paradigm is fully implemented.

There have been several research activities aiming to mitigate the threats of crosstalk attacks in AONs. Attack detection based on node wrappers is studied in [34]. A distributed algorithm for attack localization is presented in [36]. Necessary and sufficient

conditions for crosstalk attack localization are investigated in [33]. General frameworks for managing faults and alarms in AON are discussed in [37][38][39]. All these approaches are reactive in nature. Furthermore, certain crosstalk attacks are difficult to detect [34]. For instance, sporadic crosstalk attacks may disrupt service but "disappear" before it can be detected. Thus, there remains a basic question: *How resilient is an AON upon crosstalk attacks before the attacks are detected and eliminated from the network?* This motivates our study of resilient AON architectures against crosstalk attacks. In a more general context, using cross-talk attacks as an example, we hope to provide an understanding on how network architectures may affect network security in the presence of attackers.

We focus on three components of network architectures against crosstalk attacks: (a) physical layer optical devices, (b) physical topology, and (c) wavelength usage at the network layer, which is determined by network layer traffic. The goal is to quantify the effects of these factors against crosstalk attacks. One major challenge encountered in this study is to characterize the interactions of the three factors of network architecture during crosstalk attack propagation. For instance, attacks propagate to active wavelength channels of the same wavelength as the attacker's flow. Meanwhile, wavelength usage at the network layer is dependent because of the sharing of network links among different connections. Therefore, we need an approach that can provide an explicit representation of the cross-layer interactions.

We apply probabilistic graphical models to mode cross-layer attack propagation [40]. Probabilistic graphical models include directed probabilistic graphs (Bayesian Belief Networks) and undirected probabilistic graphs (Markov Random Fields), and have been

widely studied in machine learning and information theory [41][42]. Yet, probabilistic graphical models have just begun to see applications in networking (see Section 3.8 for detailed discussions). In particular, at the physical layer, we develop a directed probabilistic graph to model attack propagation under static network traffic and a given source of attack. At the network layer, we apply an undirected probabilistic graph to represent the probability distribution of active connections. The physical- and the network-layer models together form a cross-layer model that has a factor graph representation [43].

The cross-layer model is developed using a bottom-up approach and provides an explicit representation of the complex dependencies between the physical- and the network-layer. Furthermore, the graphical models facilitate the analysis of multiple factors from network architecture on network resilience. For regular topologies, we derive bounds on the network resilience. For irregular/large topologies, the cross-layer model provides computationally efficient methods for studying the resilience where the analysis is not feasible.

The remainder of Chapter 3 is organized as follows. Section 3.2 describes the problem formulation. Section 3.3 presents the attack propagation model under static traffic and a given source of attack based on directed probabilistic graph. Section 3.4 introduces the network-layer representation using undirected probabilistic graph. Section 3.5 discusses about the cross-layer model based on factor graph. Section 3.6 investigates the impacts of physical layer on network resilience. Section 3.7 studies the effects of the network layer on resilience. Section 3.8 briefly reviews graphical models in networking research. Section 3.9 concludes the chapter.

3.2 Problem Formulation

The topology of an AON is defined as an undirected graph $G(\mathbf{V}, \mathbf{E})$, with $\mathbf{V}$ being the set of nodes and $\mathbf{E}$ being the set of bi-directional links. Denote $V_i \sim V_j$ if there is one bi-directional link between V_i and V_j, $V_i, V_j \in \mathbf{V}$. Let $\mathbf{R}$ be a finite set of routes in the network. Assume that there are no wavelength converters in the AON. We define a connection on route r, $r \in \mathbf{R}$, as a bi-directional light-path on route r that consists of one unidirectional flow in each direction.[1] Assume that each wavelength can only be used by one active connection on the same network link.

This work considers single-source in-band crosstalk attacks. That is, crosstalk attack is started at the source node of a unidirectional flow on wavelength λ, and propagates to flows that use the same wavelength. As this work focuses on in-band crosstalk attacks, "flows", "connections'', and "channels" are used in the rest of Chapter 3 without referring to their associations with wavelength λ where no ambiguity occurs.

The problem we consider consists of three aspects: (a) developing the cross-layer model of attack propagation, and (b) using the model to quantify the network resilience upon crosstalk attacks. Let S_i be a random variable that denotes the number of active channels affected by the in-band crosstalk attack at the switching plane of node V_i. Vector $\mathbf{S} = (S_i : V_i \in \mathbf{V})$ corresponds to the number of affected channels at each node in the network. Let N_{ij} denote the status of route r_{ij}, where $N_{ij} = 1$ if there is an active

---

[1] Each bi-directional link consists of two optical fibers, one for each direction. Throughout Chapter 3, the term "connection" is used specifically for bi-directional traffic; the term "flow" is used to refer to uni-directional traffic.

connection on route r_{ij} between node V_i and V_j, for $r_{ij} \in \mathbf{R}$; $N_{ij} = 0$, otherwise. Vector $\mathbf{N} = (N_{ij} : r_{ij} \in \mathbf{R})$ then represents the status of all network routes in $\mathbf{R}$. Denote f_{sd} as the flow starting from node s and terminating at node d, we need to obtain the following quantities to characterize attack propagation:

(a) $P(\mathbf{S} \mid \mathbf{N} = \mathbf{n},\ R_f = f_{sd})$: The probability of the number of channels affected at each network node given the status of network routes $\mathbf{n}$ and the source of attack R_f, where R_f denotes the unidirectional flow where the attack originates. This probability represents attack propagation under static network traffic $\mathbf{n}$ and a given source of attack f_{sd}, and is to be characterized through a directed probabilistic graph in Section 3.3.

(b) $P(\mathbf{N} \mid R_f = f_{sd})$: The probability of the status of network routes given the source of attack, which is to be described using an undirected probabilistic graph in Section 3.4.

(c) $P(\mathbf{S} \mid R_f = f_{sd})$: The probability of the number of channels affected at each node given the source of attack, which models attack propagation under dynamic traffic. This probability combines the physical- and the network-layer models from (a) and (b), and shall be described with a factor graph representation in Section 3.5.

The cross-layer model is then used to study network resilience based on the network resilience loss and average network resilience loss defined as follows.

Definition 3.1 *Given that there is a crosstalk attack started on flow f_{sd}, the network resilience loss is defined as*

$$M_{f_{sd}} = \sum_{V_i \in \mathbf{V}} E_{f_{sd}}[S_i], \tag{3.1}$$

where $E_{f_{sd}}[S_i] = \sum_{S_i} s_i P(S_i = s_i \mid R_f = f_{sd})$ *is the expected number of affected channel at node* V_i *given the source of the attack.* $M_{f_{sd}}$ *denotes the total number of active channels affected when the attack starts from a particular flow.*

Definition 3.2 *The average network resilience loss of the network is defined as* $M = E_{R_f}[M_{f_{sd}}]$, *where* $E_{R_f}[\,]$ *stands for the expectation over the source of the attack* R_f, *i.e.,*

$$M = \sum_{f_{sd}} M_{f_{sd}} P(R_f = f_{sd}), \tag{3.2}$$

where

$$P(R_f = f_{sd}) = \frac{1}{2 \mid \mathbf{R} \mid} P(N_{sd} = 1). \tag{3.3}$$

Here we assume that each network route in $\mathbf{R}$ is equally likely to be an attacker's route, and the attack is started on one of the two unidirectional flows on the attacker's route with an equal probability.

3.3 Physical-Layer Attack Propagation Model: Directed Probabilistic graph

We first model attack propagation under static network traffic and a given source of attack.

3.3.1 Background of In-Band Crosstalk Attack

We focus on in-band crosstalk attacks where an attacker gains legitimate access to the network and injects signal of high power into one flow. Due to imperfect switching arrays, the attacker's channel may affect other channels that share the switching plane, causing malfunctions at several locations in the network. Figure 3.1 depicts an example

of in-band crosstalk attack. At each network node, channels of the same wavelength from different input fibers share the same switching plane [44]. Suppose that the crosstalk is initiated on flow $C1$ using wavelength λ_1 from input fiber 1. All the wavelength channels that share a switching plane with $C1$, e.g. channel $C2$ from input 2, may be contaminated by $C1$'s power leakage.

In particular, we define a network node as being affected by the attack if the amount of in-band crosstalk incurred by normal[2] channels at the switching plane of that node exceeds a predetermined threshold. Clearly, each node along the attacker's route may be affected by the attack due to the high signal power of the attack flow, but the chance for nodes that are not on the attacker's route to be affected by the attack is negligible. That is, normal flows affected by the attack flow at one or more network nodes along the attacker's route do not have attacking capability, as its signal power is unlikely to be increased by more than half the normal channel power. For instance, consider the example in Figure 3.1. Suppose, at one time instant, the attacker's jamming power is 20dB higher than the normal channel power and the optical switches have a crosstalk ratio of -35 dB. Then the power of flow C2 is increased by around -15dB of the normal channel power at node 1. The power of flow C2 at node 2 is in the same order, as in node 1, whose crosstalk leakage to flow C3 is negligible given the crosstalk ratio of –35dB. Currently, optical switches with crosstalk ratios much less than -35dB are commercially available [45]. Thus, in this work, we ignore the in-band crosstalk caused by normal flows and assume that only nodes along the attacker's route may be affected by the

[2] Normal channels refer to channels in the network that are not the attacker's channel.

attack. In addition, attack propagates to all the active channels that share the switching plane with the attacker's channel at each affected node. Based on these assumptions, we shall describe the probabilistic attack propagation model in the next subsection.

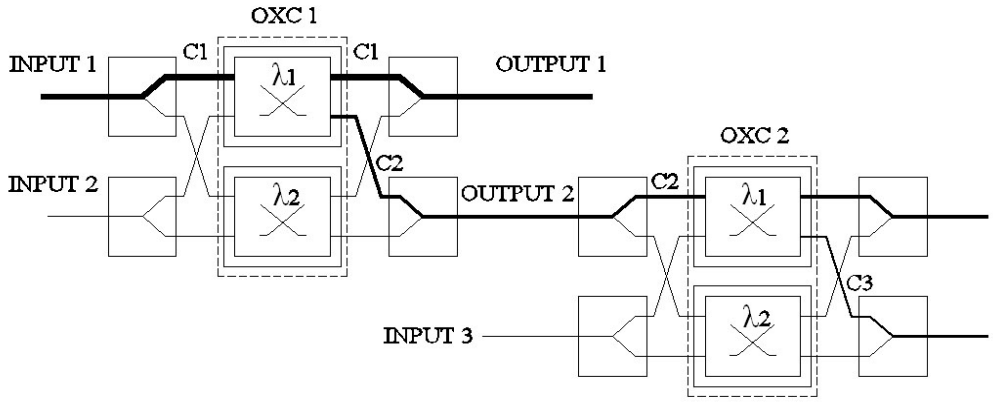

Figure 3.1 Crosstalk attack propagation in AON

3.3.2 Probabilistic Attack Propagation Model

Consider a crosstalk attack started at node s on flow f_{sd}. We index the set of nodes traversed by flow f_{sd} as $\mathbf{V}_{f_{sd}} = \{V_1, V_2, ..., V_k\}$, with V_1 and V_k being the source and destination node. The attack propagation is characterized by the status of each node in $\mathbf{V}_{f_{sd}}$ and the status of wavelength channels at those nodes. We define the status of node V_i as a binary variable X_i. Specifically, let the signal power of a normal flow at the switching plane of each node be u_n when there is no attack in the network. Let the crosstalk ratio of the switches in the network be l_c and let c_{th} be a predetermined constant. Then $X_i = 1$ if the amount of in-band crosstalk incurred by a normal channel at the switching plane of node V_i exceeds $c_{th}u_n$; $X_i = 0,$ otherwise. Furthermore, we denote node V_i as being affected by the attack if $X_i = 1$.

There are several motivations to define the status of each node under attack as a binary variable. First, the amount of in-band crosstalk at each node under attack may have a wide range of values. For simplicity, we aggregate it into two levels, which corresponds to whether a predetermined threshold is exceeded or not. Second, in network fault/attack management, the status of each network component is generally defined as a binary variable, i.e., an "up" state, which means that the component is operational, and a "down" state, which means that the component can not operate properly. Finally, in very often the network information available from attack detection and monitoring is whether the predetermined threshold or service guarantee is violated or not due to the attack, rather than the exact value of the level of crosstalk.

Clearly the status of each node in $\mathbf{V}_{f_{sd}}$ is determined by the strength of flow f_{sd}'s jamming power at that node. If f_{sd}'s jamming power has a constant value at node V_1, its jamming power at other nodes along the route depends on the characteristics of optical devices and remains non-random. Then the status of each node and how far the attack can propagate are fixed, which can be characterized using a deterministic model of crosstalk attack propagation ([33][38]).

However, in this work, our focus is to study the impacts of network architectures against crosstalk attacks in general, where the attacker's jamming power at the source of attack is unknown and has a wide range of values in different cases. Therefore, we assume that the attacker's jamming power is a random variable following certain probability distribution. Consequently, the status of network nodes under crosstalk attack becomes random, which leads to a probabilistic model of attack propagation. Intuitively, if the attacker's jamming power has a higher probability of being large; it is more likely

the attack propagates to nodes farther away from the source node of the attack [39]. Next we derive the probabilistic models of attack propagation.

We consider the attenuation of flow f_{sd}'s jamming power along its route. Denote the signal power of flow f_{sd} in the switching plane of node V_i as a random variable $U_i,\ i=1,2,...k.$ The attenuation of f_{sd}'s jamming power along its route can be captured using deterministic composite functions that depend on the characteristics of optical devices. For simplicity of illustration, we consider an example in Figure 3.2.

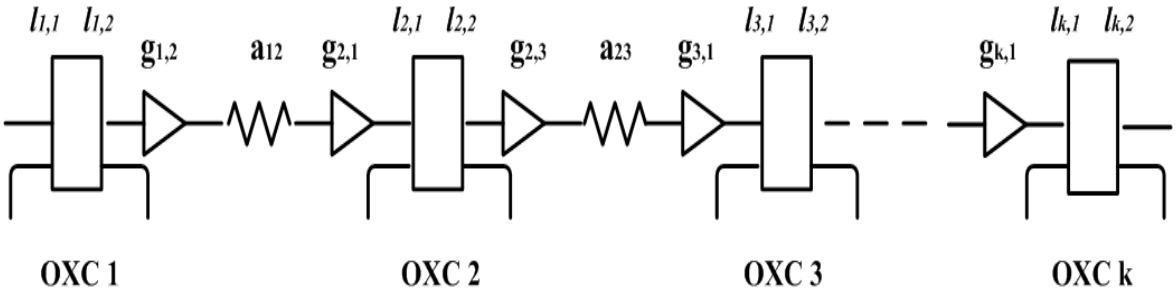

Figure 3.2 Illustration of signal power attenuation: the attacker's flow

We assume that there are input erbium-doped fiber amplifier (EDFA) and output EDFA at each side of a node respectively. Furthermore, we define the following parameters:

$l_{i,1}$: Signal loss ratio of node V_i before the flow enters the switching plane, which mainly includes signal loss at demultiplexer.

$l_{i,2}$: Signal loss ratio of node V_i after the flow enters the switching plane, which mainly includes loss at switching plane and multiplexer.

$a_{i,j}$: Signal loss ratio of the fiber span between node V_i and node V_j.

$g_{i,1}(\,)$: The gain of the EDFA at the input side of node V_i.

$g_{i,2}(\,)$: The gain of the EDFA at the output side of node V_i.

For a given network, $l_{i,1}, l_{i,2}, a_{i,j}$ are constants; $g_{i,1}(\,)$ and $g_{i,2}(\,)$ are deterministic non-linear functions of the input power to amplifiers. In this work, we adopt the following gain model for EDFAs [46]:

$$g_{ij}(P_{input}) = \begin{cases} d_{ij}, & if\ P_{input} \le p_{th}, \\ 1 + \dfrac{p_{sat}}{P_{input}} \lg \dfrac{g_0}{g_{ij}(P_{input})}, & otherwise, \end{cases} \tag{3.4}$$

where, P_{input} is the total input power; p_{sat} is the internal saturation power; g_0 is the small signal saturated gain; p_{th} is the input power threshold for successful gain clamping, and d_{ij} is the clamped gain value.

Assume that the attacker's flow (f_{sd}) does not share EDFAs with other flows. This corresponds to a conservative view of the jamming power attenuation and a worst-case scenario of in-band attack propagation, as all the photons of the EDFAs are used to amplify the attacker's signal. Then,

$$U_{i+1} = l_{i+1,1}\pi_{i+1,1}(a_{i,i+1}\pi_{i,2}(l_{i,2}U_i)), \tag{3.5}$$

where $\pi_{i,j} = P_{input} g_{i,j}(P_{input})$ is the output power of the EDFA with gain $g_{i,j}(P_{input})$ and input power P_{input}. Then composite function $\tau_{j-1,j}(\tau_{j-2,j-1}(...\tau_{i,i+1}(.)))$ capture the attenuation of the jamming power between node V_i and V_j.

Assume that, when there is no crosstalk attack in the network, amplifiers on each fiber operate in the gain clamped regions and make up the signal attenuation between two nodes. Furthermore, assume that the attacker's jamming power at the source node of the

attack follows a cumulative distribution function $\eta(U)$ with minimum power $u_{\min}$, $u_{\min} \geq c_{th} u_n / l_c$, and maximum power $u_{\max}$. Then, it can be shown that the status of each node along the attacker's route, $X_i, i = 1, 2, ..., k$, form a Markov Chain. Specifically,

$$P(X_1 = 1) = 1. \tag{3.6}$$

$$P(X_{i+1} \mid X_1, X_2, ..., X_i) = P(X_{i+1} \mid X_i), \quad i = 1, 2, ..., k-1. \tag{3.7}$$

$$P(X_{i+1} = 1 \mid X_i = 0) = 0. \tag{3.8}$$

$$P(X_{i+1} = 1 \mid X_i = 1) = \frac{P(U_{i+1} > c_{th} / l_c)}{P(U_i > c_{th} / l_c)} = \frac{1 - \eta(\delta_{1,i+1})}{1 - \eta(\delta_{1,i})}, \tag{3.9}$$

where $\delta_{1,i}, 1 \leq i \leq k-1,$ corresponds to the minimum value of jamming power at node V_1 such that attack can propagate to node V_i, and satisfies

$$\tau_{i-1,i}(\tau_{i-2,i-1}(...\tau_{1,2}(\delta_{1,i}))) = c_{th} u_n / l_c. \tag{3.10}$$

The derivation of (3.7) to (3.9) can be found in *Appendix D*.

Hence, given the non-deterministic nature of flow f_{sd}'s jamming power at the source node of attack, the status of each network node are random. How likely the crosstalk attack may propagate to other nodes along the attacker's route is represented by the Markov chain in (3.6) to (3.9). Intuitively, the status of each network node along the attacker's route forms a Markov Chain because: (1) the status of each node is defined as a binary variable and is determined by the attacker's jamming power at that node, and (2) the attacker's jamming power at node V_{i+1} is a non-increasing function of that at node V_i. It should be noted that, in this work, the probabilistic model of attack propagation is derived to characterize attack propagation in general, when the exact value of the jamming power at the source of attack is unknown or random. Given a constant and

known jamming power at the source of attack, a deterministic model is sufficient to capture attack propagation.

The conditional probabilities in (3.9) can take different forms depending on $\eta(U)$. If we further assume that the attacker's jamming power at the source node of the attack is uniformly distributed in $[u_{\min}, u_{\max}]$, (3.9) can be rewritten as

$$P(X_{i+1}=1 \mid X_i=1)=\frac{\max\{0, u_{\max}-\max\{u_{\min}, \delta_{1,i+1}\}\}}{u_{\max}-\max\{u_{\min}, \delta_{1,i}\}}, \tag{3.11}$$

where $\delta_{1,i}, 1 \le i < k$, is defined in (3.10).

For simplicity, we denote

$$P(X_{i+1}=1 \mid X_i=1)=\alpha_i, \tag{3.12}$$

where $\alpha_i=\frac{1-\eta(\delta_{1,i+1})}{1-\eta(\delta_{1,i})}$. In the rest of Chapter 3, we assume that α_i's are known.

Next we consider the number of active channels affected by the attack at the switching plane of node V_i. Let $\mathbf{R}_{ij}$ be the set of network routes that use link ij. Under static traffic, $\sum_{r_{uv}\in\mathbf{R}_{ij}} n_{uv}$ corresponds to the number of flows that enter the switching plane of node V_i through link ij; $\sum_{r_{ih}\in\mathbf{R}_{ij}} n_{ih}$ corresponds to the number of flows that are locally originated from node V_i and enter the network through link ij. Hence, under static network traffic, the total number of affected channels at the switching plane of V_i, $V_i \in \mathbf{V}_{f_{sd}}$, is given by

$$P(S_i = s_i \mid X_i = x_i, \mathbf{N} = \mathbf{n}, R_f = f_{sd})$$
$$= \begin{cases} 1, & if\ s_i = \sum_{V_i \sim V_j} \{\sum_{r_{uv} \in \mathbf{R}_{ij}} n_{uv} + \sum_{r_{ih} \in \mathbf{R}_{ij}} n_{ih}\} \,\&\, x_i = 1, \\ & \quad or \\ & s_i = 1 \,\&\, x_i = 0, \\ 0, & otherwise. \end{cases} \tag{3.13}$$

This means that, when node V_i is affected by the attack, all the active channels at the switching plane of V_i are affected by the attack; otherwise, if node V_i is not affected by the crosstalk attack, only one, i.e., only the channel used flow f_{sd} itself, is affected by the attack at the node.

Combining (3.12) and (3.13), we have the physical-layer attack propagation model,

$$P(\mathbf{S}_{f_{sd}} \mid \mathbf{N} = \mathbf{n},\ R_f = f_{sd}) =$$
$$\sum_{\mathbf{X}_{f_{sd}}} \prod_{i=1}^{k-1} P(X_{i+1} \mid X_i, R_f = f_{sd}) \prod_{i=1}^{k} P(S_i \mid X_i, \mathbf{N} = \mathbf{n}, R_f = f_{sd}), \tag{3.14}$$

where $\mathbf{S}_{f_{sd}} = (S_i : V_i \in \mathbf{V}_{f_{sd}})$, and $\mathbf{X}_{f_{sd}} = (\mathbf{X}_i : V_i \in \mathbf{V}_{f_{sd}})$, which is the status of nodes in the attacker's route.

Therefore, under static network traffic (given $\mathbf{N} = \mathbf{n}$), $(X_i, S_i : V_i \in V_{f_{sd}})$ forms a directed probabilistic graph (Bayesian Belief Network). Each node in the probabilistic graph represents either X_i or S_i. There is one directed edge from X_i to X_{i+1} and one directed edge from X_i to S_i respectively. Note that, given $\mathbf{N} = \mathbf{n}$ and $X_i = x_i$, S_i is deterministic, but S_i is included for an explicit graphical representation of attack propagation.

Figure 3.3 shows an example of a simple mesh network where all the routes in $\mathbf{R}$ are marked in dashed lines. Suppose that the crosstalk attack is started on flow *BD*. The directed probabilistic graph representation of attack propagation is shown in Figure 3.4.

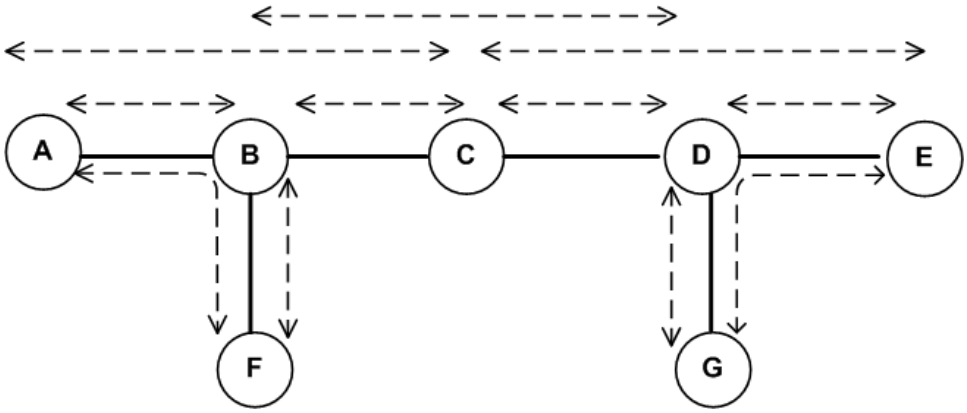

Figure 3.3 A mesh network with 11 routes

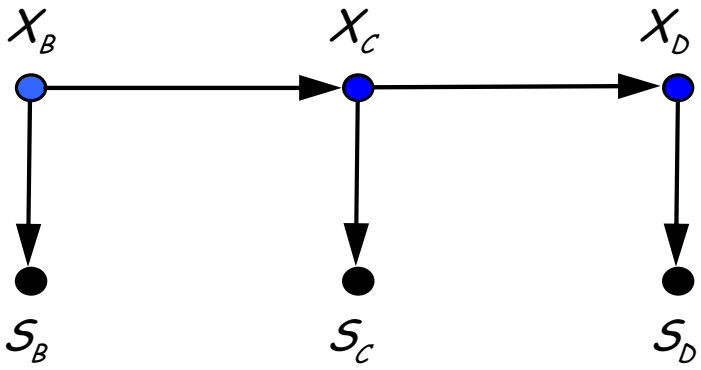

Figure 3.4 Directed probabilistic graph representation of attack propagation: attack started on flow *BD*; mesh network in Figure 3.3

Due to the complexity of modeling AON signal transmission, the physical-layer model in this work is developed with stringent assumptions, i.e.: (1) the in-band crosstalk due to channels with normal signal power and/or nonlinear effects is ignored; (2) under normal operations, the EDFAs work at gain-clamped region and make up for the signal losses between two network nodes; (3) the optical switches have the same crosstalk ratio and threshold of crosstalk leakage for the definition of node affection.

Assumption 1 is reasonable because of the low crosstalk ratio of current optical switches. If assumption 2 is relaxed so that the EDFAs work at gain-clamped region

under normal operations, but may make up for more than the signal losses between two network nodes, then the status of nodes along the attacker's route may still form a Markov Chain, however, the order of nodes in the Markov Chain does not necessarily follow the sequence of $X_1, X_2, ..., X_k$. The same is true if we relax assumption 3, so that optical switches in the network have different crosstalk ratios or the thresholds of crosstalk leakage for the definition of node affection are heterogeneous for different nodes.

The physical layer model characterizes attack propagation under static network traffic. Under dynamic traffic, however, the status of each network route $N_{sd}, r_{sd} \in \mathbf{R}$, is random and can be characterized using a network layer model.

3.4 Network-Layer Model: Undirected Probabilistic graph

To obtain the network layer model, we need to obtain $P(\mathbf{N} \mid R_f = f_{sd})$, which is the probability distribution of route status given the source of the attack. From (3.3), we have

$$P(\mathbf{N} \mid R_f = f_{sd}) = P(\mathbf{N} \mid N_{sd} = 1). \tag{3.15}$$

Then it suffices to find $P(\mathbf{N})$, which can be characterized by undirected probabilistic graph.

3.4.1 Undirected Probabilistic Graph

An undirected probabilistic graph can be represented as $\mathbf{G = (V, E)}$ [40], where $\mathbf{V}$ represents the set of vertices, and $\mathbf{E}$ represents the set of edges. Each node $V_i \in \mathbf{V}$ represents a random variable. A subset of nodes $\mathbf{V_C}$ is said to separate two other subsets

of nodes $\mathbf{V_A}$ and $\mathbf{V_B}$ if every path joining every pair of nodes $V_i \in \mathbf{V_A}$ and $V_j \in \mathbf{V_B}$ has at least one node from $\mathbf{V_C}$ [40]. An undirected probabilistic graph implies a set of conditional independence relations. That is, for any disjoint subsets of nodes in the undirected graph, $\mathbf{V_A}$, $\mathbf{V_B}$, and $\mathbf{V_C}$, if $\mathbf{V_C}$ separates $\mathbf{V_A}$ and $\mathbf{V_B}$, then $\mathbf{V_A}$ and $\mathbf{V_B}$ are conditional independent given $\mathbf{V_C}$. For example, Figure 3.5 shows an undirected probabilistic graph with 5 variables. As node V_2 and V_3 separate node V_1 from nodes in the rest of the network, $P(V_1 \mid V_2, V_3, V_4, V_5) = P(V_1 \mid V_2, V_3)$. Obviously, a node is separated from other nodes in the undirected graph by all its neighbors.

A clique denotes a subset of $\mathbf{V}$ that contains either a single node or several nodes which are all neighbors of one another. Then the joint probability distribution of $\mathbf{V}$ has a product form [40]:

$$P(\mathbf{V}) = Z^{-1} \prod_{q \in C} \psi_q(\{V_i : V_i \in \mathbf{V_q}\}), \tag{3.16}$$

where Z is the normalizing constant, $Z = \sum_{\mathbf{V}} \prod_{q \in C} \psi_q(\{V_i : V_i \in \mathbf{V_q}\})$; ψ_q is a non-negative function defined for clique $\mathbf{V_q} \in \mathbf{C}$, and $\mathbf{C}$ denotes the set of all the cliques in the graph $\mathbf{G}$.

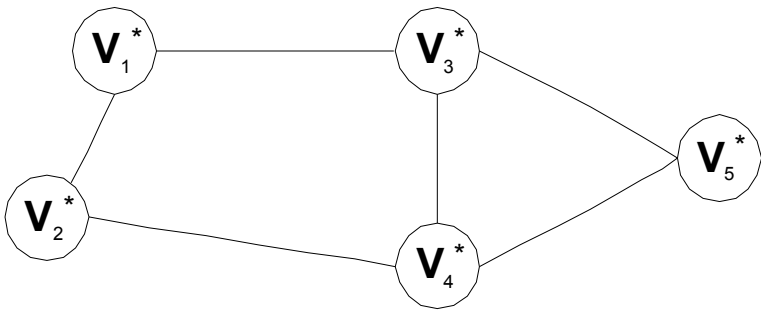

Figure 3.5 An undirected probabilistic graph

3.4.2 Network-Layer Model

The network-layer model is formed as follows. Each vertex in the undirected probabilistic graph represents the status of a route $N_{ij}, r_{ij} \in R$. Furthermore, the status of all network routes that share the same link forms a clique. In [47], it has been shown that the steady state distribution of the number of calls in progress in loss networks without control form a Markov Random Field (MRF), which is one type of undirected probabilistic graph. Here we generalize the MRF representation in [47] to an undirected probabilistic graph representation, and include the dependence among different routes due to the capacity constraint and the network load explicitly in the undirected graph.

We revisit the example of mesh network in Figure 3.3, whose network-layer model is shown in Figure 3.6. Consider route *AC*, which traverses two network links: *AB* and *BC*. Meanwhile, link *AB* is in route *AB* and route *AF*; link *BC* is in route *BC* and route *BD*. Since wavelength λ can only be used by one connection on each network link, route *AC* has a contention of wavelength usage with route *AB*, *AF*, *BC*, and *BD*. However, once the status of route *AB*, *AF*, *BC* and *BD* is known, the status of route *AC* can be determined without violating the capacity constraints. Hence, routes *AB*, *AF*, *BC* and *BD* are neighbors of route *AC* and separate route *AC* from routes in the rest of the network, as shown in Figure 3.6.

Therefore, by defining routes that share the same network link as neighbors, we capture the capacity constraint in the undirected probabilistic graph. The probability distribution of all network routes can be obtained by specifying proper clique potentials based on (3.16). The clique potentials in this work are selected to characterize both the dependencies among different network routes and the varying network load.

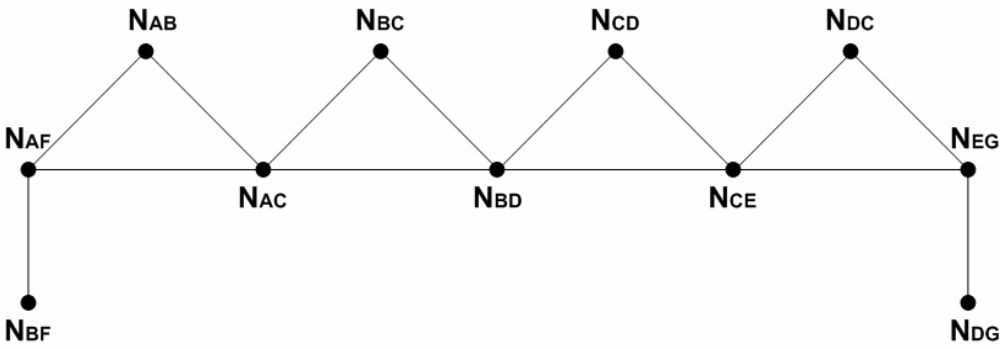

Figure 3.6 Undirected probabilistic graph representation of network routes; mesh network in Figure 3.3

In Section 3.2, we denote $\mathbf{R}_{ij}$ as a subset of routes in $\mathbf{R}$ that traverse link ij. A clique, denoted as C_{ij}, can then be formed with all the routes in $\mathbf{R}_{ij}$. Then the potential function of C_{ij}, denoted as ψ_{ij}, is obtained as follows: (1) $\psi_{ij} \neq 0$ if and only if the capacity constraint is satisfied, i.e., at most one route in $\mathbf{R}_{ij}$ is active; (2) if the wavelength is used on link ij, then $\psi_{ij} = \gamma_{ij}$; otherwise, $\psi_{ij} = 1 - \gamma_{ij}$, $0 < \gamma_{ij} < 1$. From (3.16), the joint probability of all routes satisfies

$$P(\mathbf{N}) = \frac{1}{Z_{\mathbf{N}}} \prod_{(V_i \sim V_j)} \gamma_{ij}^{\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}} (1-\gamma_{ij})^{(1-\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv})} I_1(\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}), \qquad (3.17)$$

where $I_1(\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}) = 1$ if $\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv} = 0$ or 1; and $I_1(\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}) = 0$, otherwise. The clique functions are non-zero if and only if $I_1(\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}) = 1$. Thus (3.17) characterizes the dependencies of routes that result from the capacity constraints. Meanwhile, the network load, e.g. the probability that wavelength λ is used in the network, is characterized by parameters γ_{ij}'s. γ_{ij} can be considered as a "weight" for using a

wavelength at link ij; $1-\gamma_{ij}$ can be considered as a "weight" for not using a wavelength at link ij. When $\gamma_{ij} \equiv \gamma, \forall V_i \sim V_j$, we can relate γ to the network load as follows:

Proposition 3.1: *Let* ρ *denote the network load,* $\rho = \boldsymbol{E}_{P(\mathbf{N})}[\frac{\sum_{V_i \sim V_j} \sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}}{|\mathbf{E}|}]$. *If in (3.17)* , $\gamma_{ij} \equiv \gamma, \forall V_i \sim V_j$, *then* ρ *monotonically increases in* γ.

Detailed proof of Proposition 3.1 can be found in *Appendix E*. Furthermore, (a) if $\gamma = 0.5,$ the undirected probabilistic graph represents a uniform probability distribution on all possible ways of using wavelength λ without violating the capacity constraint; (b) If $\gamma \to 1,$ ρ increases toward the maximum value, which is determined by both the network topology and the route set $\mathbf{R}$; and (c) If $\gamma \to 0,$ ρ approaches 0.

For simplicity of analysis, we assume that $\gamma_{ij} \equiv \gamma$, $\forall V_i \sim V_j$, in the rest of Chapter 3. From (3.17), it follows that

$$P(\mathbf{N} \mid R_f = f_{sd}) \propto n_{sd} P(\mathbf{N} \setminus N_{sd}, N_{sd} = 1). \tag{3.18}$$

3.5 Cross-Layer Representation

The cross-layer model of attack propagation can be obtained by combining the physical- and the network-layer model using a factor graph [43], which corresponds to the following joint probability,

$$P(\mathbf{X}_{f_{sd}}, \mathbf{S}_{f_{sd}}, \mathbf{N} \mid R_f = f_{sd}) = P(\mathbf{S}_{f_{sd}}, \mathbf{X}_{f_{sd}} \mid \mathbf{N}, R_f = f_{sd}) P(\mathbf{N} \mid R_f = f_{sd}), \tag{3.19}$$

where $\mathbf{X}_{f_{sd}} = (X_i : V_i \in \mathbf{V}_{f_{sd}})$ and $\mathbf{S}_{f_{sd}} = (S_i : V_i \in \mathbf{V}_{f_{sd}})$.

Factor graph is a bipartite graph showing how a global function can be factorized into a product of local functions. Each local function depends on a subset of the variables [43]. There are two types of nodes in a factor graph: a variable node for each variable, and a factor node for each local function. There is an edge connecting a variable node to a factor node if and only if the variable is an argument of the local function.

Figure 3.7 shows the factor graph representation for the mesh network in Figure 3.3 when the attack is started from flow *BD*. The lower portion of the factor graph represents attack propagation at the physical layer. As the attack may propagate from node V_i to V_{i+1}, $V_i, V_{i+1} \in \mathbf{V}_{f_{sd}}$, X_i and X_{i+1} are connected to the same factor node $P(X_{i+1} \mid X_i, R_f = f_{BD})$. Furthermore, the number of affected channels at node V_i is determined by X_i and routes that traverses node V_i. Therefore, S_i, X_i, and those routes passing through node V_i are connected to the factor node that corresponds to the conditional probability in (3.13).

The upper portion of the factor graph characterizes the dependence at the network layer. All the network routes that share a common network link ij are connected to the clique function ψ_{ij} in (3.17). Here, the factor graph provides an explicit representation of the dependencies among different network components during attack propagation.

Factor graphs subsume directed and undirected probabilistic graphical models, and provide more explicit representations of the factorization of probability distributions [43]. The application of factor graph provides two advantages: (1) It shows the intricate dependencies among different network components during a crosstalk attack; (2) it

provides computationally efficient algorithms to evaluate the network resilience loss, which shall be discussed in Section 3.7.

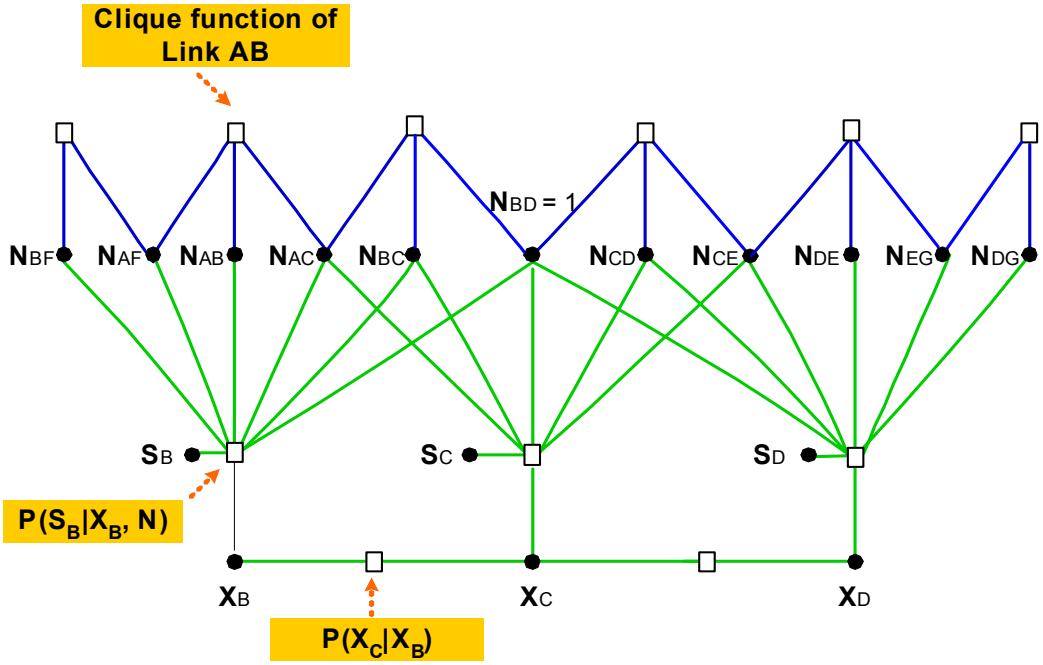

Figure 3.7 Factor graph representation of mesh network in Figure 3.3; attack started on flow *BD*.

3.6 Network Resilience: Impact of Physical Layer

We now use the cross-layer model to study the network resilience. We begin with the physical layer and quantify how the resilience varies with physical topology as well as the physical layer vulnerabilities, characterized by α_i in (3.12).

3.6.1 Impacts of Physical-Layer Vulnerabilities on Network Resilience Loss

We consider the impact of physical-layer vulnerabilities by considering the lower and upper bounds of network resilience loss $M_{f_{sd}}$. The lower bound of $M_{f_{sd}}$ results from the best-case scenario of resilience upon attack: there is no active connections on wavelength

λ that traverses link ij, $\forall V_i \in \mathbf{V}_{f_{sd}}$, $V_j \notin \mathbf{V}_{f_{sd}}, V_i \sim V_j$. In this case, at the switching plane of each node along the attacker's route, only two channels are active that correspond to the connection on the attacker's route. The upper bound result from the worst-case scenario of network resilience upon attack: there always exists an active connection inserted into the network at node V_i and traverses link ij, $\forall V_i \in \mathbf{V}_{f_{sd}}$, $V_j \notin \mathbf{V}_{f_{sd}}, V_i \sim V_j$. In this case, the number of active channels in the switching plane of node V_i is $2(d_i - 1)$ or $2d_i$, $\forall V_i \in \mathbf{V}_{f_{sd}}$, where d_i is the nodal degree of V_i.

For simplicity, in the rest of Chapter 3, we assume $\alpha_i \equiv \alpha, \forall V_i \in \mathbf{V}_{f_{sd}}$. Then, the network resilience loss can be bounded as in the following proposition.

Proposition 3.2: *The network resilience loss for a given source of attack f_{sd} can be bounded as*

$$k + \sum_{i=1}^{k} \alpha^{i-1} \le M_{f_{sd}} \le k + 2(1 + \alpha^{k-1}) + \sum_{i=1}^{k} (2d_i - 3)\alpha^{i-1}, \tag{3.20}$$

where k is the total number of nodes in $\mathbf{V}_{f_{sd}}$, $k > 1$.

The lower bound in (3.20) characterizes the effect of route-length and α on attack propagation, which increases polynomially with respect to α. Let $\varepsilon = 1 - \alpha$, then

$$k + \sum_{i=1}^{k} \alpha^{i-1} = \begin{cases} k + 1 + \alpha + o(\alpha), & as\ \alpha \to 0, \\ 2k - 0.5k(k-1)\varepsilon + o(\varepsilon), & as\ \alpha \to 1, \end{cases} \tag{3.21}$$

which shows that $M_{f_{sd}}$ is determined by the length of route r_{sd}. Furthermore, the upper bound in (3.20) increases polynomially with α, where,

$$k+2(1+\alpha^{k-1})+\sum_{i=1}^{k}(2d_i-3)\alpha^{i-1}=\begin{cases}k+2d_1-1+(2d_2-3)\alpha+o(\alpha), & if\ k>2,\\ k+2d_1-1+(2d_2-1)\alpha+o(\alpha), & if\ k=2,\end{cases}$$

$$\text{as } \alpha\to 0, \tag{3.22}$$

$$\begin{aligned}&k+2(1+\alpha^{k-1})+\sum_{i=1}^{k}(2d_i-3)\alpha^{i-1}\\ &=2\sum_{i=1}^{k}d_i+(4-2k)-\{(k-1)(2-\frac{3}{2}k)+\sum_{i=1}^{k}2d_i(i-1)\}\varepsilon+o(\varepsilon),\end{aligned}$$

$$\text{as}\,\alpha\to 1. \tag{3.23}$$

Equations (3.22) and (3.23) show that, when there is always an active connection inserted into the network at node V_i using link ij, $\forall V_i\in\mathbf{V}_{f_{sd}}, V_j\notin\mathbf{V}_{f_{sd}}, V_i\sim V_j$, if the network vulnerability is low, $M_{f_{sd}}$ is determined by the route length and the nodal degree of the source node of the attack. If the network vulnerability is high, $M_{f_{sd}}$ is determined by the total number of network links incidental on nodes along the attacker's flow, i.e., the number of links in set $\mathbf{E}_{f_{sd}}=\{e_{ij}:V_i\in\mathbf{V}_{f_{sd}}\}$. In addition, $|\mathbf{E}_{f_{sd}}|=\sum_{i=1}^{k}d_i+(1-k)$.

3.6.2 Impact of Physical Topology on Network Resilience Loss

We use the lower- and upper-bound in (3.20) to study the impact of physical topology on $M_{f_{sd}}$. For clarity, we summarize the asymptotic results on $M_{f_{sd}}$ in (3.21) to (3.23) for network resilience under various topologies in Table 3.1. Assume that there is one link-shortest route between each pair of nodes in the network. The asymptotic properties of these topologies are summarized in Table 3.2 ([48][49]). Combining the impacts of physical-layer vulnerability and physical topology, we find that,

(a) If the physical-layer vulnerability is high ($\alpha\to 1$),

(i) The upper bound of $M_{f_{sd}}$ shows that fully-connected mesh network and star network are the least resilient due to the large size of the set $\mathbf{E}_{f_{sd}}$.

(ii) The lower bound of $M_{f_{sd}}$ shows that network with a ring topology is generally the least resilient because of the large route length in a ring network.

(b) If the physical-layer vulnerability is low ($\alpha \to 0$),

(i) The upper bound of $M_{f_{sd}}$ shows that the fully-connected mesh topology is the least resilient since each node in the network has nodal degree $m-1$.

(ii) The lower bound of $M_{f_{sd}}$ shows that the ring network is generally the least resilient due to the large route length.

(c) Chord networks exhibit good resilience whose resilience loss $M_{f_{sd}}$ increases logarithmically with respect to the number of nodes in the network in the worst case.

Note that in addition to the resilience measure considered in this work, there exists other performance metrics for network resilience, e.g. two-terminal connectivity [50], and flexibility in route selection [48]. Therefore, different performance metrics of network resilience need to be considered simultaneously when choosing a resilient network design. Overall, a chord network offers excellent resilience upon crosstalk attacks and good route selection flexibility.

Table 3.1 Bounds of network resilience loss $M_{f_{sd}}$

bounds α	Upper bound of $M_{f_{sd}}$	Lower bound of $M_{f_{sd}}$
$\alpha \to 1$	$2\sum_{i=1}^{k} d_i + (4-2k) - O(1-\alpha)$	$2k - O(1-\alpha)$
$\alpha \to 0$	$k + 2d_1 - 1 + O(\alpha)$	$k + 1 + O(\alpha)$

Table 3.2 Asymptotic properties of different network topologies with *m* nodes

Topology	Ave. nodal degree	Ave. route length	Ave. size of $\mathbf{E}_{f_{sd}}$
Star	1	2	m
Ring	2	$m/4$	$m/4$
n-ary Tree	m+1	$O(\log_n m)$	$O(\log_n m)$
Mesh-Torus	4	$O(\sqrt{m})$	$O(\sqrt{m})$
Fully-Connected Mesh	m	1	m
Chord [23]	$\log_2 m$	$O(\log_2 m)$	$O(\log_2 m)$

3.7 Network Resilience: Impact of Network Layer

We now study the impact of network layer on the resilience in terms of network load. In particular, we are interested in quantifying how the network resilience varies jointly with the load, and the physical-layer vulnerability α.

3.7.1 Impact of Network Load on Network Resilience

We first consider the impact of network load ρ on $M_{f_{sd}}$. From (3.1),

$$M_{f_{sd}} = \sum_{V_i \in \mathbf{V}_{f_{sd}}} \mathrm{E}_{f_{sd}}[S_i], \tag{3.24}$$

where $\mathrm{E}_{f_{sd}}[S_i]$ is the mean number of channels affected by the attack at the switching plane of node $V_i, V_i \in \mathbf{V}_{f_{sd}}$. Furthermore,

$$E_{f_{sd}}[S_i] = 1 + \alpha^{i-1}\{1 + \sum_{V_i \sim V_j, V_j \notin \mathbf{V}_{f_{sd}}} \{E_{f_{sd}}[\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}] + E_{f_{sd}}[\sum_{r_{ih} \in \mathbf{R}_{ij}} N_{ih}]\}\}, \qquad \forall V_i \in \mathbf{V}_{f_{sd}}, \tag{3.25}$$

where $E_{f_{sd}}[\sum_{r_{ih} \in \mathbf{R}_{ij}} N_{ih}]$ is the mean number of active channels that are locally inserted into the network at node V_i and leave node V_i through link ij, and $E_{f_{sd}}[\sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}]$ is the mean

number of active flows that enter node V_i through link ji, given that the attack starts from flow f_{sd}.

A basic question arises: does the network resilience loss $M_{f_{sd}}$ always increase with ρ for arbitrary network with arbitrary route? The answer is no. For a detailed counterexample, please refer to [51]. Nevertheless, when practical route sets are considered, $M_{f_{sd}}$ indeed increases with ρ for several typical network topologies. Specially, we have the following theorems.

Theorem 3.1 *For a ring network, assume the route set* **R** *consists of the two-link disjoint routes between each pair of nodes in the network. Let* k *be the number of nodes traversed by the attacker's flow* f_{sd}. *Then,* $M_{f_{sd}}$ *monotonically increases in* ρ. *In particular,* $M_{f_{sd}}$ *satisfies*

$$v_1 + 2(1+\alpha^{k-1})\gamma \le M_{f_{sd}} \le v_1 + 2(1+\alpha^{k-1})\rho, \tag{3.26}$$

where $v_1 = k + 2\sum_{i=1}^{k} \alpha^{i-1}$. *Furthermore, for* $0 < \rho << 1$, $\rho = \gamma + o(\rho)$, *and the upper and the lower bounds meet*

$$M_{f_{sd}} = v_1 + 2(1+\alpha^{k-1})\rho + o(\rho). \tag{3.27}$$

Detailed proof of Theorem 3.1 can be found in *Appendix F*.

Theorem 3.2 *For a star network, assume that the route set* **R** *consists of the routes between each pair of nodes in the network. Let* m, $m > 1$, *be the number of nodes in the network. Let the hub node be denoted as* V_m. *Then,* $M_{f_{sd}}$ *monotonically increases in* ρ. *In particular,* $M_{f_{sd}}$ *satisfies*

$$M_{f_{sd}} \geq \begin{cases} 3+\alpha+(m-2)\alpha\gamma, & \text{if } f_{sd} = f_{A_i A_m}, i = 1,...,m-1, \\ 3+\alpha+(m-2)\gamma, & \text{if } f_{sd} = f_{A_m A_i}, i = 1,...,m-1, \\ 4+\alpha+\alpha^2+(m-3)\alpha\gamma, & \text{otherwise}, \end{cases} \tag{3.28}$$

$$M_{f_{sd}} \leq \begin{cases} 3+\alpha+2(m-2)\alpha\rho, & \text{if } f_{sd} = f_{A_i A_m}, i = 1,...,m-1, \\ 3+\alpha+2(m-2)\rho, & \text{if } f_{sd} = f_{A_m A_i}, i = 1,...,m-1, \\ 4+\alpha+\alpha^2+2(m-3)\alpha\rho, & \text{otherwise}. \end{cases} \tag{3.29}$$

Furthermore, for $0 < \rho << 1$*, the bounds are tight, and*

$$M_{f_{sd}} = \begin{cases} 3+\alpha+2(m-2)\alpha\rho+o(\rho), & \text{if } f_{sd} = f_{A_i A_m}, i = 1,...,m-1, \\ 3+\alpha+2(m-2)\rho+o(\rho), & \text{if } f_{sd} = f_{A_m A_i}, i = 1,...,m-1, \\ 4+\alpha+\alpha^2+2(m-3)\alpha\rho+o(\rho), & \text{otherwise}. \end{cases} \tag{3.30}$$

Proofs of Theorem 3.2 can be found in *Appendix G*. $M_{f_{sd}}$ generally consists of the sum of two terms: the first term, e.g. $(3+\alpha)$ in (3.30), corresponds to the number of affected wavelength channels that are used by flows on the attacker's route; and the second term, e.g. $(2(m-2)\alpha\rho+o(\rho))$ in (3.30), corresponds to the number of affected wavelength channels that are used by flows not on the attacker's route.

We also compare $M_{f_{sd}}$ for ring and star networks. In both cases, $M_{f_{sd}}$ is linearly increasing in ρ for $0 < \rho << 1$. However, for ring network, $M_{f_{sd}}$ is polynomially increasing in α; whereas for star network, $M_{f_{sd}}$ is generally linearly increasing in α. For ring networks, $M_{f_{sd}}$ is linearly increasing in k (the number of nodes in $\mathbf{V}_{f_{sd}}$). In contrast, for star networks, $M_{f_{sd}}$ is linearly increasing in m (the number of nodes in the network).

3.7.2 Impact of Network Load on Average Resilience Loss

We now focus on the impact of network load ρ on the average network resilience loss (M), which is the mean value of network resilience loss over all possible source of attacks.

Consider a ring network with $m, m>1,$ nodes, $V_1, V_2, ..., V_m$, and a route set **R** that includes all the two link-disjoint paths between each pair of nodes in the network. Then, we have the following theorem,

Theorem 3.3 $M_{ring,m} = \frac{1}{m-1}\sum_{i=1}^{m-1} a_i M_{f_{1\,i+1}}$, (3.31)

where $a_i = P(N_{1\,i+1}=1)$ *is the probability that a connection with* i *links between two terminal nodes,* V_1 *and* V_{i+1}*, is active, and* $M_{f_{1\,i+1}}$ *is the network resilience loss when the attack is started from flow* $f_{1\,i+1}$*. Furthermore,*

$$a_i = \theta^i \, f_{m-i+1} / g_m, \tag{3.32}$$

$$\theta = \gamma/(1-\gamma), \tag{3.33}$$

$$f_m = \frac{\sqrt{1+4\theta^2}+1}{2\sqrt{1+4\theta^2}}\left(\frac{1+2\theta+\sqrt{1+4\theta^2}}{2}\right)^{m-1} + \frac{\sqrt{1+4\theta^2}-1}{2\sqrt{1+4\theta^2}}\left(\frac{1+2\lambda-\sqrt{1+4\theta^2}}{2}\right)^{m-1}, \tag{3.34}$$

$$g_m = f_m + \sum_{j=1}^{m-1} j\theta^j f_{m+1-j}, \ m>1. \tag{3.35}$$

Detailed proof of Theorem 3.3 can be found in *Appendix H*. In addition, using Theorem 3.1, we have the following bounds

$$M_{ring,m} \geq \frac{1}{(m-1)}\sum_{i=1}^{m-1}\{a_i(i+1+\sum_{j=0}^{i}\alpha^j + 2(1+\alpha^i)\gamma)\}, \tag{3.36}$$

$$M_{ring,m} \leq \frac{1}{(m-1)}\sum_{i=1}^{m-1}\{a_i(i+1+\sum_{j=0}^{i}\alpha^j + 2(1+\alpha^i)\rho)\}. \tag{3.37}$$

The difference between the upper and the lower bound of $M_{ring,m}$ is $O((\rho-\gamma)/m)$. Furthermore, (3.31) can be simplified as

$$M_{ring,m} = \rho M_{f_{A_1A_2}} \Big/ (m-1) + o(\rho), \text{ as } \rho \to 0. \tag{3.38}$$

$$M_{ring,m} = \sum_{i=1}^{m-1} \frac{1}{2^{m+1}} M_{f_{A_1A_{i+1}}} \Big/ (m-1), \text{ as } \rho \to 1, m \to \infty. \tag{3.39}$$

Then, we have

$$M_{ring,m} = \rho(3+\alpha)/(m-1) + o(\rho), \text{ as } \rho \to 0, \tag{3.40}$$

which shows that

(i) When the network load is low, $M_{ring,m}$ increases almost linearly with ρ and α; and is in the order of $O(\rho/m)$.

(ii) When the network load is high,

$$M_{ring,m} = \frac{1}{m-1}\{\sum_{i=1}^{m-1} \frac{1}{2^i}(i+1+\sum_{j=0}^{i} \alpha^j + 2(1+\alpha^i)\}, \text{ as } \rho \to 1, m \to \infty. \tag{3.41}$$

Furthermore, if $\alpha = 1$, (3.41) can be simplified as

$$M_{ring,m} = \frac{1}{m-1}(6 - \frac{m+5}{2^{m-1}}) \tag{3.42}$$

which shows that $M_{ring,m}$ is in the order of $O(1/m)$.

Next consider a star network with m nodes, $V_1, V_2, ..., V_m$, where V_m is the hub node of the star network; and a route set **R** that includes all the link-disjoint paths between each pair of nodes in the network. It follows that,

Theorem 3.4 $M_{star,m} = \dfrac{b_1(M_{f_{A_1A_k}} + M_{f_{A_kA_1}}) + 2b_2(m-2)M_{f_{A_1A_2}}}{2(m-1)}, m > 3,$ (3.43)

where $b_1 = P(N_{A_1A_k} = 1)$, $b_2 = P(N_{A_1A_2} = 1)$, *and*

$b_1 = \theta t_{m-1}/t_m$; $b_2 = \theta^2 t_{m-2}/t_m$;

$t_1 = 1$;

$t_2 = 1+\theta$;

$t_i = (1+\theta)t_{i-1} + (i-2)\theta^2 t_{i-2}$, $\forall\, i > 2$.

Detailed proof of Theorem 3.4 can be found in *Appendix H*. Furthermore, using Theorem 3.2, we have the following bounds for $M_{star,m}$,

$$M_{star,m} \geq \frac{1}{2(m-1)}\{b_1(4+(1+\alpha)(2+(m-2)\gamma)) + 2b_2(m-2)(4+\alpha+\alpha^2+(m-3)\alpha\gamma)\}, \tag{3.44}$$

$$M_{star,m} \leq \frac{1}{2(m-1)}\{b_1(4+2(1+\alpha)(1+(m-2)\rho)) + 2b_2(m-2)(4+\alpha+\alpha^2+2(m-3)\alpha\rho)\}. \tag{3.45}$$

The difference between the upper and the lower bound of $M_{star,m}$ is $O(\alpha(2\rho-\gamma))$ when m is large, since b_2 is $O(1/m)$. In addition, when the network load is low,

$$M_{star,m} = \rho(3+\alpha)/m + o(\rho), \text{ as } \rho \to 0, \tag{3.46}$$

which shows that $M_{star,m}$ is $O(\rho/m)$; and increases linearly with α. When the network load is high ($\rho \to 1$) , we have

$$M_{star,m} = O(\alpha\rho), \text{ as } \rho \to 1, \tag{3.47}$$

which shows that, when the star network is under high load, $M_{star,m}$ increases linearly with α.

For a general network ***G***(**V**,**E**) with a fixed set of route $\mathbf{R}$, we have the following upper bound for M :

Theorem 3.5 $$M \leq \frac{1}{|\mathbf{R}|}\max_{f_{sd}}\{\mathbf{M}_{f_{sd}}\}\rho\,|\mathbf{E}|, \tag{3.48}$$

where $|\mathbf{E}|$ *is the cardinality of the set of edges in the network;* $|\mathbf{R}|$ *is the cardinality of the route set* ***R****.*

The proof of Theorem 3.5 can be found in *Appendix I*. In (3.48), $\rho|\mathbf{E}|/|\mathbf{R}|$ corresponds to the upper bound of the probability that the crosstalk attack occurs in the network, and is accurate when the network route set $\mathbf{R}$ only consists of routes with link-length 1. The bound in (3.48) provides a worst case estimation of M. Furthermore, suppose that all the routes in the set $\mathbf{R}$ are of the same link length l. Then the probability that an crosstalk attack happens in the network is $(\rho|\mathbf{E}|)/(l|\mathbf{R}|)$, and (3.48) can be refined as

$$M \le \frac{1}{|\mathbf{R}|l}\max_{f_{sd}}\{M_{f_{sd}}\}\rho|\mathbf{E}|. \tag{3.49}$$

When the length of each network route and the network resilience loss $M_{f_{sd}}$ are the same for each possible source of attack, the equality in (3.49) holds. Theorem 5 suggests the upper bound of average network resilience loss is affected by the following factors:

(1) The network load (ρ) in the network. The upper bound in (3.49) increases at least linearly with ρ.

(2) The number of links in the network. The larger the number of links in the network, the less resilient the network is. The upper bound in (3.49) increases linearly with the number of links in the network.

(3) The number of routes in the network. The larger the number of routes in the network, the more resilient the network is. This is because that the probability for a route to be chosen as the attacker's route is smaller.

Next we use (3.48) to study a mesh-torus network with m nodes and a route set $\mathbf{R}$, which includes: (1) the unique link-shortest route between each pair of nodes if applicable; and (2) one shortest route between each pair of nodes, which forms the border of the sub-grid with the two nodes at the diagonally opposite corners.

Theorem 3.6

$$\max_{f_{sd}}\{M_{f_{sd}}\} \le \begin{cases} \dfrac{6(1-\alpha^{\sqrt{m}+1})}{(1-\alpha)}+4, & \text{if } \alpha \ne 1, \\ 6\sqrt{m}+4, & \text{otherwise.} \end{cases} \tag{3.50}$$

Then, from (3.48), we have $M_{\mathbf{torus,m}} \le \dfrac{2m\rho}{m(m-1)} \max_{f_{sd}}\{M_{f_{sd}}\}$,

$$M_{\text{torus,m}} \le \begin{cases} \dfrac{2\rho}{(m-1)}\left(\dfrac{6(1-\alpha^{\sqrt{m}+1})}{(1-\alpha)}+4\right), & \text{if } \alpha \ne 1, \\ \dfrac{2\rho}{(m-1)}(6\sqrt{m}+4), & \text{otherwise.} \end{cases} \tag{3.51}$$

Furthermore, when $\rho \to 0$, *it can be found that*

$$M_{\text{torus,m}} = \rho(3+\alpha)/(m-1)+o(\rho), \quad \text{as } \rho \to 0. \tag{3.52}$$

Detailed proof of Theorem 3.6 is omitted here.

We compare the average network resilience loss for ring, star and mesh networks in Table 3.3. It can be observed that:

(1) When the network load is low ($0 < \rho << 1$), M is $O(\rho/m)$. This is because when the load is close to 0, the network is most likely in either of two states: (a) there is no active connection in the network; or (b) there is an active connection of link length 1. Specifically, with probability $O(\rho)$, the attack is started on a route of link length 1; with

probability $o(\rho)$, the attack is started on a route of longer lengths. For instance, as each route is the attacker's route with equal probability, the attack starts on routes of link length 1 in the mesh-torus network with probability $2\rho/(m-1)$ and $M_{f_{sd}} = (3+\alpha) + o(\rho)$ if $\rho << 1$.

(2) When the network load is high ($\rho \to 1$), the star network is the least resilient, with M being $O(\alpha)$. This is because, for the star network, nodes in the set $\mathbf{V}_{f_{sd}}, \forall r_{sd} \in \mathbf{R}$, has the most number of neighboring links. Ring and mesh-torus networks show good network resilience in $O(\rho/m)$.

Table 3.3 Average network resilience loss (*M*)

M	$\rho \to 0$	$\rho \to 1$
Ring network	$\rho(3+\alpha)/(m-1)$	$O(1/m)$
Star network	$\rho(3+\alpha)/m$	$O(\alpha)$
Mesh-torus	$2\rho(3+\alpha)/(m-1)$	$\begin{cases} O(1/(1-\alpha)m), & \text{if } \alpha \neq 1, \\ O(1/\sqrt{m}), & \text{otherwise.} \end{cases}$

3.7.3 Irregular Topologies

For networks with irregular topologies, we resort to the sum-product algorithm on the factor graph. The sum-product algorithm is then compared with the exact resilience calculation through enumerations of all network traffic patterns. Enumeration has the computational complexity exponential in the number of routes, and is thus not applicable to networks with even a medium number of routes. The computational complexity of the sum-product algorithm is exponential in the maximum nodal degree of the factor graph for the worst case [43], and is thus much more efficient than enumeration. The sum-

product algorithm provides exact results when the factor graph has no loops, and provides approximate results when the factor graph contains loops [43].

When there are a large number routes in the set **R**, to further reduce the computational complexity of the sum-product algorithm, the following intermediate variables can be introduced: (1) $W_{ij} = \sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}, W_{ij} \in \{0,1\}$, which is the number of flows that enter the switching plane of node V_i through link ij; (2) $H_{ij} = \sum_{r_{ih} \in \mathbf{R}_{ij}} N_{ih}, H_{ij} \in \{0,1\}$, which is the number of flows locally originated at node i and leaves node V_i through link ij. Then the factor graph representation can be transformed accordingly. On the other hand, it is also possible to transform a factor graph with loops into a loop-free factor graph, so that exact results can be obtained using the sum-product algorithm at the cost of computational complexity [43].

We first consider three networks shown in Figure 3.8. In each network, the route set has 21 routes, which corresponds to one link-shortest route between each pair of nodes. Using the sum-product algorithm, we first compute the network resilience loss given the source of attack $M_{f_{sd}}$ for each f_{sd}. We then use the sum-product algorithm to find the probability of $P(N_{sd} = 1)$. Finally, (3.2) is used to compute the average network resilience loss.

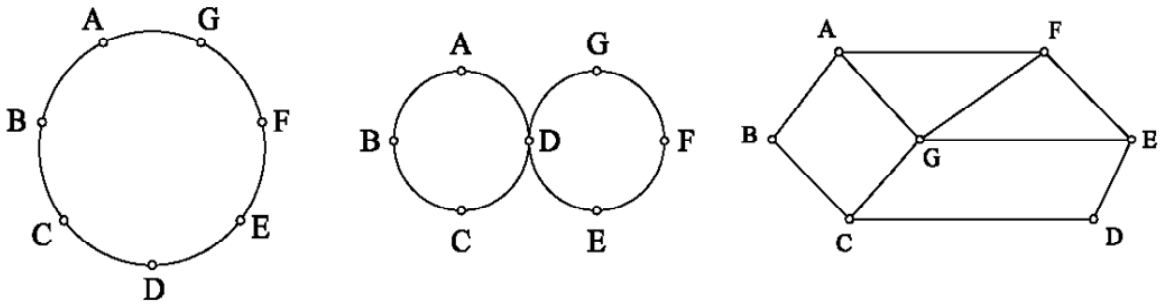

Figure 3.8 Ring, double-ring, and mesh networks

Figure 3.9 depicts the relationship between ρ and average network resilience loss M for the networks in Figure 3.8 with $\alpha = 0.6$. It can be observed that:

(a) M monotonically increases with ρ, in networks with all-to-all traffic and link-shortest path routing. Moreover, for low load, M increases linearly with ρ.

(b) The sum-product algorithm results in an almost exact M for the mesh and ring networks, even though the factor graph representations contain loops. The performance of sum-product algorithm is not as accurate yet acceptable for the double-ring network. This suggests that the sum-product algorithm can be used for large networks where exact calculation of resilience is infeasible.

Next, we use the sum-product algorithm to study the network resilience for the National Science Foundation (NSF) network topology [52]. The NSF network topology has 14 network nodes and 21 bi-directional links. Assume that there is one link-shortest route between each pair of nodes in the networks. Then, there are 91 routes in $\mathbf{R}$. The corresponding factor graph representation contains loops, and thus sum-product algorithm provides an approximation for M.

Figure 3.10 shows the relationship between ρ and M for the NSF network topology with $\alpha = 0.3, 0.6, 0.9$. It suggests that, if the set of network routes consists of one link-shortest route between each pair of nodes in the network, M generally increases with the network load. Furthermore, when the network load is low, M increases linearly with ρ.

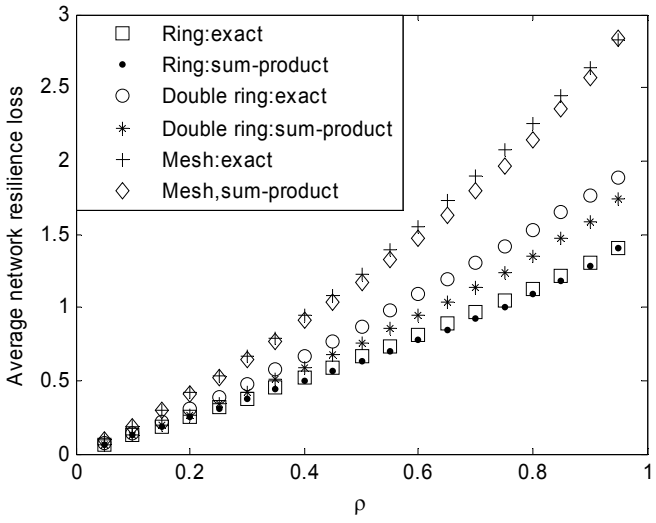

Figure 3.9 Average network resilience loss vs. network load; $\alpha = 0.6$, three networks in Figure 3.8

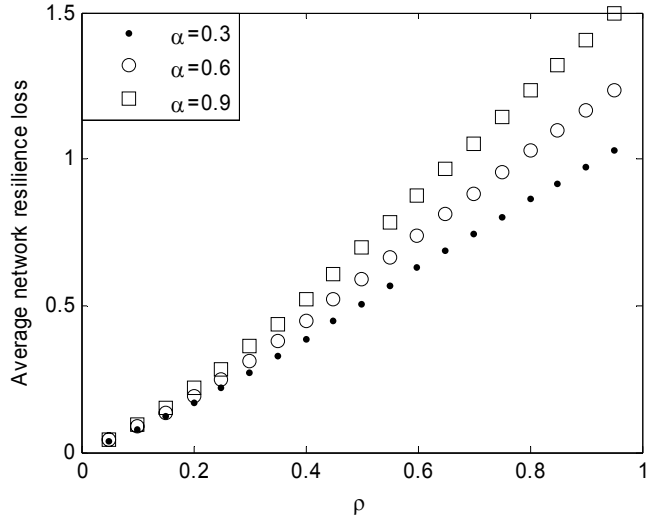

Figure 3.10 Average network resilience loss vs. network load; $\alpha = 0.3, 0.6, 0.9$; NSF network topology

3.8 Related Work in Probabilistic Graphical Models

Bayesian Belief Network has been used in fault localization and detection (see [53] and references therein) in complex communication systems. There the construction of the Bayesian Belief Network representation is usually assumed based on the causal relationships and the main difficulty then lies in estimation of model parameters, i.e., conditional probabilities. In [54], dependency graph is used for IP fault localization, where the problem of shared-risk-link-group is formulated using a bipartite graph.

Markov Random Field (MRF) has been used to study the blocking probability in a loss network [47] as discussed in Section 3.4. This work generalizes the work in [47] by using undirected probabilistic graphs to capture the basic dependency among different routes due to the capacity constraint, and the network load. In [55], self-localization in sensor networks is formulated using MRF with single-node and pair-wise clique potentials, and Belief Propagation algorithm is used for self-calibration. In [56], a distributed architecture for inference in sensor networks is proposed using graphical models, where network nodes form a spanning tree.

Factor graphs have been applied to the problem of multicast link loss inference in sensor networks [57]. The factor graph is constructed based on the concept of link and route costs with two fundamental assumptions: link costs are assumed to mutually independent and path flows are assumed to be mutually independent. In this work, we maintain the dependence among different flows, and obtain the factor graph through decomposition of the joint probability distribution of network nodes, links and connections. In [58], factor graph has been used for scalable source/channel decoding in

large-scale sensor networks. In this case, factor graph provides a simplified model of the correlation among sensor data and enables scalable iterative decoding.

In [59], a similar bottom-up approach is used to derive a cross-layer model for self-configuration of ad hoc wireless networks based on probabilistic graphical models. The resulting model is shown to be a Markov Random Field for the physical- and the link layer [59].

3.9 Summary of Chapter 3

In this Chapter, we have studied resilience of all-optical networks (AONs) under in-band crosstalk attacks. Our goal is to develop a cross-layer model that characterizes attack propagation in the network, and to study the resilience of AON architectures from both the physical- and the network layer. We have found that probabilistic graphical models can serve this goal. In particular, at the physical layer, a directed probabilistic graph can model attack propagation when network under static traffic. At the network layer, an undirected probabilistic graph can represent the probability distribution of active connections. A cross-layer model is then obtained by combining the physical- and network-layer models into a factor graph representation.

There are several benefits resulting from the cross-layer model based on graphical models. The model provides an explicit representation of the dependencies and interactions between the physical- and the network layer. In addition, it facilitates the analytical investigation of network resilience for ring, star, and special cases of mesh topologies. Finally, the cross-layer model facilitates the implementation of computationally efficient approaches, e.g. the sum-product algorithm, for evaluating network resilience.

Through both analysis and numerical study, we have explored several factors from both the physical- and the network layer that affect the resilience. Factors from the physical-layer include: (1) the physical-layer vulnerability, parameters in Bayesian Belief Network that characterize how likely the attack propagates, and (2) the physical topology. Factors from the network layer include active network connections that are characterized using network load, i.e., the probability that the wavelength, on which the attack is initiated, is used in the network. We show that for all the topologies studied in Chapter 3, the average network resilience loss increases linearly with respect to the physical-layer vulnerability and light network load under link-shortest routing, and all-to-all traffic. In addition, ring and mesh-torus network show good resilience, which are inversely proportional to the number of the nodes in the network. Numerical results also suggest that for networks with link-shortest routing and all-to-all traffic, the network resilience loss increases at least linearly with respect to the network load.

CHAPTER 4

TRAFFIC-BASED NETWORK RELIABILITY

4.1 Introduction of Chapter 4

Network reliability is one of the fundamental problems in networking. In the past decade, as network complexity and scale increase dramatically, network failures have become a norm rather than an exception [3], which may result from hardware/software faults, operator errors, malicious attacks, and natural disasters [68]. Meanwhile, new applications, e.g. on-line financial transactions, require a high-level of network reliability that has not been observed before. Therefore it is imperative to quantify network reliability and service disruption upon failures.

Reliability has been defined through deterministic and probabilistic reliability metrics [50]. Two basic deterministic reliability metrics are the cohesion and connectivity of the underlying graph of the network [50][61], which denote the minimum cardinality of the an edge cut-set and an edge cut-set respectively. Probabilistic metrics assume that each component may fail with a certain probability and can be categorized as "non-traffic-based" and "traffic-based" [63]. The "non-traffic-based" approaches focus the physical network topology, and evaluate the connectivity of the network from the probabilistic information on node and link failures. 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 [60]. Non-traffic-based measures put no constraints at the network layer, i.e., on link capacity, traffic distribution, and operation schemes upon failures. Furthermore, they are not meaningful for well-connected physical topologies, where the network connectivity remains high even after failures occur. Hence non-traffic

based reliability can access the reliability in terms of physical connectivity but not service disruption.

On the other hand, "traffic-based" metrics take into consideration the amount of traffic carried by the network that is related to service disruption. In particular, traffic-based measures focus on network performance upon failures by considering multiple factors such as the physical layer failures, the impact of the failures on the network layer, and the network operation schemes (i.e., whether protection is provided by the network). In this work, we focus on traffic-based reliability metrics, which include the amount and percentage of lost traffic and thus reflect services affected by failures [63].

There are several challenges in the study of traffic-based network reliability. First, Traffic-based reliability metrics combine both the physical layer failure and the network layer traffic. Thus, network-layer traffic models need to be considered in studying traffic-based reliability. Second, there exist dependencies among network layer traffic as well as among physical layer failures. Finally, the reliability varies with respect to different network operation schemes, e.g. no protection and 1+1 protection [82]. All these factors show that traffic-based reliability is network-centric and should be studied across network and physical layers.

Therefore, in this chapter, we systematically investigate different factors that affect traffic-based network reliability. Specifically, we focus on the effects of the following factors:

- Physical topologies
- Dependent failure at the physical layer
- Network operation schemes upon failures, i.e., with or without failure protection,

- Network layer traffic models.

In our investigation, we first assume a uniform deterministic traffic model at the network layer. This allows us to focus on the impacts of the first three factors on network reliability. We then adopt a random network layer traffic model with Poisson arrivals to further investigate the effect of network layer traffic. To obtain analytical results on network reliability, we apply the approach of Erlang Fixed Point Approximation (EFPA) [81]. To represent the dependencies among network traffic and physical layer failures, we make use of probabilistic graphical models [40]. We provide the advantages and drawbacks of using such a commonly-used traffic, and demonstrate the need of considering other traffic models to study service disruption upon failures.

The rest of Chapter 4 is organized as follows. Section 4.2 discusses related work on traffic-based network reliability. Section 4.3 describes the problem formulation. Section 4.4 investigates the impact of different factors that affect traffic-based network reliability under the uniform deterministic traffic model. Section 4.5 discusses the network reliability under random traffic model with Poisson arrivals. Section 4.6 summarizes the chapter.

4.2 Related Work

There has been extensive research in connectivity-based network reliability metrics. The problems of computing connectivity-based metrics are generally NP-hard. Therefore, different algorithms for evaluating *k-terminal* reliability have been proposed, e.g. [60]. In [77], four algorithms for computing terminal-pair reliability proposed by different authors are compared. In addition, a new algorithm is proposed in [77] based on network adjacency matrix and breadth-first search.

In [63], traffic-based network reliability metrics are defined as the percentage of network traffic lost due to failures, which is then used to study the reliabilities of ring networks without protection and pre-planed protection. However, the reliability analysis in [63] is restricted to independent failures, ring networks, and deterministic network layer traffic. A systematic investigation of different factors that affect traffic-based network reliability is missing.

Another closely related research filed is the design of highly reliable networks. In [50], the metric of *k-terminal* reliability is used to investigate high-reliability topological architectures for networks under stress, where the network component is assumed to have a large probability of failure. The work in [50] considers the effects of physical topologies and dependent failures on network reliability. However, as the reliability metrics used in [50] are connectivity-based, it ignores the impact of network layer traffic and the network operation schemes upon failures (whether the network has failure protection). In [50], the model of dependent failures is based on Markov Chain, which is simple and tractable for the derivation of analytical results, but is inconsistent due to the cyclic nature of physical topology.

In [73], logical topology design of optical network is considered, where the objective is to guarantee that a single failure of one fiber link in the physical layer will not disconnect the logical network. In this case, the reliability metric can be considered as "all-terminal connectivity" in the logical topology upon single link-failure in the physical topology. In [73], it is found that the problem of survivable routing is NP-complete. In [74], a technique for fault-tolerant logical topology design in WDM networks with uni-cast and multicast IP flows is proposed, which uses the dynamic capabilities of IP routing

and obtains a different optimal logical topology design for each failure state of the physical network. In [72], multi-commodity flow (MF) models for topology design of packet-switched networks are considered. MF models have also been used as approximations in the design of circuit-switched networks with reliability constraints. In [72], it is shown that MF models are different from the actual flows in the network obtained from a real-time adaptive call routing algorithm, and MF models can take into account network reliability constraint by incorporating each network failure state in the optimal design problem.

In [68], a general framework is proposed to quantify the 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 using a Markov process. However, due to its complexity, the framework is not tractable for reliability analysis at the network level with dependent network failures. In [68][69], two frameworks to evaluate network survivability upon failures are proposed, where the focuses are to definitions of network survivability metrics for different types of network failures, e.g., catastrophic/disastrous failure, major network failure, and minor network failure.

Thus, one important open issue in traffic-based network reliability is the systematic investigation of different factors that affect the reliability, which include: network topology, failure dependencies, network operation schemes upon failures, and network traffic models. For comparison, we list the focuses of prior studies and this work in Table 4.1.

Table 4.1 Comparison of prior study and this work

	Reliability metrics	Network topology	Dependent failure	Network operation schemes	Network traffic model
[63]	Traffic-based reliability	Ring-based topologies	Not considered	Without protection; With 1+1 protection	Deterministic traffic model
[50]	Connectivity-based reliability	Different network topologies	Dependent failure model based on Markov chains	Not considered	Uniform deterministic traffic model
[68]	Definition of Traffic-based reliability	A single communication link	Not considered	Not considered	Random traffic model
[69][70]	Definitions of Traffic-based reliability	N/A	N/A	N/A	N/A
This work	Traffic-based reliability	Different network topologies	Dependent failure model based on Bayesian Belief Networks	Without protection; with 1+1 protection	Uniform deterministic traffic model; Uniform random traffic model

4.3 Problem Formulation

We now formulate network reliability by incorporating the physical-layer topology, protection schemes, and network layer traffic. Let $\mathbf{G}(\mathbf{V},\mathbf{E})$ be a physical-layer topology, where $\mathbf{V}$ is the set of nodes and $\mathbf{E}$ is the set of bi-directional links. Assume fixed routing. Let $\mathbf{R}$ be a set of routes used by the network for setting up connections. The route set may $\mathbf{R}$ be determined by such factors as traffic demand 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 1+1 protection, we assume that $\mathbf{R}$ consists of one primary route and one link-disjoint route 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 number of active connections between node i and j.

Assume that links in **E** may fail with a certain probability. We can then denote the status of link i as a binary random variable Z_i: $Z_i = 1$ if there is a failure at link i; and $Z_i = 0$ otherwise. Furthermore, we denote the status of connections between node m and n as a binary random variable S_{mn}. Specifically, S_{mn} =1 if the connections are lost due to network failure events; and S_{mn} =0, otherwise.

For instance, for networks without connection protection upon failures, S_{mn}=1 if there is one or more link failures on route R_{mn}; and S_{mn}=0 otherwise. Specifically, we have

$$P(S_{mn} = 0) = P(\sum_{e_i \in \mathbf{E}_{R_{mn}}} Z_i = 0), \tag{4.1}$$

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 between node m and n; and S_{mn}=0, otherwise. Specifically, we have

$$P(S_{mn} = 0) = P(\sum_{e_i \in \mathbf{E}_{R_{mn,p}}} Z_i = 0 \cup \sum_{e_i \in \mathbf{E}_{R_{mn,b}}} Z_i = 0), \tag{4.2}$$

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. Then, the reliability of the network is measured using the two metrics $\mathbb{Z}$ and $\mathbb{k}$ following the same idea as in [63], which is defined as follows.

Definition 4.1: *Network reliability measure $\mathbb{Z}$ is the expected amount of lost traffic due to network failures, where*

$$\mathbb{Z} = \sum_{ij} E[D_{ij}\phi_{ij}S_{ij}], \tag{4.3}$$

Where ϕ_{ij} is the bandwidth rate of each connection between node i and node j. In this work, we assume that $\phi_{ij} = 1$, which means that each connection carries one unit of bandwidth. However, our investigation of traffic-based reliability can be extended to the case of heterogeneous bandwidth rate in a straightforward way.

Definition 4.2: *Network reliability measure* $\mathbb{k}$ *is the percentage of lost traffic due to physical link failures, where*

$$\mathbb{k} = \frac{\sum_{ij} E[D_{ij} S_{ij}]}{\sum_{ij} E[D_{ij}]}. \tag{4.4}$$

In this work, we focus on open-loop analysis of network reliability. This implies that traffic allocation upon failures is not considered. Our goal is to gain insights from this relatively simple scenario on impacts of multiple factors on network resilience. Under such an assumption and let $\phi_{ij} = 1$, we have

$$\mathbb{Z} = \sum_{ij} E[D_{ij}] E[S_{ij}], \tag{4.5}$$

where $E[D_{ij}]$ is the expected number of active connection between node i and j, and $E[S_{ij}]$ can be regarded as the service availability for routes between node i and j. The product of expected values in (4.5) shows that, the interaction between network layer traffic and physical layer failures is considered in an average sense.

4.4 Reliability under Uniform Deterministic Traffic

We begin with a simple network layer model, i.e., uniform deterministic traffic, in order to study the effects of physical topologies, network management schemes (with and without protection), and dependencies among physical layer failures, which is lacking in

prior work as discussed in Section 4.2. Uniform deterministic traffic assumes that there is one active connection between each pair of nodes in the network, i.e., $D_{ij} = 1, \forall\, i, j \in \mathbf{V}$. Thus, the network resilience is determined by physical layer and network management schemes, and the reliability measures reduce to

$$\mathbb{Z} = \sum_{i,j \in \mathbf{V}, i \neq j} E[S_{ij}], \tag{4.6}$$

and

$$\mathbb{k} = \frac{2 \sum_{i,j \in \mathbf{V}, i \neq j} E[S_{ij}]}{k(k-1)}, \tag{4.7}$$

where k is the number of nodes in the network, and there are in total $k(k-1)/2$ connections under the uniform deterministic traffic model. Since $\mathbb{k} = \frac{2}{k(k-1)}\mathbb{Z}$, we only need to focus on metric $\mathbb{k}$. We assume that route $r_{ij}, r_{ij} \in \mathbf{R}$, is the link-shortest route between node i and j in the rest of Section 4.4.

4.4.1 Independent Failure and without Protection

In this subsection, we assume that each link in $\mathbf{E}$ fails independently of each other with probability p. Furthermore, each connection in the network has no failure protection, i.e., the traffic between i and j is lost if there is one or more link failures on route r_{ij}. We first consider arbitrary physical topology $\mathbf{G}(\mathbf{V}, \mathbf{E})$. Then focus on typical regular topologies including ring, star, and mesh-torus networks.

4.4.1.1 Arbitrary Physical Topology

For an arbitrary topology, we have the following theorem on reliability measure $\mathbb{k}$:

Theorem 4.1: $\mathbb{k} = \frac{2}{k(k-1)} \sum_{l=l_{\min}}^{l_{\max}} h_l (1-(1-p)^l) \le 1-(1-p)^{\bar{h}}$, (4.8)

where h_l *is the number of routes in* $\mathbf{R}$ *with* l *links, and* $\bar{h}$ *is the average length of routes in* $\mathbf{R}$, *and* $\bar{h} = \frac{2}{k(k-1)} \sum_{l=l_{\min}}^{l_{\max}} l h_l$.

The proof of Theorem 4.1 is based on Jensen Inequality and the details are omitted here. In particular, from Theorem 4.1,

(1) When the probability of link failure (p) is small, we have

$$\mathbb{k} = \bar{h}p + o(p), \qquad \text{as } p \to 0, \tag{4.9}$$

which means that, when the network has a small probability of failure, the network reliability is determined by the average length of the routes in **R**.

(2) When the probability of link failure (p) is large, we have

$$\mathbb{k} = 1 - \frac{2h_{l_{\min}}}{k(k-1)} \varepsilon^{l_{\min}} + o(\varepsilon^{l_{\min}}), \qquad \text{as } p \to 1, \tag{4.10}$$

where $\varepsilon = 1-p$. This shows that, when the network has a high probability of failure, e.g. the network is working under high stress [50], the network reliability is determined by the length of the shortest routes in **R.**

Furthermore, from Theorem 4.1, we have the following corollary

Corollary 4.1: *Of all the network topologies with* k *nodes, the fully-connected graph is the most reliable. In addition, of all the network topologies with the same number nodes and the same number of links, the Moore graph is the most reliable if p<<1.*

A Moore graph, if exists, has the minimum average shortest route between each pair of nodes, which is given by the Moore bound in [78]. The result in Corollary 4.1

complements the findings in [50], where it has been shown that the Moore graph has the best *all-terminal* reliability, when the link failure probability is low with independent failure assumptions.

4.4.1.2 Typical Regular Topologies

In this subsection, we consider three typical network topologies, ring, star, and mesh-torus networks with k nodes. Using Theorem 4.1, we have the following corollaries.

Corollary 4.2: *For a ring network with* k *nodes,* $k \geq 3$,

$$\mathbb{k}_{ring} = \begin{cases} 1 - \frac{2}{k-1}\{(\frac{1-p}{p})(1-(1-p)^{\frac{k-1}{2}})\}, & k \text{ odd}, \\ 1 - \frac{2}{k-1}\{(\frac{1-p}{p})(1-(1-\frac{p}{2})(1-p)^{\frac{k}{2}-1}), & k \text{ even}. \end{cases} \tag{4.11}$$

From Corollary 4.2, it can be found that

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

$$\mathbb{k}_{ring} = \begin{cases} \frac{k+1}{4}p + o(p), & k \text{ odd}, \\ \frac{k^2}{4(k-1)}p + o(p), & k \text{ even}, \end{cases} \quad \text{as } p \to 0, kp << 1. \tag{4.12}$$

(2) When the probability of link failure (p) is large,

$$\mathbb{k}_{ring} = 1 - \frac{2}{k-1}\varepsilon + o(\varepsilon), \quad \text{as } p \to 1, p = 1 - \varepsilon. \tag{4.13}$$

Corollary 4.3: For star network with k nodes, $k > 2$,

$$\mathbb{k}_{star} = p + \frac{k-2}{k}(p - p^2). \tag{4.14}$$

Furthermore, from Corollary 4.3, it can be shown that

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

$$\mathbb{k}_{star} = p + \frac{k-2}{k} p, \quad \text{as } p \to 0. \tag{4.15}$$

(2) When the probability of link failure (p) is large,

$$\mathbb{k}_{star} = 1 - \frac{2}{k}\varepsilon + o(\varepsilon), \quad \text{as } p \to 1, \varepsilon = 1 - p. \tag{4.16}$$

Corollary 4.4: *For a mesh-torus network with k nodes, $\sqrt{k}$ odd and $\sqrt{k} > 3$*

$$\mathbb{k}_{torus} = 1 - \frac{1}{(m_1^2 + m_1)p^2}\{1 - p + (1-p)^{2m_1+2} - (2-p)(1-p)^{m_1+1}\}, \tag{4.17}$$

where $m_1 = \frac{\sqrt{k}-1}{2}$.

Furthermore, from Corollary 4.4, it can be found that

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

$$\mathbb{k}_{torus} = \frac{\sqrt{k}-1}{2} p + o(P), \quad \text{as } p \to 0, \sqrt{k}\,p << 1. \tag{4.18}$$

(2) When the probability of link failure (p) is large,

$$\mathbb{k}_{torus} = 1 - \frac{4\varepsilon}{(k-1)} + o(\varepsilon), \quad \textbf{as } p \to 1, p = 1 - \varepsilon. \tag{4.19}$$

The network reliabilities of the three typical topologies are summarized in Table 4.2. It can be found that, with independent link failure and without traffic protection,

(1) When the probability of link failure (p) is small: with the same number of nodes, the star network is the most reliable ($2p$), whereas the ring network is the least reliable ($O(kp)$). Intuitively, that is because of the average shortest routes in the star network.

(2) When the probability of link failure (p) is large: with the same number of nodes, the three networks have similar network reliabilities. That is because the three networks have similar number of shortest routes with link length 1.

Table 4.2 Network reliabilities of ring, star, and mesh-torus networks; independent failure and without fault protection

	$p \to 0$	$p \to 1$
Ring	$O(k)p$	$1-(1-p)\frac{2}{k-1}$
Star	$p+\frac{k-2}{k}p$	$1-(1-p)\frac{2}{k}$
Mesh-Torus	$O(\sqrt{k})p$	$1-(1-p)\frac{4}{k-1}$

4.4.2 Independent Failure and with 1+1 Protection

We now consider network reliability with independent link failure and 1+1 fault protection. With 1+1 protection, the active connection on route r_{ij} is rerouted to a predetermined link-disjoint backup route between node i and j, if there is one or more link failures on route r_{ij}. The traffic is lost if there is one or more link failures at both route r_{ij} and its backup route.

4.4.2.1 Arbitrary Physical Topology

For arbitrary physical topology, with independent failures and 1+1 protection, we have the following theorem.

Theorem 4.2: $$\mathbb{k} = 1-\frac{2}{k(k-1)}\{\sum_{i\neq j,\ i,j\in \mathbf{V}} (1-p)^{l_{ij,1}} + (1-p)^{l_{ij,2}} - (1-p)^{l_{ij,1}+l_{ij,2}}\}, \qquad (4.20)$$

where $l_{ij,1}$ *and* $l_{ij,2}$ *are the lengths of route* r_{ij} *and its backup route respectively.*

In particular, from Theorem 4.2,

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

$$\mathbb{k} = \frac{1}{k-1}\sum_{i=1}^{k-1} l_{i,1} l_{i,2} p^2 + o(p^2), \quad \text{as } p \to 0. \tag{4.21}$$

Comparing (4.21) to (4.9), we can find that fault protection increases the network reliability significantly.

(2) When the probability of link failure (p) is large,

$$\mathbb{k} = 1 - \frac{2h_{l_{\min}}}{k(k-1)} \varepsilon^{l_{\min}} + o(\varepsilon^{l_{\min}}), \quad \text{as } \varepsilon = 1-p \text{ and } p \to 1. \tag{4.22}$$

The proof of Theorem 4.2 is based on the following,

$$S_{ij} = 1 - (1-p)^{l_{ij,1}} + (1-p)^{l_{ij,2}} + (1-p)^{l_{ij,1}+l_{ij,2}}, \tag{4.23}$$

which means that, with independent failure and 1+1 protection, the connection between node i and j is lost if there are failures at both route r_{ij} and it backup route. Details proof of Theorem 4.2 are omitted here.

4.4.2.2 Typical Regular Topologies

We now consider the ring and mesh-torus network with independent failures and 1+1 protections. From Theorem 4.2, we have the following corollaries.

Corollary 4.5: *For ring network with* k *nodes,* $k \geq 3$,

$$\mathbb{k}_{ring} = 1 + (1-p)^k - \frac{2}{k-1}\left(\frac{(1-p)-(1-p)^k}{p}\right). \tag{4.24}$$

In particular, from (4.21) and (4.22),

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

$$\mathbb{k}_{ring} = \frac{k(k+1)}{6} p^2 + o(p^2), \quad \text{as } p \to 0. \tag{4.25}$$

(2) When the probability of link failure (p) is large,

$$\mathbb{k}_{ring} = 1 - \frac{2}{k-1}\varepsilon + o(\varepsilon), \quad \text{as } p \to 1,\ p = 1-\varepsilon. \tag{4.26}$$

For mesh-torus network with k node, $\sqrt{k} > 3, k$ odd, the analytical form of $\mathbb{k}_{torus}$ with 1+1 protection is rather complicated. However, it can be found that

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

$$\mathbb{k}_{torus} = \frac{1}{24}(7k + 6k^{\frac{1}{2}} - 3)p^2 + o(p^2), \quad \text{as } p \to 0. \tag{4.27}$$

(2) When the probability of link failure (p) is large,

$$\mathbb{k}_{torus} = 1 - \frac{4}{k-1}\varepsilon + o(\varepsilon), \quad \text{as } p \to 1,\ p = 1-\varepsilon. \tag{4.28}$$

The network reliabilities of the three typical regular topologies with independent failures are summarized in Table 4.3. It can be found that

(1) With independent failure and 1+1 protection, the mesh-torus network is more reliable than the ring network ($O(kp^2)$). That is because the mesh-torus network generally has shorter primary and backup routes than the ring network.

(2) Compare the same network topology with and without fault protection, it can be found that 1+1 protection increases the network reliability increases significantly when the probability of link failure (p) is small. Specifically, the percentage of lost traffic due to failure decreases by a factor of $O(k)$ and $O(\sqrt{k})$ for the ring and mesh-torus network respectively.

Table 4.3 Network reliabilities of ring, star, and mesh-torus networks; independent Failure

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

4.4.3 Dependent Failure and without Fault Protection

4.4.3.1 Dependent Failure Models

Traditional study of network reliability usually assumes that links in the network fail independently, however, in many scenarios, the status of network links are dependent. For example, the concept of Shared Risk Link Groups (*SRLG*) is proposed to define a set of network elements that are under the impacts of common risk factors [66]. The concept of shared risk factors may include: shared conduit, shared right of way, shared office, and geographic proximity [66]. Parameters such as conditional failure probability per *SRLG* are proposed in [66]. For instance, for two links L_1 and L_2 that share a common physical conduit *D*, a conditional probability of 50% could mean that link L_1 fails with probability 50% if link L_2 fails because of the failure of conduit *D*.

There has been a lot of research about dependent failure models in communication networks, which was pioneered by Spragins [64]. In [64], network failures are modeled using a birth-death process. The dependencies among failures are included in the model

by assuming that the arrival rate of failures varies with the number of existing failures in the network. Since then, different approaches have been proposed to study the dependencies of network failures. In [50], a Markov model was proposed, which assumes a Markov dependency among failures on a sequence of links of interests. A commonly used model of dependent failures is based on the work in [65], and can be represented using a Bayesian Belief Network [75][76]. Two types of random variables are defined in the Bayesian Belief Network representation: (1) variables that correspond to the status of each network link; and (2) variables that correspond to the occurrence of network events, which may cause one or more links to fail. Such a representation is more general and can be considered as a super set of failure models.

In this work, we adopt the dependent failure model in [75][65] and represent it using Bayesian Belief Network. We assume that incident network links may fail simultaneously due to a common risk. This is motivated by the observation that most of the dependent link failures are among links that are incident to a common network node. Incident networks links normally share common risks of failures, e.g. sharing of network node equipments, power. In addition, incident links are located in the same geographic area and are subject to the same abnormal event such as earthquakes and hurricanes.

For instance, we consider the NSF network topology in Figure 4.1, whose dependent failure model based on Bayesian Network is depicted in Figure 4.2. There are 21 links in the NSF network and the status of each link are denoted as $Z_1, Z_2, ..., Z_{21}$: $Z_i = 1$ if link i fails; and $Z_i = 0$ otherwise. Each link may fail due to two types of events:

(1) Events that may only affect the status of link $i, i = 1, 2, ..., 21$, which is denoted as A_i. In this work, we define random variables X_i: $X_i = 1$ if event A_i occurs; and $X_i = 0$

otherwise. In addition, we assume that A_i occurs with probability a_i and the occurrence of event A_i causes link i to fail with probability p_{ai}.

(2) Events that may affect the status of all the links incident at a node $j, j \in \mathbf{V}$, which is denoted as $B_j, j \in \mathbf{V}$. Here we define random variables $Y_j, j \in \mathbf{V}$: $Y_j = 1$ if event B_j occurs; and $Y_j = 0$ otherwise. In addition, we assume that $B_j, j \in \mathbf{V}$, occurs with probability b_j and the occurrence of event B_j may cause link i, which is a link incident on node j, to fail with probability $p_{b,ij}$. In this case, all the links that are incident on node j form a shared risk link group correspond to common risk factor associated with node j.

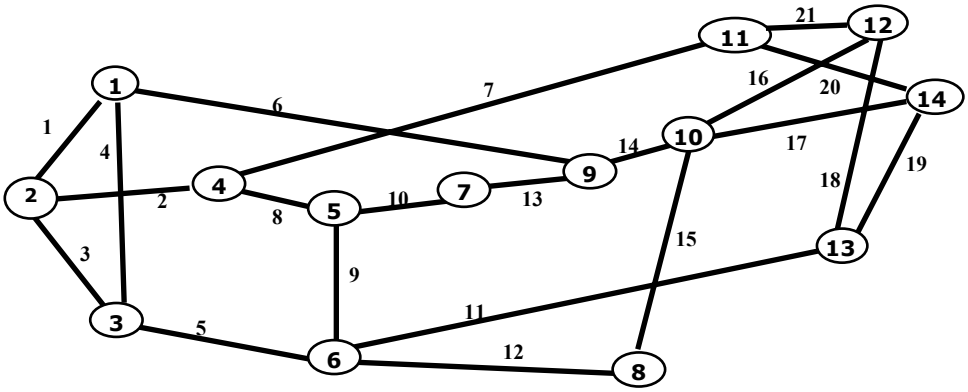

Figure 4.1NSF network topology

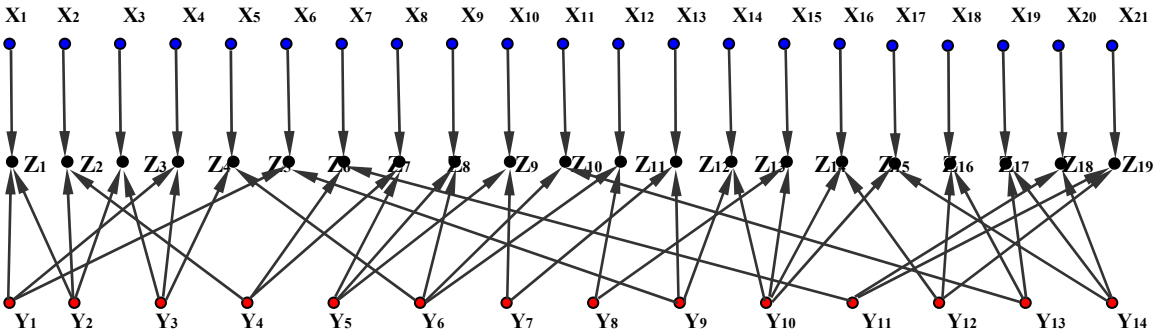

Figure 4.2 Bayesian Belief Network representation of dependent failure models; NSF network

Assuming that all the risk events associated with each link cause the link to fail independent of each other, we have the following set of conditional probabilities for the NSF network based on the dependent failure model in Figure 4.2,

$$P(X_i = 1) = a_i, \quad 1 \le i \le 21; \tag{4.29}$$

$$P(Y_j = 1) = b_j, \quad 1 \le j \le 14; \tag{4.30}$$

$$P(Z_i = 1 \mid X_i, Y_{i_1}, Y_{i_2}) = 1 - (1 - p_{ai})^{X_i} (1 - p_{b,i\,i_1})^{Y_{i_1}} (1 - p_{b,i\,i_2})^{Y_{i_2}}, \quad 1 \le i \le 21; \tag{4.31}$$

$$P(Z_i = 1) = 1 - (1 - a_i p_{ai})(1 - b_i p_{b,i\,i_1})(1 - b_{i+1} p_{b,i\,i_2}), \quad 1 \le i \le 21, \tag{4.32}$$

where

(1) X_i denotes whether event A_i, which can only affect the status of link i, occurs or not, e.g. (a) fiber cut or inline amplifiers failures at link *i*; (b) abnormal events that only affect the geographic location of link *i*. Event A_i occurs with probability a_i, which could be in the range of 10^{-4} to 10^{-8} depending on various factors, such as the vulnerability of the geographic location to natural disasters. The occurrence of event A_i causes link i to fail with probability p_{a_i}, which could be in the range of 0 to 1 based on the severance of the risk event.

(2) Y_{i_1} and Y_{i_2} denote the occurrence of the two risk events B_{i_1} and B_{i_2}, which may affected all the links connected to each of the terminal node of link i respectively. Examples of such events include: (a) failures of the shared network equipments at the node; (b) an abnormal event that that may affect the geographical area where the node is located such as power failure, natural disasters; (c) intentional/unintentional damage of the node. Event B_{i_1} occurs with probability b_{i_1}, which could be in the same range of a_i,

i.e., 10^{-4} to 10^{-8}. The occurrence of event B_{i_1} and B_{i_2} causes link i to fail with probability $p_{b_{i_1}}$ and $p_{b_{i_2}}$, which is also in the range of 0 to 1 based on the severance of the risk event. For simplicity of analysis, we assume that $a_i \equiv a$, $b_{ij} \equiv b$, $p_{ai} \equiv p_a$, and $p_{b_{ij}} \equiv p_b$ in the rest of this chapter.

4.4.3.2Arbitrary Topology

We first consider network reliability with dependent failure and no failure protection in the network. Without loss of generality, we consider the route in **R** between node m and n. We index the nodes along the route as node 0, 1, 2, …, j, and denote the status of links on the route as $Z_{1,mn}, Z_{2,mn}, ..., Z_{j,mn}$, where j is the number of links on the route. For simplicity, we omit the subscript mn in the rest of the section. Then, we have the following theorem,

Theorem 4.3: *Let j be the number of links on route r_{mn}, with dependent failures and no failure protection,*

$$P(S_{mn} = 0) = (1 - ap_a)^j (1 - bp_b)^2 (1 - b(2p_b - p_b^2))^{j-1}, \qquad (4.33)$$

where $S_{mn} = 0$ if there is no link failure on route r_{mn}; and $S_{mn} = 1$ otherwise. In addition, the failure independent assumption overestimates the probability that connections on r_{mn} is lost than the failure dependent assumption, i.e.

$$\frac{1 - \prod_{l=1}^{j} P(Z_j = 0)}{1 - P(Z_1 = 0, Z_2 = 0, ..., Z_j = 0)} = \frac{1 - (1 - ap_a)^j (1 - 2bp_b + b^2 p_b^2)^j}{1 - (1 - ap_a)^j (1 - 2bp_b + b^2 p_b^2)(1 - 2bp_b + bp_b^2)^{j-1}} - 1. \qquad (4.34)$$

The proof of Theorem 4.3 can be found in *Appendix J*. In particular, if $p_b = 1$, which means that the occurrence of event $B_i, i \in \mathbf{V}$, causes all the links incident on node i fail with probability 1, then

$$\frac{1 - \prod_{i=1}^{j} P(Z_i = 0)}{1 - P(Z_1 = 0, Z_2 = 0, ..., Z_j = 0)} = \frac{(j-1)b}{jap_a + (j+1)b}, \qquad \text{if } a << 1 \text{ and } b << 1. \quad (4.35)$$

Clearly, the independent model of failures is a special case of the dependent model with $b = 0$ for all event $B_i, i \in \mathbf{V}$, which means that there is no event that may cause two network links fail simultaneously. From (4.35), we can find that the failure independent 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 reliability. The failure independent assumption overestimate the percentage of lost traffic by a factor close to 100% if $a = O(b)$ or $a << b$. Furthermore, from Theorem 4.3, we have the following corollary

Corollary 4.6: *With failure dependent assumption and without failure protection, 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 under the condition that* $a << 1$ *and* $b << 1$.

The results in Corollary 4.6 are similar to those in Corollary 4.7, and complement the findings in [50], where it has been shown that the Moore graph has the best *all-terminal* reliability, when the link failure probability is low with independent failure assumptions.

4.4.3.3 Typical Topologies

We now consider the ring, star, and mesh-torus network with dependent failures and without failure protection. From Theorem 4.3, we have the following corollaries.

Corollary 4.7: *For ring network with* k *nodes,* $k > 3$,

$$\mathbb{k}_{dep,ring} = \begin{cases} 1 - \dfrac{2(1-bp_b)^2}{(k-1)(1-2bp_b+bp_b^2)}\{(\dfrac{1-q}{q})(1-(1-q)^{\frac{k-1}{2}})\}, & k\ odd, \\ 1 - \dfrac{2(1-bp_b)^2}{(k-1)(1-2bp_b+bp_b^2)}\{(\dfrac{1-q}{q})(1-(1-\dfrac{q}{2})(1-q)^{\frac{k}{2}-1})\}, & k\ even, \end{cases} \tag{4.36}$$

where $q = 1-(1-ap_a)(1-2bp_b+bp_b^2)$. In comparison, the marginal probability of link failure $p = 1-(1-ap_a)(1-2bp_b+b^2p_b^2)$.

In addition, when the probability failure (p) is low, i.e., the probabilities of occurrences for event A_i and B_{ij} , $\forall\, i, j \in V, i \sim j,$ are small,

$$\mathbb{k}_{dep,ring} = \begin{cases} bp_b^2 + \dfrac{(k+1)}{4}(ap_a + 2bp_b - bp_b^2), & k\ odd, \\ bp_b^2 + \dfrac{k^2}{4(k-1)}(ap_a + 2bp_b - bp_b^2), & k\ even, \end{cases} \quad \text{as } a, b \to 0. \tag{4.37}$$

Since $p = 1-(1-ap_a)(1-2bp_b+b^2p_b^2)$, (4.12) can be rewritten as

$$\mathbb{k}_{ring} = \begin{cases} \dfrac{(k+1)}{4}(ap_a + 2bp_b), & k\ odd, \\ \dfrac{k^2}{4(k-1)}(ap_a + 2bp_b), & k\ even, \end{cases} \quad \text{as } a, b \to 0. \tag{4.38}$$

Comparing (4.37) and (4.38), we can find that, for large ring networks, independent assumption overestimate the percentage of lost traffic by a factor of $\frac{bp_b^2}{ap_a + 2bp_b - bp_b^2}$. In addition, the overestimation is larger for a larger value of b or p_b.

Corollary 4.7: For star network with k nodes, $k \geq 3$,

$$\mathbb{k}_{dep,star} = 1 - \frac{(1-bp_b)^2}{k(1-2bp_b+bp_b^2)}\{2(1-q)+(k-2)(1-q)^2\}, \tag{4.39}$$

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

In addition, when the probability of failure (p) is small, i.e., the probabilities of occurrences for event A_i and B_{ij} , $\forall\, i, j \in V, i \sim j,$ are small,

$$\mathbb{k}_{dep,star} = (1+\frac{k-2}{k})(ap_a + 2bp_b - bp_b^2). \tag{4.40}$$

Since (4.14) can be rewritten as

$$\mathbb{k}_{star} = (1+\frac{k-2}{k})(ap_a + 2bp_b), \quad \text{as } p \to 0.$$

Therefore, independent assumption overestimates the percentage of lost traffic by a factor of $\frac{bp_b^2}{ap_a + 2bp_b - bp_b^2}$ for large star networks.

Corollary 4.8: *For mesh-torus network with k nodes, $\sqrt{k} > 3$, k odd*

$$\mathbb{k}_{dep,torus} = 1 - \frac{1}{(m_1^2+m_1)q^2}\frac{(1-bp_b)^2}{(1-2bp_b+bp_b^2)}\{1-q+(1-q)^{2m_1+2}-(2-q)(1-q)^{m_1+1}\},$$

where $m_1 = \frac{\sqrt{k}-1}{2}$, $q = 1-(1-ap_a)(1-2bp_b+bp_b^2)$.

In addition, when the probability of failure (p) is small, i.e., the probabilities of occurrences for event A_i and $B_{ij}, \forall\, i,\, j \in V, i \sim j,$ is small,

$$\mathbb{k}_{dep,torus} = \frac{\sqrt{k}-1}{2}(ap_a + 2bp_b - bP_b^2) - bp_b^2, \quad \text{as } a,b \to 0. \tag{4.41}$$

Comparing (4.41) with (4.18), we can find that independent assumption overestimates the percentage of lost traffic by a factor of $\frac{bp_b^2}{ap_a + 2bp_b - bp_b^2}$ for large mesh-torus networks.

4.4.4 Dependent Failure and 1+1 Fault protection

4.4.4.1 Arbitrary Topology

Without loss of generality, we consider an active connection between node m and n on a route in **R** with j_1 links. Assume that its backup route has j_2 links. Without loss of generality, we assume $j_1 \le j_2$. Then the probability that the connection is not lost for due to failure events for different values of j_1, j_2 are given in *Appendix K*.

Theorem 4.4: *When the probability of failure (p) is small and* $p_b = 1$,

$$P(S_{mn} = 1) = 2b + j_1 j_2 a^2 p_a^2 + (2j_1 j_2 - j_1 - j_2)abp_a + o(a^2) + o(b), \quad \text{as } a^2 << 1 \text{ and } b << 1. \tag{4.42}$$

The proof of Theorem 4.4 can be found in *Appendix K*, where $p_b = 1$ means that the occurrence of type B events at each network node causes all incident links on that node fail simultaneously with probability 1.

With the link failure independent assumption, the probability that the connection between node m and n is lost due to failures on both its primary and backup route is

$$j_1 j_2 a^2 p_a^2 + 4 j_1 j_2 abp_a + o(a^2) + o(b).$$

Thus, with fault protection, the failure independent assumption may correspond to an optimistic view of network reliability. It may underestimate the probability that the connection is lost due to failures significantly. When $p_b = 1$, $a^2 << 1$ *and* $b << 1$, the independent assumption under-estimate the percentage of lost traffic due to failures by a factor of $\frac{2b + j_1 j_2 a^2 p_a^2 + (2j_1 j_2 - j_1 - j_2)abp_a}{j_1 j_2 a^2 p_a^2 + 4 j_1 j_2 abp_a}$. Thus, with dependent failures, fault protection helps the most when the probability of occurrence is small for events that may cause several links fail simultaneously. That is different from the case of independent failures, where fault protection can always improves the network reliability significantly.

4.4.4.2 Typical Topologies

For the ring and mesh-torus networks, from Theorem 4.4, we have the following corollaries.

Corollary 4.9: *For ring network with* k *nodes,* $k > 2$

$$\mathbb{k}_{dep,ring} = \begin{cases} 2b + \frac{k(k+1)}{6} ap_a(ap_a + 2b) - \frac{k+1}{2} abp_a, & k \text{ odd}, \\ 2b + \frac{k(k+1)}{6} ap_a(ap_a + 2b) - \frac{k^2}{2(k-1)} abp_a, & k \text{ even}, \end{cases}$$

$$as\ p_b = 1, a^2, b \to 0. \qquad (4.43)$$

which corresponds to the case that the probability of link failure $p << 1$.

Corollary 4.10: *For mesh-torus network with* k *nodes,* $\sqrt{k} > 3$, k *odd*

$$\mathbb{k}_{dep,torus} = 2b + \frac{7k + 6\sqrt{k} - 3}{24} ap_a(ap_a + 2b) - \frac{\sqrt{k} - 1}{2} abp_a,$$

$$as\ p_b = 1, a^2, b \to 0. \qquad (4.44)$$

which corresponds to the case that the probability of link failure $p << 1$.

In this section, we adopt a simple network layer model to study the effects of physical topologies, network operation schemes (with/without fault protection), and dependencies among physical layer failures on network reliability. Next, we then adopt a random network layer traffic model with Poisson arrivals to further investigate the effect of network layer traffic distributions on network reliability.

4.5 Reliability under Uniform Random Traffic

We now consider a uniform random network-layer traffic model. We denote the network as $\mathbf{G}(\mathbf{V},\mathbf{E})$, with each link j in $\mathbf{E}$ has capacity C. Assume fixed routing on a set of routes $\mathbf{R}$. Without fault protection, $\mathbf{R}$ consists of one link-shortest route between each pair of nodes in the network. With 1+1 protection, $\mathbf{R}$ consists of two link-disjoint routes between each pair of nodes in the network, one of which is a link-shortest route.

We consider in this work a commonly-used model that assumes 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 identically and independent distributed (i.i.d) exponential random variable with unit mean. Then, it has been shown in [81] that, at the equilibrium stage, the stationary distribution of the number of connections in progress in the network is:

$$\pi(\mathbf{N}) = Z^{-1}\prod_{r\in\mathbf{R}}\frac{v^{N_r}}{N_r!}, \quad \mathbf{N}\in\mathbb{S}, \tag{4.45}$$

where N_r is the number of connections on route r, and $\mathbf{N} = (N_r : r \in \mathbf{R})$. $\mathbb{S}$ is the set of vector $\mathbf{N}$ that satisfies the network link capacity constraint. The stationary distribution in (4.45) is intractable due to the difficulty to derive the normalization constant Z. Therefore, we use the Erlang Fixed Point Approximation [81] to obtain analytical results of network reliability.

Erlang Fixed Point Approximation (EFPA) has been shown both theoretically and empirically to be an effective approximation method to investigate the stationary distribution of the network traffic with Poisson arrivals. In particular, for the previously discussed network layer model, there always exist a unique fixed point solution and the solution has been shown to be asymptotically correct [81]. Empirically, EFPA performs well especially for networks with large link capacities and/or networks with non-linear structure. In this work, EFPA is adopted to obtain analytical results of traffic-based network reliability metrics.

4.5.1 Independent Failure and Without Fault protection

When the network has no fault protection, we assume that the route set $\mathbf{R}$ consists of one link-shortest route between each pair of nodes in the network and the arrival rate of connection requests at each route is v. The traffic-based network reliability metrics become

$$\mathbb{Z} = \sum_{ij} E[D_{ij}]E[S_{ij}], \tag{4.46}$$

and

$$\mathbb{k} = \frac{\sum_{ij} E[D_{ij}]E[S_{ij}]}{\sum_{ij} E[D_{ij}]}, \tag{4.47}$$

where $E[D_{ij}]$ is the expected number of active connections on each route $r_{ij} \in \mathbf{R}$ depends on the random traffic model, and $E[S_{ij}]$ is the probability that active connections on route $r_{ij} \in \mathbf{R}$ is lost due to failures. From (4.46) and (4.47), clearly the number of active connections on different network routes varies with the random traffic model, thus affect the amount and percentage of lost connections due to network failures. Next we study the reliability of several typical topologies.

4.5.1.1 Ring Network

For a ring network with k nodes, $k \geq 3$, it can be found that,

$$\mathbb{Z}_{ring} = \begin{cases} k\sum_{l=1}^{\frac{k-1}{2}} \{v(1-B_{ring})^l (1-(1-p)^l)\}, & \text{if } k \text{ is odd,} \\ k\sum_{l=1}^{\frac{k}{2}-1} \{v(1-B_{ring})^l (1-(1-p)^l)\} + \frac{k}{2}\{v(1-B_{ring})^{\frac{k}{2}} (1-(1-p)^{\frac{k}{2}})\}, & \text{if } k \text{ is even,} \end{cases} , \tag{4.48}$$

where $\mathbb{Z}_{ring}$ denotes the average amount of lost traffic due to failures in the ring network.

$$\mathbb{k}_{ring} = \begin{cases} 1 - \dfrac{\sum_{l=1}^{\frac{k-1}{2}} [(1-B_{ring})(1-p)]^l}{\sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l}, & \text{if } k \text{ is odd,} \\ 1 - \dfrac{2\sum_{l=1}^{\frac{k}{2}-1} \{(1-B_{ring})^l (1-p)^l\} + (1-B_{ring})^{\frac{k}{2}} (1-p)^{\frac{k}{2}}}{2\sum_{l=1}^{\frac{k}{2}-1} (1-B_{ring})^l + (1-B_{ring})^{\frac{k}{2}}}, & \text{if } k \text{ is even,} \end{cases} , \tag{4.49}$$

where $\mathbb{k}_{ring}$ denotes the average percentage of lost traffic due to failures in the ring network. B_{ring} in (4.48) and (4.49) can be considered as the link blocking probability obtained form Erlang Fixed Point equations, specifically,

$$B_{ring} = Erlang(\rho_{ring}, C) = \frac{\rho_{ring}^{C}}{C!}(\sum_{i=0}^{C}\frac{\rho_{ring}^{i}}{i!}) \ , \tag{4.50}$$

and

$$\rho_{ring} = \begin{cases} \sum_{j=1}^{\frac{k-1}{2}} \{jv(1-B_{ring})^{(j-1)}\}, \ \text{if } k \text{ is odd}, \\ \sum_{j=1}^{\frac{k}{2}-1} \{jv(1-B_{ring})^{(j-1)}\} + \frac{v}{4}(1-B_{ring})^{\frac{k}{2}-1}, \quad \text{if } k \text{ is even}, \end{cases} . \tag{4.51}$$

In particular, when the network is under heavy load, i.e., $\rho >> C$, we have the following theorem.

Theorem 4.5: *For the k node ring network, under heavy load, as* $v \to \infty$,

$$B_{ring} = 1 - \frac{C-1}{v+1}, \tag{4.52}$$

$$\mathbb{Z}_{ring} = k(C-1)p + o(\frac{C^2 p}{v}), \tag{4.53}$$

$$\mathbb{k}_{ring} = p \, . \tag{4.54}$$

The proof of Theorem 4.5 can be found in *Appendix L*. *(4.52)* 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.

4.5.1.2 Star Network

For star network with k nodes, $k > 2$,

$$\mathbb{Z}_{star} = 0.5(k-2)(k-1)v(1-B_{star})^2(1-(1-p)^2) + (k-1)v(1-B_{star})p, \tag{4.55}$$

$$\mathbb{k}_{star} = \frac{(1-B_{star})p + 0.5(k-2)(1-B_{star})^2(1-(1-p)^2)}{(1-B_{star})p + 0.5(k-2)(1-B_{star})^2}, \tag{4.56}$$

where

$$B_{star} = Erlang(\rho_{star}, C) = \frac{\rho_{star}^C}{C!}(\sum_{i=0}^{C}\frac{\rho_3^i}{i!}), \tag{4.57}$$

$$\rho_{star} = v + (k-2)(1-B_{star})v. \tag{4.58}$$

Furthermore, we have the following theorem.

Theorem 4.6: *For the k node star network, under heavy load, as $v \to \infty$,*

$$\mathbb{Z}_{star} = (k-1)Cp + o(\frac{C^2 p}{v}), \tag{4.59}$$

$$\mathbb{k}_{star} = p, \text{ as } v \to \infty. \tag{4.60}$$

The proof of Theorem 4.6 is similar to that of Theorem 4.7. Details are omitted. (4.59) and (4.60) 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.

4.5.1.3 Mesh-Torus Network

For mesh-torus network with k nodes, $\sqrt{k} > 3$, k odd

$$\mathbb{Z}_{torus} = 2(2m_1+1)^2\{\sum_{i=1}^{m_1} iv(1-B_{torus})^i(1-(1-p)^i) + \sum_{i=m_1+1}^{2m_1}(2m_1+1-i)v(1-B_{torus})^i(1-(1-p)^i)\}, \tag{4.61}$$

$$\mathbb{k}_{torus} = 1 - \frac{\sum_{i=1}^{m_1} i(1-B_{torus})^i (1-p)^i + \sum_{i=m_1+1}^{2m_1} (2m_1+1-i)(1-B_{torus})^i (1-p)^i}{\sum_{i=1}^{m_1} i(1-B_{torus})^i + \sum_{i=m_1+1}^{2m_1} (2m_1+1-i)(1-B_{torus})^i}, \quad (4.62)$$

where $m_1 = \frac{\sqrt{k}-1}{2}$, $B_{torus} = Erlang(\rho_{torus}, C)$, and

$$\rho_{torus} = \sum_{j=1}^{m_1} j^2 v(1-B_{torus})^{j-1} + \sum_{j=m_1+1}^{2m_1} j(2m_1+1-j)v(1-B_{torus})^{j-1}. \quad (4.63)$$

In addition, we have the following theorem.

Theorem 4.7: *Under heavy load, for the mesh-torus network under consideration, as* $v \to \infty$,

$$\mathbb{Z}_{torus} = 2k(C-1)p + o(\frac{C^2 p}{v}), \quad (4.64)$$

$$\mathbb{k}_{torus} = p. \quad (4.65)$$

The proof of Theorem 4.7 is similar to tat of Theorem 4.5. Details are omitted. From (4.64) and (4.65), it can be found that: under heavy load, the expected number of lost connections due to failures approaches $2k(C-1)p$ and the expected percentage of lost connections due to failures approaches p in the mesh-torus network.

4.5.1.4 Other Results on Reliability of Typical Topologies

We have obtained the following theorems for the network reliabilities of the ring, star, and mesh torus network discussed in Section 4.5.2 under the uniform random traffic model.

Theorem 4.8 *The link blocking probability from EFPA monotonically increases with the arrival rate, i.e.,* $\frac{\partial B}{\partial v} > 0,$ *for the ring, star, and mesh torus networks, with independent failure and no fault protection.*

The proof of Theorem 4.8 can be found in *Appendix M*. Intuitively, Theorem 3.8 results from the observation that: as the connection arrival rate increases, the number of free capacities on each network link generally decreases, and thus the link-blocking probability increases.

Theorem 4.9 *The percentage of lost traffic due to failures is monotonically nonincreasing with the arrival rate, i.e.,* $\frac{\partial \mathbb{k}}{\partial v} \le 0$, *for the ring, star, and mesh torus networks, with independent failure and no fault protection.*

The proof of Theorem 4.9 can be found in *Appendix N*. Theorem 4.9 can be explained as follows. As the connection arrival rate increases, a larger percentage of active connections are on short routes. Since the shorter routes are less likely to subject to network failures than longer routes, the expected percentage of lost traffic due to failures decreases as connection arrival rate decreases.

Theorem 4.10 *Both the amount of lost traffic and the percentage of lost traffic monotonically increase with the arrival rate, i.e.,* $\frac{\partial \mathbb{Z}}{\partial p} > 0$ and $\frac{\partial \mathbb{k}}{\partial p} > 0$, *for the ring, star, and mesh torus networks, with independent failure and no fault protection.*

The proof of Theorem 4.3 is straightforward, and is omitted. In addition, we can find that, the amount of lost traffic does not vary monotonically with the arrival rate. Furthermore,

$\frac{\partial^2 \mathbb{Z}}{\partial v \partial p} > 0$, which means that for a larger link failure probability p, it is more likely that the amount of lost traffic increases with the arrival rate.

4.5.2 Independent Failure and With Fault protection

In this subsection, we consider network reliability with independent failure and with 1+1 protection using the uniform random traffic model.

4.5.2.1 Ring Network

With 1+1 protection, the capacity needs to be allocated to both the primary and the backup route. Therefore, for the ring network, each connection request always requires capacity from k links regardless of the source and destination. Thus,

$$\mathbb{Z} = kv(1 - B_{ring,pro})\{1 + (1-p)^k - \frac{2}{k-1}(\frac{(1-p)-(1-p)^k}{p})\}, \tag{4.66}$$

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

$$\mathbb{k}_{ring} = 1 + (1-p)^k - \frac{2}{k-1}(\frac{(1-p)-(1-p)^k}{p}). \tag{4.67}$$

From (4.66) and (4.67), it can be found that, for the ring network, with independent failure and 1+1 protection:

(1) $\frac{\partial B_{ring,pro}}{\partial v} > 0$, which means that the link blocking probability obtained from EFPA monotonically increases with the arrival rate.

(2) $\frac{\partial \mathbb{Z}_{ring,pro}}{\partial v} > 0$, which means that the amount of lost traffic increases monotonically with the arrival rate. This is different for the case of ring network without protection.

(3) $\frac{\partial \mathbb{k}_{ring,pro}}{\partial v} = 0$, which means that the percentage of lost traffic due to failures does not change with respect to arrival rate. This is different from the case of ring network without fault protection.

(4) $\frac{\partial \mathbb{Z}_{ring,pro}}{\partial p} > 0$ and $\frac{\partial \mathbb{k}_{ring,pro}}{\partial p} > 0$, which means that both the amount of lost traffic and the percentage of lost traffic monotonically increase with the arrival rate.

4.5.2.2 Mesh-Torus Network

For mesh-torus network with k nodes, $\sqrt{k} > 3$, k odd

$$\mathbb{Z}_{torus,pro} = 2(2m_1+1)^2 v\{\sum_{i=1}^{m_1}[(i-1)(1-B_{torus,pro})^{2i}(1-(1-p)^i)^2 + \sum_{i=1}^{m_1}(1-B_{torus,pro})^{2m_1+1}(1-(1-p)^i)(1-(1-p)^{2m_1+1-i}) + \sum_{i=m_1+1}^{2m_1}(2m_1+1-i)(1-B_{torus,pro})^{2i}(1-(1-p)^i)^2\}, \quad (4.68)$$

$$\mathbb{k}_{torus,pro} = \frac{\mathbb{Z}_{torus,pro}}{2(2m_1+1)^2 v\{\sum_{i=1}^{m_1}[(i-1)(1-B_{torus,pro})^{2i} + (1-B_{torus,pro})^{2m_1+1}] + \sum_{i=m_1+1}^{2m_1}(2m_1+1-i)(1-B_{torus,pro})^{2i}\}}. \quad (4.69)$$

From (4.68) and (4.69), it can be found that, for the mesh torus network, with independent failure and 1+1 protection,

(1) $\frac{\partial B_{torus,pro}}{\partial v} > 0$, which means that the link blocking probability increases with the arrival rate.

(2) The amount of lost traffic does not vary monotonically with the arrival rate. This is different from the ring network with fault protection.

(3) $\frac{\partial \mathbb{k}_{torus,pro}}{\partial v} < 0$, which means that the percentage of lost traffic due to failures monotonically decreases with the arrival rate. This is different from the case of ring networks with fault protection.

(4) $\frac{\partial \mathbb{Z}_{torus,pro}}{\partial p} > 0$ and $\frac{\partial \mathbb{k}_{torus,pro}}{\partial p} > 0$, which means that both the amount of lost traffic and the percentage of lost traffic monotonically increase with the arrival rate.

4.5.3 Dependent Failure and without Fault protection

4.5.3.1Numerical Results

In this subsection, we consider the network reliability with dependent failures and without protection. From Theorem 4.3, we can find that the independent failure assumption overestimates the amount and percentage of lost traffic due to failures. Specifically, for an active connection on a route with j links, the failure independent assumption overestimates its probability of loss due to failures by a factor of $\frac{(j-1)b}{jap_a + (j+1)b}$ for $a, b << 1$.

For instance, we consider the percentage of lost traffic due to failures for a 14 node ring network and the 14 node NSF network using Erlang Fixed Point method.

Using the NSF network topology as an example, we first revisit the model of dependent failures used in this study. We consider an arbitrary network link *i.* In our model, link *i* may fail due to two types of events:

(1) Events that may only affect the status of link i, which is denoted as A_i. For instance, in optical networks, event A_i may include: (a) fiber cut or inline amplifiers failures at

link *i*; (b) abnormal events that may only cause link *i* to fail such as natural disasters that only affect the geographic location of link *i*; and (c) intentional/unintentional damage of the link. We let the probability of occurrence of A_i be a_i and the occurrence of event A_i causes link i to fail with probability p_{ai}.

(2) Events that may affect the status of link i and other network links that share a common risk factor with link i. In this work assume that incident network links may fail simultaneously due to a common risk. This is because most of the dependent link failures are among links that are incident to a common network node, which share common risks of failures such as network node equipments, power outages. In addition, incident links are located in the same geographic area and are subject to the same abnormal event such as earthquakes and hurricanes. In particular, we denote events that may affect the status of all the links incident at a node $j, j \in \mathbf{V}$, as $B_j, j \in \mathbf{V}$. Furthermore, we assume that $B_j, j \in \mathbf{V}$, occurs with probability b_j and the occurrence of event B_j may cause link i, which is a link incident on node j, to fail with probability $p_{b,ij}$.

For illustration, we consider two sets of parameters for dependent failure models: one corresponds to high probability of failure; the other corresponds to small probability of failure. Figure 4.3 depicts the percentage of lost traffic vs. the connection arrival rate for the 14 node ring and NSF networks. 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 $p = 2.5 \times 10^{-4}$.

Figure 4.4 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 $p = 2.5 \times 10^{-6}$.

It can be found that the failure independent assumption over-estimates 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 (45% for the ring network and 25% for the NSF network). The magnitude of over-estimation of the percentage of lost traffic 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 our findings in Theorem 4.5.

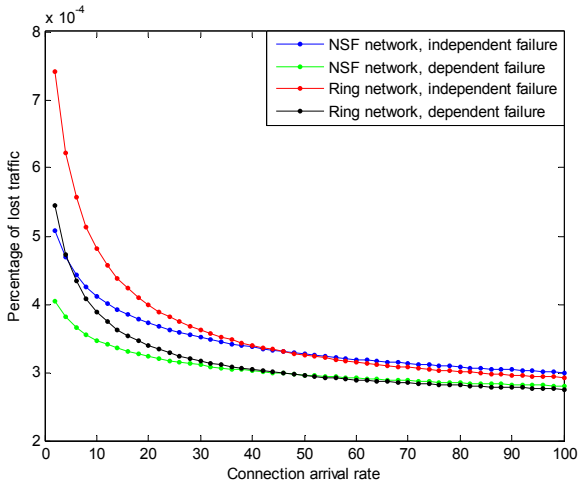

Figure 4.3 Percentage of lost traffic vs. connection arrival rate; 14-node ring and NSF networks; $a = 10^{-4}$, $p_a = 0.5$, $b = 10^{-4}$, $p_b = 1.0$, $C = 20$

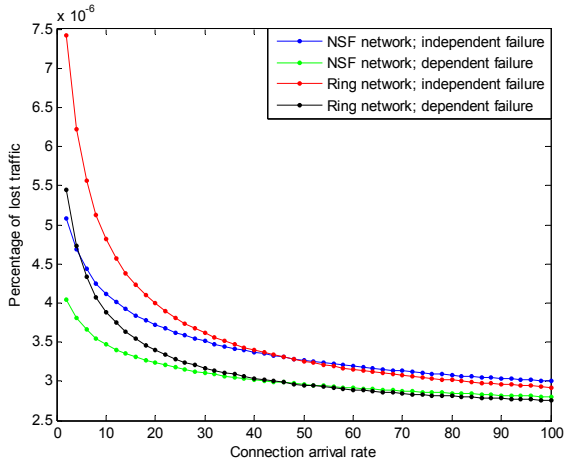

Figure 4.4 Percentage of lost traffic vs. connection arrival rate; 14-node ring and NSF networks; $a = 10^{-6}$, $p_a = 0.5$, $b = 10^{-6}$, $p_b = 1.0$, $C = 20$

4.5.3.2. Graphical Representation of Dependencies

When the link failures are dependent, there are dependencies at both the physical layer and the network layer. A visual display of the dependencies can be obtained through a factor graph representation [43] of the network layer traffic and the physical layer failures.

For simplicity of illustration, we consider a 5-node ring network. There are total 10 routes in **R**, which corresponds to one link-shortest route between each pair of nodes in the network. The factor graph representation of the interaction between the physical layer and network layer are shown in Figure 4.5.

The upper part of the representation in Figure 4.5 correspond to the network layer traffic model, where N_i, $i = 1, 2, ..., 10$, denotes the number of active connections on route i. The lower part of the representation correspond to the physical layer dependent failure models, where $Z_i, i = 1, 2, ..., 5$ denotes the status of link i; $X_i, i = 1, 2, ..., 5,$ denotes the occurrence of event A_i that may only affect link i; $Y_i, i = 1, 2, ..., 5,$ denotes the occurrence of event B_i that may affect both links incident on node i. The green dot in the factor graph representation then corresponds to the number of active connections lost due to failures at each network route.

The graphical representation provides an explicit display of the dependencies among link failures at the physical layer and the dependencies among traffic flows at the network layer. In addition, it shows potential as a strong approach to consider more sophisticated network traffic models and to further investigate the interaction between the physical layer failures and network layer traffic.

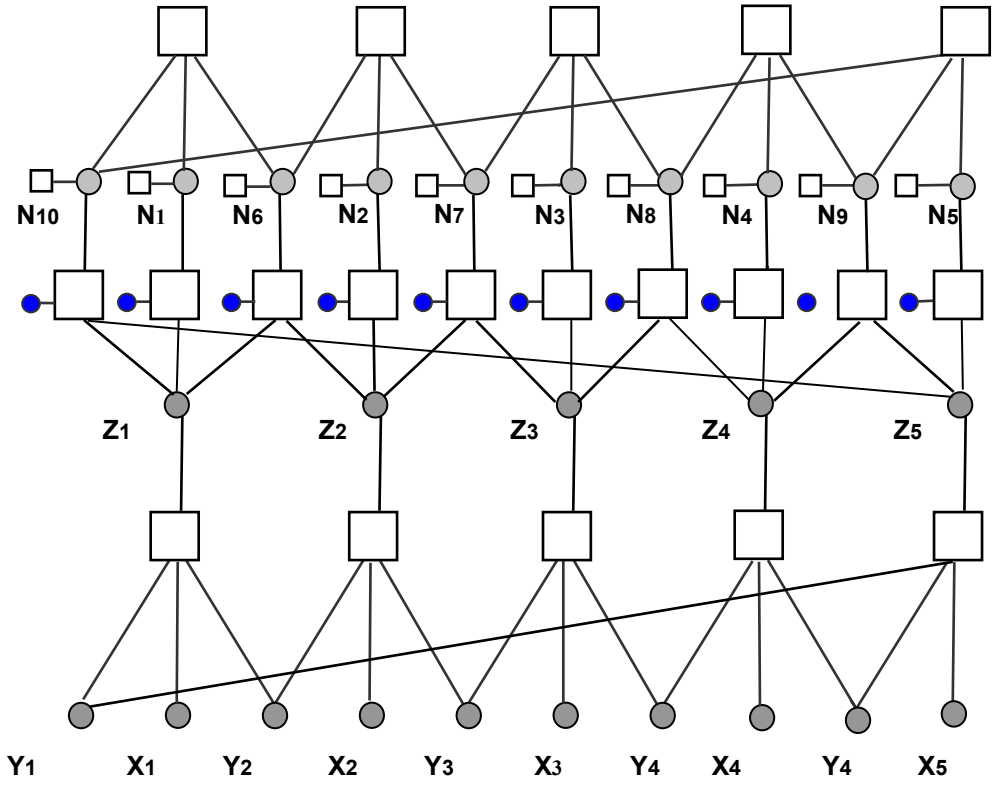

Figure 4.5 Factor graph representation of the network and the physical layer model; 5-node ring network

4.6 Summary of Chapter 4

In this Chapter, we have systematically investigated different factors that affect traffic-based network reliability. We first adopted a uniform deterministic traffic at the network layer, which allows us to focus on the impacts of the first three factors on network reliability. We have summarized the network reliabilities of ring, star and mesh-torus networks when the probability of link failure is small in Table 4.4. It has been found that:

(1) The effect of physical topologies

Networks with the smallest average route length are the most reliable. For instance, without protection, the average percentage of lost traffic due to failures for the star network is around $2(ap_a + bp_b)$ when the probability of link failure is small; whereas the

percentage of lost traffic for the ring and mesh-torus network are $O(k(ap_a + bp_b))$ and $O(\sqrt{k}(ap_a + bp_b))$ respectively.

Table 4.4 Network reliabilities; ring, star, and mesh-torus network; uniform deterministic traffic model; small probability of link failure

	Ring	Star	Mesh-Torus
Independent failure; without failure protection	$\frac{(k+1)}{4}(ap_a + 2bp_b)$	$(1+\frac{k-2}{k})(ap_a + 2bp_b)$	$\frac{\sqrt{k}-1}{2}(ap_a + 2bp_b)$
Dependent failure; without failure protection	$bp_b^2 + \frac{(k+1)}{4}(ap_a + 2bp_b - bp_b^2)$	$(1+\frac{k-2}{k})(ap_a + 2bp_b - bp_b^2)$	$\frac{\sqrt{k}-1}{2}(ap_a + 2bp_b - bP_b^2) - bp_b^2$
Independent failure; with failure protection	$\frac{k(k+1)}{6}ap_a(ap_a + 2bp_b)$	N/A	$\frac{7k+6\sqrt{k}-3}{24}\ ap_a(ap_a + 2bp_b)$

(2) The effect of dependencies among physical layer failures

The failure independent assumption may have different effect when the network operates with or without fault protections. Generally, for networks without protection, failure independent assumption overestimates the percentage of lost traffic. Specifically, for an active connection on a route with j links, the failure independent assumption overestimates its probability of loss due to failures by a factor of $\frac{(j-1)b}{jap_a + (j+1)b}$ for $a, b << 1$. For networks with protection, the failure independent assumption may underestimate the percentage of lost traffic significantly by a factor of $\frac{2b + j_1 j_2 a^2 p_a^2 + (2j_1 j_2 - j_1 - j_2)abp_a}{j_1 j_2 a^2 p_a^2 + 4j_1 j_2 abp_a}$. Thus with failure protection, independent failure assumption may overestimate network reliability drastically.

(3) Effect of fault protection

When the link failures are independent in the network, fault protection can increases network reliability significantly, e.g., reduce the percentage of lost traffic by a factor of $O(\frac{1}{k}p)$ for the ring network. When the link failures are dependent in the network, to increase the effectiveness of fault protection, it is important to reduce the probability of occurrence for those events that are common risks of several links.

Furthermore, we have adopted a random network layer traffic model with Poisson arrivals to further investigate the effect of network layer traffic distributions on network reliability. We have focused on the interaction between the network reliability measures and the connection arrival rate. The findings on several typical topologies are summarized in Table 4.5. It can be found that:

(1) For the ring, star, mesh-torus networks considered, the percentage of lost traffic monotonically decreases with connection arrival rate if there is no connection fault protection. Based on the metric of percentage of lost connections due to failures, the network is more reliable with a larger connection rate.

(2) The amount of lost traffic upon failure does not vary monotonically with connection arrival rate. Furthermore, the interaction may change depending on the physical layer link failure probabilities. For instance, whether the network connections have fault protection or not changes the interaction between network reliability metrics and connection arrival rate, as in the case of ring network.

Table 4.5 Network reliabilities; ring, star, and mesh-torus networks; uniform random traffic model

	Ring	Star	Mesh-Torus
Independent failure; without failure protection	$\frac{\partial B}{\partial v} > 0,$ $\frac{\partial k}{\partial v} \leq 0$ $\frac{\partial \mathbb{Z}}{\partial v} > 0$ or $\frac{\partial \mathbb{Z}}{\partial v} < 0$ $\frac{\partial \mathbb{Z}}{\partial p} > 0$ and $\frac{\partial k}{\partial p} > 0$	$\frac{\partial B}{\partial v} > 0,$ $\frac{\partial k}{\partial v} \leq 0$ $\frac{\partial \mathbb{Z}}{\partial v} > 0$ or $\frac{\partial \mathbb{Z}}{\partial v} < 0$ $\frac{\partial \mathbb{Z}}{\partial p} > 0$ and $\frac{\partial k}{\partial p} > 0$	$\frac{\partial B}{\partial v} > 0,$ $\frac{\partial k}{\partial v} \leq 0$ $\frac{\partial \mathbb{Z}}{\partial v} > 0$ or $\frac{\partial \mathbb{Z}}{\partial v} < 0$ $\frac{\partial \mathbb{Z}}{\partial p} > 0$ and $\frac{\partial k}{\partial p} > 0$
Independent failure; with failure protection	$\frac{\partial B}{\partial v} > 0,$ $\frac{\partial \mathbb{Z}}{\partial v} > 0,$ $\frac{\partial k}{\partial v} = 0$ $\frac{\partial \mathbb{Z}}{\partial p} > 0$ and $\frac{\partial k}{\partial p} > 0$	N/A	$\frac{\partial B}{\partial v} > 0,$ $\frac{\partial k}{\partial v} < 0$ $\frac{\partial \mathbb{Z}}{\partial v} > 0$ or $\frac{\partial \mathbb{Z}}{\partial v} < 0$ $\frac{\partial \mathbb{Z}}{\partial p} > 0$ and $\frac{\partial k}{\partial p} > 0$

We also obtained the asymptotic results of network reliability metrics with respect to arrival rate for typical network topologies under heavy load regime. It has been shown that, under heavy load regime, the percentage of lost traffic due to failures approaches p with failure independent assumption. In addition, we provided graphical representation of the dependencies among the network layer and the physical layer.

Our investigation of traffic-based reliability focuses on "open-loop" analysis. Thus one future direction of research is to further consider the interaction of network traffic and the physical failure models. In addition, our investigation of traffic-based network reliability is limited to circuit-switched networks. Another future research direction is to extend the study to packet-switched networks.

CHAPTER 5

CONCLUSION

This final chapter summarizes the contributions of the thesis and discusses about the future directions of research.

5.1 Contributions

The main contributions of this thesis include: (1) fundamental understanding of scalable management and resilience of next-generation optical networks with flow switching; and (2) application of probabilistic graphical models, an emerging approach in machine learning, to the research of communication networks.

To understand scalable network management, we have investigated network management information for light-path assessment across administrative domains. Our technical approach is based on the framework of decision theory and probabilistic graphical models. Our focus has been on studying the scalability of management information, which includes aggregated information of each subnet, and local information from wavelength converters on network boundaries. We have formulated the problem based on decision theory, and defined the performance of using partial management information through the Bayes probability of error. A bound in terms of blocking probability is derived to estimate such a performance. We then defined the scalability of management information as the growth rate with respect to network size and resource when a desired performance is achieved. A scalable case has been studied where the partial management information grows only logarithmically with the number of wavelengths per link. Our study reveals that when the number of wavelengths is large,

the resulting Bayes error is negligibly small for most of the network load conditions. Therefore, a small loss in performance (the Bayes error) may be traded off with a large saving in network management information.

To understand network resilience under malicious attacks, we have studied resilience of all-optical networks (AONs) under in-band crosstalk attacks. We have developed a cross-layer model of attack propagation based on probabilistic models. The model provides an explicit representation of the dependencies and interactions between the physical- and the network layer. In addition, it facilitates the analytical investigation of network resilience for ring, star, and special cases of mesh topologies, and provides computationally efficient approaches, e.g. the sum-product algorithm, for evaluating network resilience. Through both analysis and numerical study, we have explored several factors from both the physical- and the network layer that affect the resilience. Factors from the physical-layer include: (1) the physical-layer vulnerability, parameters in Bayesian Belief Network that characterize how likely the attack propagates, and (2) the physical topology. Factors from the network layer include active network connections that are characterized using network load, i.e., the probability that the wavelength, on which the attack is initiated, is used in the network. We have shown that for all the topologies studied in this thesis, the average network resilience loss increases linearly with respect to the physical-layer vulnerability and light network load under link-shortest routing, and all-to-all traffic. In addition, ring and mesh-torus network show good resilience, which are inversely proportional to the number of the nodes in the network. Numerical results also suggest that for networks with link-shortest routing and all-to-all

traffic, the network resilience loss increases at least linearly with respect to the network load.

To understand network performance upon failure events, we systematically investigate traffic-based network reliability. We first adopt a uniform deterministic traffic at the network layer, which allows us to focus on the impacts of network topology, failure dependency, and failure protection on network reliability and obtain analytical results on the network reliabilities of ring, star and mesh-torus networks. We then apply a random network layer traffic model with Poisson arrivals to further investigate the effect of network layer traffic distributions on network reliability. We study the interaction between the network reliability and the connection arrival rate, and obtain asymptotic results of network reliability metrics with respect to arrival rate for typical network topologies under heavy load regime.

5.2 Future Research Directions

5.2.1 Management Information for Inter-Domain Light-Path Assessment

The problem of light-path assessment is related to wavelength routing. One thought resulting from this work is to use aggregated information for wavelength routing when it is impractical to flood detailed link state information across the whole network. For instance, light-path assessment could be done for each candidate route based on aggregated information from each network domain and instantaneous measurements from a limited number of links. The optimal route can then be chosen accordingly. Detailed relationships need to be derived between light-path assessment and wavelength routing, which can be one of the extensions to this work.

5.2.2 Resilience of All-Optical Networks under In-Band Crosstalk Attacks

The cross-layer model of crosstalk attack propagation is developed under stringent assumptions. Therefore, one future research direction is to develop more general physical-layer models of attack propagation under less stringent conditions. Another research direction is to consider the effect of dynamic network resource allocation algorithms on attack propagation. Finally, the technique of probabilistic graphical models may also apply to other faults/attacks problems in all-optical networks.

5.2.3 Traffic-Based Network Reliability

Our investigation of traffic-based reliability focuses on "open-loop" analysis. Thus one future direction of research is to further consider the interaction of network traffic and the physical failure models. In addition, our investigation of traffic-based network reliability is limited to circuit-switched networks. Another future research direction is to extend the study to packet-switched networks.

APPENDIX A

PROOF OF THEOREM 2.1

Proof: Consider the following *a posterior* probability:

$$f(x) = P(\omega = 1 \big| X = x). \tag{A.1}$$

The Bayes rule decides

$$\begin{cases} \omega = 1 \quad if \quad f(x) \geq 1/2, \\ \omega = 0 \quad otherwise. \end{cases}$$

Therefore,

$$\begin{aligned} P_e &= \sum_X P_{e|X=x} P(X = x) \\ &= \sum_X P(X = x) \min\{f(x), (1 - f(x))\} \\ &\leq \min\{\sum_X P(X = x) f(x), \sum_X P(X = x)(1 - f(x))\}. \end{aligned} \tag{A.2}$$

Since $P_b = 1 - \sum_X P(X = x) f(x)$, we have

$$0 \leq P_e \leq \min\{P_b, (1 - P_b)\}.$$

APPENDIX B

DERIVATION OF THE CORRELATION COEFFICIENT IN (2.26)

Let $W_{mi} = 1$ if wavelength m is used for an inter-domain call at domain i, $W_{mi} = 0$ otherwise; Let $L_{mi} = 1$ if wavelength m is used for a local call at the first link of domain i, $L_{mi} = 0$ otherwise, where $m = 1, 2, \cdots, F$, and $i = 1, 2, \cdots, L$. From the assumptions in Section 2.6.1, the following joint probabilities hold for $i = 1, 2, \cdots, L-1$:

$$P(W_{mi} = 1, W_{m\,i+1} = 1) = \rho_2[P_n P_l + (1 - P_l)]; \tag{B.1}$$

$$\begin{aligned} P(W_{mi} = 1, L_{m\,i+1} = 1) &= \sum_{k=0}^{1} P(W_{mi} = 1, W_{m\,i+1} = k, L_{m\,i+1} = 1) \\ &= \sum_{k=0}^{1} P(W_{mi} = 1) P(W_{m\,i+1} = k \,|\, W_{mi} = 1) P(L_{m\,i+1} = 1 \,|\, W_{mi} = 1, W_{m\,i+1} = k) \\ &= P(W_{mi} = 1) P(W_{m\,i+1} = 0 \,|\, W_{mi} = 1)\, P(L_{m\,i+1} = 1 \,|\, W_{mi} = 1, W_{m\,i+1} = 0) \\ &= \rho_2 (P_l - P_n P_l)(\frac{\rho_1}{1 - \rho_2}); \end{aligned} \tag{B.2}$$

$$\begin{aligned} P(L_{mi} = 1, L_{m\,i+1} = 1) &= \sum_{k=0}^{1} P(L_{mi} = 1, W_{m\,i+1} = k, L_{m\,i+1} = 1) \\ &= \sum_{k=0}^{1} P(L_{mi} = 1) P(W_{m\,i+1} = k \,|\, L_{mi} = 1) P(L_{m\,i+1} = 1 \,|\, L_{mi} = 1, W_{m\,i+1} = k) \\ &= P(L_{mi} = 1) P(W_{m\,i+1} = 0 \,|\, L_{mi} = 1)\, P(L_{m\,i+1} = 1 \,|\, L_{mi} = 1, W_{m\,i+1} = 0) \\ &= \rho_1 (1 - P_n)(\frac{\rho_1}{1 - \rho_2}); \end{aligned} \tag{B.3}$$

$$P(L_{mi} = 1, W_{m\,i+1} = 1) = \rho_1 P_n. \tag{B.4}$$

Then,

$$\begin{aligned} C_{i\,i+1} &= E[N_i N_{i+1}] - F^2 \rho^2 \\ &= E[N_{ii} N_{i+1\,i+1}] + E[N_{ii} M_{i+1}] + E[M_i N_{i+1\,i+1}] + E[M_i M_{i+1}] - F^2 \rho^2. \end{aligned} \tag{B.5}$$

From (B.1), we have,

$$\begin{aligned} E[N_{ii}N_{i+1\,i+1}] &= E[\sum_{m=1}^{F} L_{mi} \sum_{n=1}^{F} L_{n\,i+1}] \\ &= E[\sum_{m=1}^{F} L_{mi}L_{m\,i+1}] + F(F-1)\rho_1^2 \\ &= FP(L_{mi}=1, L_{m\,i+1}=1) + F(F-1)\rho_1^2 \\ &= F\rho_1(1-P_n)(\frac{\rho_1}{1-\rho_2}) + F(F-1)\rho_1^2. \end{aligned} \tag{B.6}$$

Similarly, we have

$$\begin{aligned} E[N_{ii}M_{i+1}] &= E[\sum_{m=1}^{F} L_{mi} \sum_{n=1}^{F} W_{n\,i+1}] \\ &= F\rho_1 P_n + F(F-1)\rho_1\rho_2; \end{aligned} \tag{B.7}$$

$$\begin{aligned} E[M_i N_{i+1\,i+1}] &= E[\sum_{m=1}^{F} W_{mi} \sum_{n=1}^{F} L_{n\,i+1}] \\ &= F\rho_2(P_l - P_n P_l)(\frac{\rho_1}{1-\rho_2}) + F(F-1)\rho_1\rho_2; \end{aligned} \tag{B.8}$$

$$\begin{aligned} E[M_i M_{i+1}] &= E[\sum_{m=1}^{F} W_{mi} \sum_{n=1}^{F} W_{n\,i+1}] \\ &= F\rho_2(P_n P_l + 1 - P_l) + F(F-1)\rho_2^2. \end{aligned} \tag{B.9}$$

From (2.11), we have

$$\rho_2 = (1-\rho_2)P_n + \rho_2[P_n P_l + (1-P_l)]. \tag{B.10}$$

Then $C_{i\,i+1}$ can be simplified as

$$C_{i\,i+1} = F[\frac{(1-\rho)^2(\rho_2 - P_n)}{(1-\rho_2)}]. \tag{B.11}$$

Therefore,

$$\rho_g = \frac{C_{ij}}{\sigma^2} = \frac{C_{ij}}{F\rho(1-\rho)} = \frac{(1-\rho)(\rho_2 - P_n)}{(1-\rho_2)\rho}.$$

APPENDIX C

PROOF OF THEOREM 2.2

Proof: The non-blocking probability of the dependent model satisfies $P_{ad} = E[f(\omega = 1 | X)]$. Since $X = (N_1, ..., N_L)$ are jointly Gaussian, we can expand P_{ad} in terms of ρ_{ij}'s as follows,

$$P_{ad} = P_{ad}^{*} + \frac{\partial P_{ad}}{\partial \rho_g}\Big|_{\rho_g = 0} \rho_g + o(\rho_g), \tag{C.1}$$

where P_{ad}^{*} is the non-blocking probability of the dependent model when all the inter-domain calls only last for one subnet ($P_l = 1$). Specifically, we have

$$P_{ad}^{*} = \left\{1 - [1 - (1-\rho)(1-\rho_c)^{H-1}]^F\right\}^L. \tag{C.2}$$

Let $\gamma = [1 - (1-\rho_c)^{H-1}]$, then

$$\begin{aligned} &\frac{\partial P_{ad}}{\partial \rho_g} \\ &= \frac{\partial}{\partial \rho_g}\left(\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} P(N_1, N_2, \cdots, N_L)\prod_{i=1}^{L}(1-\gamma^{(F-N_i)})dN_1 dN_2 \ldots dN_L\right) \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\frac{\partial}{\partial \rho_g}\left(P(N_1, N_2, \cdots, N_L)\prod_{i=1}^{L}(1-\gamma^{(F-N_i)})\right)dN_1 dN_2 \ldots dN_L. \end{aligned} \tag{C.3}$$

When $\rho_g = 0$,

$$\frac{\partial P_{ad}}{\partial \rho_g} = \left\{1 - [1 - (1-\rho)(1-\rho_c)^{H-1}]^F\right\}^{L-2} q_{ij}, \tag{C.4}$$

where $q_{ij} = (L-1)\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}(1-\gamma^{F-N_i})(1-\gamma^{F-N_j})\frac{\partial f(\pi_i, \pi_j; \rho_{ij})}{\partial \rho_{ij}}\Big|_{\rho_{i,j}=0} dN_i dN_j$,

with $f(\pi_i, \pi_j; \rho_{ij})$ being the joint Gaussian p.d.f. of N_i and N_j.

Simplifying q_{ij}, we have,

$$q_{ij} = \frac{(L-1)}{F\rho(1-\rho)}\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(\pi_i, \pi_j, 0)(N_i - F\rho)(N_j - F\rho)(1-\gamma^{F-N_i})(1-\gamma^{F-N_j})dN_i dN_j\}. \tag{C.5}$$

Using the characteristic functions of Gaussian r.v.'s, we have

$$q_{ij} = (L-1)\gamma^{2(F-\mu)+\sigma^2 \ln\gamma}\sigma^2 \ln^2 \gamma, \tag{C.6}$$

Therefore, we have

$$P_{ad} = P_{ad}^{*}(1+\eta) + o(\rho_g), \tag{C.7}$$

where

$$\eta = \frac{q_{ij}}{\{1-[1-(1-\rho)(1-\rho_c)^{H-1}]^F\}^2}\rho_g.$$

APPENDIX D

DERIVATION OF (3.7) TO (3.9)

Let U_i denote the jamming power of the attack flow at node $V_i, \forall V_i \in \mathbf{V}_{f_{sd}}$. We first show that if $U_i \geq U_{i+1}$ for $1 \leq i < k$, then $P(X_{i+1} \mid X_1, X_2 ..., X_i) = P(X_{i+1} \mid X_i)$.

Suppose $U_i \geq U_{i+1}$. Since $X_i = 1$, if $U_i > c_{th}/(l_c u_n)$; and $X_i = 0,$ otherwise, it follows that

$$P(X_1 = x_1, X_2 = x_2, ..., X_i = x_i) \neq 0, \text{ only if } x_1 \geq x_2 \geq ... \geq x_i. \tag{D.1}$$

Let $k_1 = \max\{j : x_j = 1 \,\&\, 1 \leq j \leq i\}$, which is the largest index of nodes affected by the attack among $V_1, V_2, ..., V_i$. Then,

(a) If $1 \leq k_1 < i$, then $X_1 = 1, ... X_{k_1} = 1, X_{k_1+1} = 0, ..., X_i = 0$.

$$\begin{aligned} &P(X_{i+1} = 0 \mid X_1 = 1, ... X_{k_1} = 1, X_{k_1+1} = 0, ..., X_i = 0) \\ &= \frac{P(X_1 = 1, ..., X_{k_1} = 1, X_{k_1+1} = 0, ..., X_i = 0, X_{i+1} = 0)}{P(X_1 = 1, ..., X_{k_1} = 1, X_{k_1+1} = 0, ..., X_i = 0)} \\ &= \frac{P(X_{k_1} = 1, X_{k_1+1} = 0)}{P(X_{k_1} = 1, X_{k_1+1} = 0)} = 1. \end{aligned} \tag{D.2}$$

Obviously, $P(X_{i+1} = 0 \mid X_i = 0) = 1.$ Therefore,

$$P(X_{i+1} \mid X_1, X_2 ..., X_i) = P(X_{i+1} \mid X_i).$$

(b) If $1 \leq k_1 = i$, $X_1 = 1, ..., X_i = 1.$

$$\begin{aligned} P(X_{i+1} = 0 \mid X_1 = 1, ..., X_i = 1) &= \frac{P(X_1 = 1, ..., X_i = 1, X_{i+1} = 0)}{P(X_1 = 1, ..., X_i = 1)} \\ &= \frac{P(U_1 > c_{th}/(l_c u_n), ..., U_i > c_{th}/(l_c u_n), U_{i+1} < c_{th}/(l_c u_n))}{P(U_1 > c_{th}/(l_c u_n), ..., U_i > c_{th}/(l_c u_n))} \\ &= \frac{P(U_i > c_{th}/(l_c u_n), U_{i+1} < c_{th}/(l_c u_n))}{P(U_i > c_{th}/(l_c u_n))} \\ &= \frac{P(X_i = 1, X_{i+1} = 0)}{P(X_i = 1)} = P(X_{i+1} = 0 \mid X_i = 1). \end{aligned} \tag{D.3}$$

Next we show $U_i \geq U_{i+1}$, assuming that, when there is no crosstalk attack in the network, amplifiers on each fiber operate in the gain clamped regions and make up the signal attenuation between the two nodes. From (3.5), we have

$$U_{i+1} = \tau_{i,i+1}(U_i) = l_{i+1,1}\pi_{i+1,1}(a_{i,i+1}\pi_{i,2}(l_{i,2}U_i)). \tag{D.4}$$

$$l_{i+1,1}a_{i,i+1}l_{i,2}d_{i,2}d_{i+1,1} = 1, \tag{D.5}$$

where $d_{i,2}$ denotes the clamped gain of EDFA at the output side of node V_i; $d_{i+1,1}$ denotes the clamped gain of EDFA at the input side of node V_{i+1}. Then,

If $l_{i,2}U_i \leq p_{th,(i,2)}$, $U_{i+1} = U_i$;

If $l_{i,2}U_i > p_{th,(i,2)}$, $\pi_{i,2}(l_{i,2}U_i) < d_{i,2}U_i$,

which corresponds to the case where the EDFA with subscript $(i,2)$ works at the saturation region. Therefore,

$$U_{i+1} < l_{i+1,1}d_{i+1,1}a_{i,i+1}d_{i,2}l_{i,2}U_i. \tag{D.6}$$

It follows that $U_{i+1} < U_i$.

To prove (3.9), it suffices to show that $\tau_{i,i+1}(U_i)$ monotonically increases in U_i, where

$$U_{i+1} = \tau_{i,i+1}(U_i) = l_{i+1,1}\pi_{i+1,1}(a_{i,i+1}\pi_{i,2}(l_{i,2}U_i)). \tag{D.7}$$

Since $l_{i+1,1}, a_{i,i+1},$ and $l_{i,2}$ are constants, to show that $\tau_{i,i+1}(U_i)$ monotonically increases in U_i, it suffices to show that $\pi_{ij}(P_{input})$ monotonically increase in P_{input}. This can be obtained by showing $\frac{\partial(P_{input}g(P_{input}))}{\partial P_{input}} > 0$ for (3.4). This means that: the higher the input power at EDFA, the higher the output power, when the EDFA worked at either the saturated or the non-saturated region.

APPENDIX E

PROOF OF PROPOSITION 3.1

Proof: From (3.17), assume $\gamma_{ij} \equiv \gamma$, then,

$$P(\mathbf{N}) = \frac{1}{Z_{\mathbf{N}}} \prod_{(V_i \sim V_j)} \gamma^{\sum_{r_{sd} \in \mathbf{R}_{ij}} N_{sd}} (1-\gamma)^{(1-\sum_{r_{sd} \in \mathbf{R}_{ij}} N_{sd})} I_1(\sum_{r_{sd} \in \mathbf{R}_{ij}} N_{sd}). \tag{E.1}$$

Let $W_{ij} = \sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}$ and $\mathbf{W} = (W_{ij} : V_i \sim V_j)$. $\mathbf{W}$ is a vector that represent the wavelength usage at each link in the network. We denote a configuration of $(\mathbf{N}, \mathbf{W})$ with non-zero probability as a traffic pattern, i.e., a traffic pattern $(\mathbf{N}, \mathbf{W})$ satisfies the capacity constraints and $P(\mathbf{N} = \mathbf{n}, \mathbf{W} = \mathbf{w}) > 0$. Let $\mathbf{T}_k, k = 0,1,...,|\mathbf{E}|,$ be the set of traffic patterns that k links in the network are used by active connections, with $|\mathbf{E}|$ being the number of links in $\mathbf{E}$. Let $|\mathbf{T}_k|$ denote the cardinality of $\mathbf{T}_k$, then,

$$\begin{aligned} \rho &= \boldsymbol{E}_{P(\mathbf{N})}[\sum_{V_i \sim V_j} \sum_{r_{sd} \in \mathbf{R}_{ij}} N_{sd} \Big/ |\mathbf{E}|] \\ &= \frac{\sum_{k=0}^{|\mathbf{E}|} k\gamma^k (1-\gamma)^{|\mathbf{E}|-k} |\mathbf{T}_k|}{|\mathbf{E}| \sum_{k=0}^{|\mathbf{E}|} \gamma^k (1-\gamma)^{|\mathbf{E}|-k} |\mathbf{T}_k|} \\ &= \frac{\sum_{k=1}^{|\mathbf{E}|} k\theta^k |\mathbf{T}_k|}{|\mathbf{E}| \sum_{k=0}^{|\mathbf{E}|} \theta^k |\mathbf{T}_k|} \overset{definition}{=} \xi(\theta), \end{aligned} \tag{E.2}$$

where $\theta = \gamma/(1-\gamma), \theta > 0.$

$$\begin{aligned} \frac{\partial(\xi(\theta))}{\partial\theta} = \frac{1}{|\mathbf{E}|(\sum_{k=0}^{|\mathbf{E}|} \theta^k |\mathbf{T}_k|)^2} \cdot \{&(\sum_{k=1}^{|\mathbf{E}|} k^2\theta^{k-1} |\mathbf{T}_k|)(\sum_{k=0}^{|\mathbf{E}|} \theta^k |\mathbf{T}_k|) \\ &- (\sum_{k=1}^{|\mathbf{E}|} k\theta^k |\mathbf{T}_k|)(\sum_{k=1}^{|\mathbf{E}|} k\theta^{k-1} |\mathbf{T}_k|)\}. \end{aligned} \tag{E.3}$$

Using Cauchy-Schwartz Inequality, it can be shown that

$$\partial(\xi(\theta))/\partial\theta > 0, \forall\ \theta > 0\,. \tag{E.4}$$

Since $\partial\theta/\partial\gamma > 0, \forall\ 0 < \gamma < 1,$ we have

$$\partial\rho/\partial\gamma > 0, \forall\ 0 < \gamma < 1. \tag{E.5}$$

Therefore, ρ increases monotonically in γ.

APPENDIX F

PROOF OF THEOREM 3.1

Proof: Consider a ring network $G(\mathbf{V},\mathbf{E})$ with m nodes $(m>1)$. The route set $\mathbf{R}$ consists of the two link-disjoint routes between each pair of nodes in the network. Suppose the crosstalk attack is started on flow f_{ij} between node V_i and V_j, $i,j=1,2,...,m,\ i<j.$ The set of nodes traversed by flow f_{ij} is $\mathbf{V}_{f_{ij}}=\{V_i,V_{i+1},...,V_j\}$. Then at most two nodes, node V_{i-1} and node V_{j+1}, are neighbors of nodes in $\mathbf{V}_{f_{ij}}$, but are not in $\mathbf{V}_{f_{ij}}$ themselves. Without loss of generality, we focus on the conditional wavelength usage at link between V_j and V_{j+1}.

To show that $M_{f_{ij}}$ monotonically increases in ρ for the ring network, from (3.25), it suffices to show that $E_{f_{ij}}[\sum_{r_{uv}\in\mathbf{R}_{j\,j+1}} N_{uv}]$ and $E_{f_{ij}}[\sum_{r_{jh}\in\mathbf{R}_{j\,j+1}} N_{jh}]$ monotonically increase with parameter γ in (E.1) for the ring network.

Let $W_{ij}=\sum_{r_{uv}\in\mathbf{R}_{ij}} N_{uv}$ and $H_{ij}=\sum_{r_{ih}\in\mathbf{R}_{ij}} N_{ih}$. Then for the ring network, denote $E_{f_{ij}}[\sum_{r_{uv}\in\mathbf{R}_{j\,j+1}} N_{uv}]$ as $w_{j\,j+1}(m,f_{ij},ring)$; denote $E_{f_{ij}}[\sum_{r_{jh}\in\mathbf{R}_{j\,j+1}} N_{jh}]$ as $\varpi_{j\,j+1}(m,f_{ij},ring)$, where m is the number of nodes in the ring network.

Let $w_{12}(l,bus)$ denote the mean value of W_{12} in an l-node network of bus topology with a route set that includes the route between each pair of nodes, where subscript l denotes the number of nodes in the bus network. Since,

$$w_{j\,j+1}(m,f_{ij},ring)=\varpi_{j\,j+1}(m,f_{ij},ring)=w_{12}(m-j+i,bus), \tag{F.1}$$

it is sufficient to show that $w_{12}(l, bus), \forall\, l > 1,$ increases monotonically with γ.

As in *Appendix E*, let $\theta = \gamma/(1-\gamma)$ and $\mathbf{W} = (W_{ij} : V_i \sim V_j)$. In addition, a configuration of $(\mathbf{N}, \mathbf{W})$ with non-zero probability is denoted as a traffic pattern. Let $sum(\mathbf{W})$ denote the summation of all the components in $\mathbf{W}$, then from (E.1),

$$P(\mathbf{N}, \mathbf{W}) \propto \theta^{sum(\mathbf{W})} \prod_{V_i \sim V_j} I_2(W_{ij} = \sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}), \tag{F.2}$$

where $I_2(A) = 1$ if A is true; and $I_2(A) = 0$, otherwise. If $(\mathbf{N}, \mathbf{W})$ is a traffic pattern, (F.2) can be simplified as $P(\mathbf{N}, \mathbf{W}) \propto \theta^{sum(\mathbf{W})}$.

Let $\mathbf{T}_{(l),bus}$ denote the set of all traffic patterns on the bus network with l nodes ($l > 1$). By counting all possible ways of using link A_1A_2, we have for the l-node bus network,

$$P(W_{12} = 1) \propto \theta \sum_{\mathbf{T}_{(l-1),bus}} \theta^{sum(\mathbf{W}_{(l-1),bus})} + \theta^2 \sum_{\mathbf{T}_{(l-2),bus}} \theta^{sum(\mathbf{W}_{(l-2),bus})} + ... + \theta^l. \tag{F.3}$$

$$P(W_{12} = 0) \propto \sum_{\mathbf{T}_{(l-1),bus}} \theta^{sum(\mathbf{W}_{(k-1),bus})}. \tag{F.4}$$

Let $f_l(\theta) = \sum_{\mathbf{T}_{(l),bus}} \theta^{sum(\mathbf{W}_{(l),bus})}$, $\forall l > 1$, and $f_1(\theta) = 1$. We have,

$$P(W_{12} = 1) \propto \theta f_{l-1}(\theta) + \theta^2 f_{l-2}(\theta) + ... + \theta^l.$$

$$P(W_{12} = 0) \propto f_{l-1}(\theta).$$

Furthermore, we have the following recursive equations,

$$f_1(\theta) = 1;$$

$$f_2(\theta) = 1 + \theta;$$

$$f_i(\theta) = (1 + 2\theta) f_{i-1}(\theta) - \theta f_{i-2}(\theta), \;\; i = 3, 4, ..., l. \tag{F.5}$$

Then,

$$w_{12}(l,bus)=\begin{cases}\dfrac{\theta}{1+\theta}, & if\ l=2,\\ 1-\dfrac{f_{l-1}(\theta)}{(1+2\theta)f_{l-1}(\theta)-\theta f_{l-2}(\theta)}, & if\ l>2.\end{cases} \tag{F.6}$$

Obviously, $\dfrac{\partial w_{12}(l,bus)}{\partial\theta}>0,$ for $l=2$.

If $l>2,$

$$\frac{\partial w_{12}(l,bus)}{\partial\theta}=\frac{2f_{l-1}^{'}(\theta)+\theta(f_{l-1}^{'}f_{l-2}-f_{l-1}f_{l-2}^{'})}{((1+2\theta)f_{l-1}(\theta)-\theta f_{l-2}(\theta))^{2}}. \tag{F.7}$$

From (F.5),

$$f_l^{'}f_{l-1}-f_lf_{l-1}^{'}=2f_{l-1}^{2}-f_{l-1}f_{l-2}+\theta(f_{l-1}^{'}f_{l-2}-f_{l-1}f_{l-2}^{'}). \tag{F.8}$$

Since $f_2^{'}f_1-f_2f_1^{'}=2\theta^2+4\theta+1>0$, through Mathematical induction, from (F.8), we have $f_l^{'}f_{l-1}-f_lf_{l-1}^{'}>0,\ \forall l>1,$ and $\dfrac{\partial w_{12}(l,bus)}{\partial\theta}>0,\ \forall\ l>1$.

Since $\theta=\gamma/(1-\gamma),$ and $0<\theta<1$, it follows that

$$\frac{\partial w_{12}(l,bus)}{\partial\gamma}>0,\ \forall l>1. \tag{F.9}$$

From Proposition 3.1, $M_{f_{ij}}$ monotonically increases in ρ for the ring network.

The upper and lower bound of $M_{f_{sd}}$ in (3.26) is obtained by showing that

$$\gamma\le w_{j\,j+1}(m,f_{ij},ring)\le\rho. \tag{F.10}$$

Here we first show that for arbitrary network topologies $\mathbf{G}(\mathbf{V},\mathbf{E})$, if $r_{ij}\in\mathbf{R}$, i.e., there is one route from node V_i to V_j in $\mathbf{R}$, where $V_i\in\mathbf{V}_{f_{sd}}$, $V_j\notin\mathbf{V}_{f_{sd}}$, and $V_i\sim V_j$, then,

$$E_{f_{sd}}[W_{ij}]\ge\gamma, \tag{F.11}$$

Obviously, the ring network considered here satisfies the condition in (F.11).

Let $\mathbf{E}_1 = \{e_{ij} : V_i \sim V_j, r_{sd} \notin \mathbf{R}_{ij}\}$. $\mathbf{E}_1$ denotes the set of links that are not traversed by flow f_{sd}: . Let $\mathbf{R}_1$ be the set of routes in $\mathbf{R}$ that only traverse links in $\mathbf{E}_1$. Let $\mathbf{E}_2 = \mathbf{E}_1 \setminus \{e_{ij}\}$, and $\mathbf{R}_2$ be the set of routes in $\mathbf{R}$ that only traverse links in $\mathbf{E}_2$. Clearly, $\mathbf{R}_2 \subset \mathbf{R}_1 \subset \mathbf{R}$, if $r_{ij} \in \mathbf{R}$. Let $\mathbf{T}_{\mathbf{E}_1} = \{(\mathbf{N}_{\mathbf{E}_1}, \mathbf{W}_{\mathbf{E}_1})\}$ be the set of traffic patterns restricted to a network formed by link set $\mathbf{E}_1$ with route set $\mathbf{R}_1$. Let $\mathbf{T}_{\mathbf{E}_2} = \{(\mathbf{N}_{\mathbf{E}_2}, \mathbf{W}_{\mathbf{E}_2})\}$ be the set of traffic patterns restricted to a network formed by link set $\mathbf{E}_2$ with route set $\mathbf{R}_2$. Then,

$$E_{f_{sd}}[W_{ij}] = \frac{\theta Z_1(\theta) + Z_2(\theta)}{(1+\theta)Z_1(\theta) + Z_2(\theta)}, \tag{F.12}$$

where

$Z_1(\theta) = \sum_{\mathbf{T}_{\mathbf{E}_2}} \theta^{sum(\mathbf{W}_{\mathbf{E}_2})}$ and $Z_2(\theta) = \sum_{\mathbf{T}_{\mathbf{E}_1}} \theta^{sum(\mathbf{W}_{\mathbf{E}_1})} - (1+\theta)Z_1(\theta)$.

In addition, $Z_2(\theta) > 0$ if there is a route that traverses link ij and one or more links in set $\mathbf{E}_2$; $Z_2(\theta) = 0$, otherwise. Since $Z_1(\theta) > 0,$ we have

$$E_{f_{sd}}[W_{ij}] \geq \frac{\theta}{1+\theta} = \gamma\,. \tag{F.13}$$

To show that $w_{j\,j+1}(m, f_{ij}, ring) \leq \rho$, from (F.1), it suffices to show that

$$w_{12}(m - j + 1, bus) \leq \rho\,, \tag{F.14}$$

which can be proved through the following two lemmas.

Lemma 3.1 $w_{12}(l, bus) \leq w_{12}(l+1, bus),\ \forall\, l > 1.$

Lemma 3.2 $w_{12}(m, bus) \leq \rho, \forall m > 1.$

Lemma 3.1 and 3.2 are proved using induction similarly as in the proof of (F.9). Detailed proof is omitted here. Using (F.10), we can obtain (3.26) from (3.25).

APPENDIX G

PROOF OF THEOREM 3.2

Proof: For a network of star topology with m nodes, $m > 2$, and a route set $\mathbf{R}$ that consists of the routes between each pair of nodes. Let node V_m be the hub node of the star network. Let $W_{ij} = \sum_{r_{uv} \in \mathbf{R}_{ij}} N_{uv}$ and $H_{ij} = \sum_{r_{ih} \in \mathbf{R}_{ij}} N_{ih}$. We first show that, when the attack is started on flow f_{1m}, $w_{mi}(m, f_{1m}, star) + \varpi_{mi}(m, f_{1m}, star)$, $i = 2, ..., m-1$, increases monotonically with γ, where

$$w_{mi}(m, f_{1m}, star) = E_{f_{1m}}[\sum_{r_{uv} \in \mathbf{R}_{mi}} N_{uv}],$$

and

$$\varpi_{mi}(m, f_{1m}, star) = E_{f_{1m}}[\sum_{r_{mh} \in \mathbf{R}_{mi}} N_{mh}].$$

Let $\mathbf{T}_{(l),star}$ denote the set of all traffic patterns on the star network with l nodes. By counting all possible ways of using link mi, it can be found that, for the l-node star network,

$$P(W_{mi} = 1 \mid R_f = f_{1m}) \propto \theta \sum_{\mathbf{T}_{(m-1),star}} \theta^{sum(\mathbf{W}_{(m-1),star})} + (m-2)\theta^2 \sum_{\mathbf{T}_{(m-2),star}} \theta^{sum(\mathbf{W}_{(m-2),star})}; \quad \text{(G.1)}$$

$$P(W_{mi} = 0 \mid R_f = f_{1m}) \propto \sum_{\mathbf{T}_{(m-1),star}} \theta^{sum(\mathbf{W}_{(m-1),star})}; \quad \text{(G.2)}$$

$$P(H_{mi} = 1 \mid R_f = f_{1m}) \propto \theta \sum_{\mathbf{T}_{(m-1),star}} \theta^{sum(\mathbf{W}_{(m-1),star})}; \quad \text{(G.3)}$$

$$P(H_{mi} = 0 \mid R_f = f_{1m}) \propto \sum_{\mathbf{T}_{(m-1),star}} \theta^{sum(\mathbf{W}_{(m-1),star})} + (m-2)\theta^2 \sum_{\mathbf{T}_{(m-2),star}} \theta^{sum(\mathbf{W}_{(m-2),star})}. \quad \text{(G.4)}$$

Let $t_1 = 1$ and $t_l(\theta) = \sum_{\mathbf{T}_{(l),star}} \theta^{sum(\mathbf{W}_{(l),star})}$, $l > 1$. Then, we have the following recursive equations,

$t_2 = 1 + \theta$;

$t_l = (1+\theta)t_{l-1} + (l-2)\theta^2 t_{k-2}$, $\forall\, l > 2$.

Therefore, from (G.1)- (G.4),

$$w_{mi}(m, f_{1m}, star) + \varpi_{mi}(m, f_{1m}, star) = 1 + \frac{(\theta - 1)t_{m-1}}{(1+\theta)t_{m-1} + (m-2)\theta^2 t_{m-2}}. \tag{G.5}$$

Through induction similarly as in the proof of (F.9), we have $\frac{\partial\{\, w_{mi}(m, f_{1m}, star) + \varpi_{mi}(m, f_{1m}, star)\}}{\partial \gamma} > 0$.

Similarly, when the attack is started from flow $f_{A_1A_2}$, it can be shown that $\frac{\partial\{w_{mi}(m, f_{12}, star) + \varpi_{mi}(m, f_{12}, star)\}}{\partial \gamma} > 0$.

Thus, from (3.25), it follows that $M_{f_{ij}}$ monotonically increases in ρ for the star network.

The upper and lower bound of $M_{f_{sd}}$ in (3.28) and (3.29) is obtained by showing that

$$\gamma < w_{mi}(m, f_{1m}, star) + \varpi_{mi}(m, f_{1m}, star) \le 2\rho\,, \tag{G.6}$$

and

$$\gamma < w_{mi}(m, f_{12}, star) + \varpi_{mi}(m, f_{12}, star) \le 2\rho. \tag{G.7}$$

Since

$$\varpi_{mi}(m, f_{1m}, star) \le w_{mi}(m, f_{1m}, star)\,, \tag{G.8}$$

and

$$\varpi_{mi}(m, f_{12}, star) \le w_{mi}(m, f_{12}, star), \tag{G.9}$$

(G.6) and (G.7) can be obtained by showing

$$\gamma \le w_{mi}(m, f_{1m}, star) \le \rho\,, \tag{G.10}$$

$$\gamma \le w_{mi}(m, f_{12}, star) \le \rho\,. \tag{G.11}$$

The proof of (G.11) is similar to that of (F.10), and is omitted.

APPENDIX H

PROOF OF THEOREM 3.3 AND 3.4

H. 1 Proof of Theorem 3.3

We first derive $a_i = P(N_{1\,i+1} = 1)$. Through solving the difference equation in (F.5), it can be found that

$$f_m = \frac{\sqrt{1+4\theta^2}+1}{2\sqrt{1+4\theta^2}}\left(\frac{1+2\theta+\sqrt{1+4\theta^2}}{2}\right)^{m-1} + \frac{\sqrt{1+4\theta^2}-1}{2\sqrt{1+4\theta^2}}\left(\frac{1+2\theta-\sqrt{1+4\theta^2}}{2}\right)^{m-1}. \quad \text{(H.1)}$$

Let $\mathbf{T}_{(l),ring}$ be the set of all traffic patterns on a ring network with l nodes and a route set that includes all possible link-disjoint shortest paths between each pair of nodes in the network. Let $g_m = \sum_{\mathbf{T}_{(m),ring}} \theta^{sum(\mathbf{W}_{(m),ring})}$ By counting different ways of using one single link in the ring network, we have

$$g_k = f_k + \theta f_k + 2\theta^2 f_{k-1} + \ldots + (k-1)\theta^{k-1} f_2. \quad \text{(H.2)}$$

Therefore, $a_i = P(N_{A_1A_{i+1}} = 1) = \theta^i f_{k-i+1} / g_k$.

Using the lower and upper bound of $M_{f_{sd}}$ for the ring network in (3.26), we obtain Theorem 3.3.

H.2 Proof of Theorem 3.4

From (G.1)-(G.4), we have

$$P(N_{1\,m} = 1) = \theta t_{k-1} / t_k;\ P(N_{A_1A_2} = 1) = \theta^2 t_{m-2} / t_m;\ \forall k > 3. \quad \text{(H.3)}$$

Using the lower and upper bound of $M_{f_{sd}}$ for the star network in (3.28) and (3.29). We can obtain Theorem 3.4.

APPENDIX I

PROOF OF THEOREM 3.5

Proof: From (3.2),

$$M = \sum_{f_{sd}} M_{f_{sd}} \, P(N_{sd} = 1) \Big/ 2 \,|\, \mathbf{R} \,|$$

$$\begin{aligned} &\leq \frac{\sum_{f_{sd}} P(N_{sd} = 1)}{2 \,|\, \mathbf{R} \,|} \max_{f_{sd}} \{M_{f_{sd}}\} \\ &= \frac{\boldsymbol{E}[sum(\mathbf{N})]}{|\, \mathbf{R} \,|} \max_{f_{sd}} \{M_{f_{sd}}\}, \end{aligned} \tag{I.1}$$

where $\mathbf{N} = (N_{sd} : r_{sd} \in \mathbf{R})$, and $\boldsymbol{E}[\,]$ stands for expectation.

$$\boldsymbol{E}[sum(\mathbf{N})] = \sum_{\mathbf{W}} \boldsymbol{E}[sum(\mathbf{N}) \,|\, \mathbf{W}] P(\mathbf{W}),$$

where $\mathbf{W} = (W_{ij}, i \sim j)$.

Since $\boldsymbol{E}[sum(\mathbf{N}) \,|\, \mathbf{W}] \leq \boldsymbol{E}[sum(\mathbf{W}) \,|\, \mathbf{W}]$,

$$\boldsymbol{E}(sum(\mathbf{N})) \leq \sum_{\mathbf{W}} \boldsymbol{E}(sum(\mathbf{W}) \,|\, \mathbf{W}) P(\mathbf{W}) = \boldsymbol{E}(sum(\mathbf{W})). \tag{I.2}$$

Since $\boldsymbol{E}[sum(\mathbf{W})] = \rho \,|\, \mathbf{E} \,|$, from (I.2), it follows that

$$\boldsymbol{E}(sum(\mathbf{N})) \leq \rho \,|\, \mathbf{E} \,| \tag{I.3}$$

and

$$M \leq \frac{1}{|\, \mathbf{R} \,|} \max_{f_{sd}} \{M_{f_{sd}}\} \rho \,|\, \mathbf{E} \,|. \tag{I.4}$$

APPENDIX J

PROOF OF THEOREM 4.3

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 J*. The proof of Theorem 4.3 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.

$$P(S_{mn}=0)=\sum_{X_1,...,X_j,Y_0,...,Y_j} P(S_{mn}=0\mid X_1,...,X_j,Y_0,...,Y_j)P(X_1,...,X_j,Y_0,...,Y_j)\,. \tag{J.1}$$

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

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

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

$$P(X_1,X_2,...,X_j,Y_0,Y_1...,Y_j)=\prod_{i=1}^{j}P(X_i)\prod_{l=0}^{j}P(Y_l)\,. \tag{J.3}$$

Thus, from (J.2) and (J.3),

$$\begin{aligned}&P(S_{mn}=0)\\&=\prod_{i=1}^{j}\{\sum_{X_i}(1-p_a)^{X_i}P(X_i)\}\prod_{l=1}^{j-1}\{\sum_{Y_l}(1-p_b)^{2Y_l}P(Y_l)\}\sum_{Y_0}(1-P_b)^{Y_0}P(Y_0)\sum_{Y_j}(1-P_b)^{Yj}P(Y_j).\end{aligned} \tag{J.4}$$

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 (J.4),

$$P(S_{mn}=0)=(1-ap_a)^j(1-bP_b)^2(1-b(2p_b-P_b^2))^{j-1}. \tag{J.5}$$

Since $P(Z_i=0)=(1-aP_a)(1-bP_b)^2$, it follows that

$$\frac{1-\prod_{l=1}^{j}P(Z_j=0)}{1-P(Z_1=0,Z_2=0,...,Z_j=0)}=\frac{1-(1-ap_a)^j(1-2bp_b+b^2p_b^2)^j}{1-(1-ap_a)^j(1-2bp_b+b^2p_b^2)(1-2bp_b+bp_b^2)^{j-1}}-1.$$

APPENDIX K

PROOF OF THEOREM 4.4

Proof: We let the number of links on the primary route and the backup route between node m and n be j_1 and j_2 respectively. Without loss of generally we assume that $j_1 \le j_2$. The proof of Theorem 4.4 is obtained by considering all possible combination of events that the connection on mn are not lost due to failures. Specifically, we denote the following binary random variables

(1) E_{11}: $E_{11} = 1$ if there is a failure on the first link of the primary route; $E_{11} = 0$ otherwise.

(2) E_{12}: $E_{12} = 1$ if there is a failure on the first link of the backup route; $E_{12} = 0$ otherwise.

(3) E_{21}: $E_{21} = 1$ if there is a failure on the last link of the primary route; $E_{21} = 0$ otherwise.

(4) E_{22}: $E_{22} = 1$ if there is a failure on the last link of the backup route; $E_{22} = 0$ otherwise.

(5) E_1: $E_1 = 1$ if there is one or more failures on one or more links of the primary route that are neither the first link nor the last link; $E_1 = 0$ otherwise.

(6) E_2: $E_2 = 1$ if there is one or more failures on one or more links of the backup route that are neither the first link nor the last link; $E_2 = 0$ otherwise.

Therefore, let $\sigma = b(2p_b - p_b^2)$, then,

(1) If $j_1 = 1$ and $j_2 = 2$, the connection is not lost due to failures upon the following events:

(i) $P(E_{11}=0)=(1-ap_a)(1-bp_b)^2$.

(ii) $P(E_{11}=1,E_{12}=0,E_{22}=0)=(1-\sigma)(1-ap_a)^2\{(1-bp_b)^2-(1-ap_a)(1-\sigma)^2\}$.

Thus,

$P(S_{mn}=0)=P(E_{11}=0)+P(E_{11}=1,E_{12}=0,E_{22}=0)$.

In particular,

$P(S_{mn}=0)=(1-ap_a)(1-b)^2(1+(1-ap_a)(1-b)ap_a)$ if $p_b=1$. (K.1)

In addition, if $a^2 \ll 1$ and $b \ll 1$,

$P(S_{mn}=0)=1-abp_a-2b-2a^2p_a^2$. (K.2)

(2) If $j_1=1$ and $j_2>2$, we need to consider E_{11},E_{12},E_{22},E_2.

(i) $P(E_{11}=0)=(1-ap_a)(1-bp_b)^2$.

(ii) $P(E_{11}=1,E_{12}=0,E_2=0,E_{22}=0)$
$=(1-ap_a)^{j_2}(1-\sigma)^{j_2-1}\{(1-bp_b)^2-(1-ap_a)(1-\sigma)^2\}$.

Thus,

$P(S_{mn}=0)=P(E_{11}=0)+P(E_{11}=1,E_{12}=0,E_{22}=0)$.

In particular,

$P(S_{mn}=0)=(1-ap_a)(1-b)^2(1+(1-ap_a)^{j_2-1}(1-b)^{j_2-1}ap_a)$ if $p_b=1$. (K.3)

In addition, if $a^2 \ll 1$ and $b \ll 1$,

$P(S_{mn}=0)=1-2b-(j_2-1)abp_a-j_2a^2p_a^2$. (K.4)

(3) If $j_1=2$ and $j_2=2$, we need to consider $E_{11},E_{12},E_{21,}E_{22}$.

(i) $P(E_{11}=0,E_{21}=0)=(1-ap_a)^2(1-bp_b)^2(1-\sigma)$.

(ii) $P(E_{11}=0,E_{21}=1,E_{12}=0,E_{22}=0)=(1-ap_a)^3(1-\sigma)^2\{(1-bp_b)^2-(1-ap_a)(1-\sigma)^2\}$.

(iii) $P(E_{11}=1,E_{21}=0,E_{12}=0,E_{22}=0)$
$=(1-ap_a)^3(1-\sigma)^2\{(1-bp_b)^2-(1-ap_a)(1-\sigma)^2\}$.

(iv) $P(E_{11}=1,E_{21}=1,E_{12}=0,E_{22}=0)=(1-ap_a)^2(1-\sigma)$
$\times\{b[(1-bp_b)-(1-\sigma)(1-p_b)(1-ap_a)]^2=(1-b)[(1-bp_b)-(1-\sigma)(1-ap_a)]^2\}$.

In particular,

$$P(S_{mn}=0)=(1-ap_a)^2(1-b)^3(1+2(1-ap_a)(1-b)ap_a+b+a^2p_a^2(1-b)) \text{ if } p_b=1. \quad \text{(K.5)}$$

In addition, if $a^2 \ll 1$ and $b \ll 1$,

$$P(S_{mn}=0)=1-2b-4abp_a-4a^2p_a^2. \quad \text{(K.6)}$$

(4) If $j_1=2$ and $j_2>2$, we need to consider $E_{11},E_{12},E_{21,}E_{22},E_2$,

(i) $P(E_{11}=0,E_{21}=0)=(1-ap_a)^2(1-bp_b)^2(1-\sigma)$.

(ii) $P(E_{11}=0,E_{21}=1,E_{12}=0,E_{22}=0,E_2=0)$
$=(1-ap_a)^{j_2+1}(1-\sigma)^{j_2}\{(1-bp_b)^2-(1-ap_a)(1-\sigma)^2\}$.

(iii) $P(E_{11}=1,E_{21}=0,E_{12}=0,E_{22}=0,E_2=0)$
$=(1-ap_a)^{j_2+1}(1-\sigma)^{j_2}\{(1-bp_b)^2-(1-ap_a)(1-\sigma)^2\}$.

(iv) $P(E_{11}=1,E_{21}=1,E_{12}=0,E_{22}=0,E_2=0)$
$=(1-ap_a)^{j_2}(1-\sigma)^{j_2-1}\{b[(1-bp_b)-(1-\sigma)(1-p_b)(1-ap_a)]^2$
$+(1-b)[(1-bp_b)-(1-\sigma)(1-ap_a)]^2\}$.

In particular,

$$P(S_{mn}=0)=(1-ap_a)^{j_2}(1-b)^{j_2+1}(1+2(1-ap_a)(1-b)ap_a+b+a^2p_a^2(1-b)) \text{ . if } p_b=1. \quad \text{(K.7)}$$

In addition, if $a^2 \ll 1$ and $b \ll 1$,

$$P(S_{mn}=0)=1-2b-(3j_2-2)abp_a-2j_2a^2p_a^2. \quad \text{(K.8)}$$

(5) If $j_1>2, j_2>2$,

(i) $P(E_{11}=0, E_{12}=1, E_1=0, E_{21}=0)$
$= (1-ap_a)^{j_2}(1-\sigma)^{j_2-1}(1-bp_b)^2(1-(1-ap_a)(1-\sigma)).$ (K.9)

(ii) $P(E_{11}=1, E_{12}=0, E_2=0, E_{22}=0)$
$= (1-ap_a)^{j_1}(1-\sigma)^{j_1-1}(1-bp_b)^2(1-(1-ap_a)(1-\sigma)).$ (K.10)

(iii) $P(E_{11}=0, E_{12}=0, E_1=0, E_{21}=0, E_{22}=1)$
$= (1-ap_a)^{j_1+1}(1-b(2p-p_b^2))^{j_1}(1-bp_b)^2(1-(1-ap_a)(1-b(2p-p_b^2))).$ (K.11)

(iv) $P(E_{11}=0, E_{12}=0, E_2=0, E_{21}=1, E_{22}=0)$
$= (1-ap_a)^{j_2+1}(1-b(2p-p_b^2))^{j_2}(1-bp_b)^2(1-(1-ap_a)(1-b(2p-p_b^2))).$ (K.12)

(v) $P(E_{11}=0, E_{12}=0, E_1E_2=0, E_{21}=0, E_{22}=0)$
$= (1-bp_b)^2\{(1-ap_a)^{j_1+2}(1-b(2p_b-p_b^2))^{j_1+1} + (1-ap_a)^{j_2+2}(1-b(2p_b-p_b^2))^{j_2+1}\}$
$-(1-ap_a)^{j_1+j_2}(1-b(2p-p_b^2))^{j_1+j_2}$.

(K.13)

Add up (K.9) to (K.13), we can obtain $P(S_{mn}=0)$. In addition, if $p_b=1, a^2 \ll 1$ and $b \ll 1$,

$$P(S_{mn}=0) = 1-2b-(2j_1j_2-j_1-j_2)abp_a - j_1j_2a^2p_a^2. \quad \text{(K.14)}$$

Thus, combining (K.2), (K.4), (K.6), (K.8), and (K.14), we have

$P(S_{mn}=0) = 1-2b-(2j_1j_2-j_1-j_2)abp_a - j_1j_2a^2p_a^2$, for $j_1 \geq 1, j_2 > j_1$,

if $p_b=1, a^2 \ll 1$ and $b \ll 1$.

APPENDIX L

PROOF OF THEOREM 4.5

Proof:

$B_{ring} = Erlang(\rho_{ring}, C) = \frac{\rho_{ring}^{C}}{C!}(\sum_{i=0}^{C}\frac{\rho_{ring}^{i}}{i!})$. From [81],

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

Thus,

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

Therefore,

$B_{ring} = 1 - \frac{C-1}{v+1}$, as $v \to \infty$.

$\mathbb{Z}_{ring} = k(C-1)p + o(\frac{C^2 p}{v})$, as $v \to \infty$.

$\mathbb{k}_{ring} = p$, as $v \to \infty$.

APPENDIX M

PROOF OF THEOREM 4.8

Proof: We show that $\frac{\partial B}{\partial v} > 0$ for the ring networks with an odd number of nodes. The proof of $\frac{\partial B}{\partial v} > 0$ for ring networks with an even number of nodes, star, mesh-torus networks can be obtained using a similar approach. The main idea of the proof is based on taking derivatives of the implicit function *B*.

$$B_{ring} = Erlang(\rho_{ring}, C) = \frac{\rho_{ring}^{C}}{C!}(\sum_{i=0}^{C}\frac{\rho_{ring}^{i}}{i!}) \ , \tag{M.1}$$

and

$$\rho_{ring} = \sum_{j=1}^{\frac{k-1}{2}}\{jv(1-B_{ring})^{(j-1)}\} . \tag{M.2}$$

Thus,

$$\frac{\partial B_{ring}}{\partial v} = \frac{\partial Erlang(\rho_{ring}, C)}{\partial \rho_{ring}}\frac{\partial \rho_{ring}}{\partial v} .$$

From [79],

$$\frac{\partial Erlang(\rho_{ring}, C)}{\partial \rho_{ring}} = B_{ring}(\frac{C}{\rho_{ring}} - 1 + B_{ring}). \tag{M.3}$$

Therefore,

$$\frac{\partial B_{ring}}{\partial v} = B_{ring}(\frac{C}{\rho_{ring}} - 1 + B_{ring})\frac{\partial \rho_{ring}}{\partial v} .$$

$$\frac{\partial B_{ring}}{\partial v} = B_{ring}(\frac{C}{\rho_{ring}} - 1 + B_{ring})\{\sum_{j=1}^{\frac{k-1}{2}} j(1-B_{ring})^{j-1} - \sum_{j=2}^{\frac{k-1}{2}} j(j-1)v(1-B_{ring})^{j-2}\frac{\partial B_{ring}}{\partial v}\} . \tag{M.4}$$

It follows that,

$$\frac{\partial B_{ring}}{\partial v} = B_{ring}\left(\frac{C}{\rho_{ring}} - 1 + B_{ring}\right)\frac{\sum_{j=1}^{\frac{k-1}{2}} j(1-B_{ring})^{j-1}}{1 + B_{ring}\left(\frac{C}{\rho_{ring}} - 1 + B_{ring}\right)\sum_{j=2}^{\frac{k-1}{2}} j(j-1)v(1-B_{ring})^{j-2}} > 0 .$$

APPENDIX N

PROOF OF THEOREM 4.9

Proof: We show that $\frac{\partial \mathbb{k}}{\partial v} > 0$ for the ring networks with an odd number of nodes. The proof of $\frac{\partial \mathbb{k}}{\partial v} > 0$ for ring networks with an even number of nodes, star, mesh-torus networks can be obtained in a similar way. The main idea of the proof is based on mathematical induction.

Since $\partial \mathbb{k}_{ring} = 1 - \frac{\sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l (1-p)^l}{\sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l}$, we have

$$\frac{\partial \mathbb{k}_{ring}}{\partial v} = \frac{\sum_{l=1}^{\frac{k-1}{2}} l(1-B_{ring})^{l-1}(1-p)^l \sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l - \sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l (1-p)^l \sum_{l=1}^{\frac{k-1}{2}} l(1-B_{ring})^{l-1}}{(\sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l)^2} \frac{\partial B_{ring}}{\partial v}. \tag{N.1}$$

Denote $\sum_{l=1}^{\frac{k-1}{2}} l(1-B_{ring})^{l-1}(1-p)^l \sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l - \sum_{l=1}^{\frac{k-1}{2}} (1-B_{ring})^l (1-p)^l \sum_{l=1}^{\frac{k-1}{2}} l(1-B_{ring})^{l-1} = \Theta(k)$.

Next we show that $\Theta(k) \le 0$ for $k \ge 3$. k odd.

If $k = 3, \Theta(k) = 0;$ if $k = 5, \Theta(k) < 0$. Furthermore,

$$\Theta(k+2) - \Theta(k) = (1-B_{ring})^{\frac{k+1}{2}} \{\sum_{l=1}^{\frac{k-1}{2}} (\frac{k+1}{2} - l)(1-B_{ring})^l \sum_{l=1}^{\frac{k-1}{2}} [(1-p)^{\frac{k+1}{2}} - (1-p)l]\} < 0 .$$

Thus, $\frac{\partial \mathbb{k}_{ring}}{\partial v} \le 0.$

REFERENCES

[1] "Report of the National Science Foundation Workshop on Network Research Testbeds," organizers, V. W. S. Chan and A. Mankin, Nov. 2002.

[2] V. W. S. Chan, "Guest editorial: optical communications and networking series," IEEE Journal on Selected Areas in Communications, Vol. 23, No. 8, pp. 1441-1443, Aug. 2005.

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

[4] A. Jukan and H. R. As, "Service-specific resource allocation in WDM networks with quality constraints," IEEE Journal on Selected Areas in Communications, vol. 18, pp. 2051-2061, Oct. 2000.

[5] P. Green, "Progress in optical networking," IEEE Communications Magazine, vol. 39, pp. 54-61, Jan. 2001.

[6] R. Ramaswarmi and K. Sivarajan, Optical Networks, A practical Perspective, The Morgan Kaufman Publishers, San Fransico, 1998.

[7] Y. Xue, M. Lazer, A. Nagarajan, O. Aparicio and S. Wright, "Carrier optical services requirements," IETF Draft, Mar. 2002.

[8] D. Mitra, Bell Laboratories, Lucent Technologies, Murray Hill, NJ, private communication between Dr. C. Ji and Dr. D. Mitra.

[9] R. A. Barry and P. A. Humblet, "Models of blocking probability in all-optical networks with and without wavelength changers," IEEE Journal on Selected Areas in Communications, vol. 14, pp. 858-867, June 1996.

[10] Y. Zhu, G. N. Rouskas and H. G. Perros, "A path decomposition approach for computing blocking probabilities in wavelength routing networks," IEEE/ACM Transactions on Networking, vol. 8, pp. 747-762, Dec. 2000.

[11] S. Subramaniam, M. Azizoglu and A. K. Somani, "All-optical networks with sparse wavelength conversion," IEEE/ACM Transactions on Networking, vol. 4, pp. 544-557, Aug. 1996.

[12] R. Ramaswami and A. Segall, "Distributed network control for wavelength routed optical network," IEEE/ACM Transactions on Networking, vol. 5, no. 6, pp. 936-943, Dec. 1997.

[13] D. Awduche and Y. Rekhter, "Multiprotocol lambda switching: combining MPLS traffic engineering control with optical crossconnects," IEEE Communications Magazine, vol. 39, pp. 111-116, Mar. 2001.

[14] N. Chandhok, A. Durresi, R. Jagannathan, R. Jain and K. Vinodkrishnan, "IP over optical networks: a summary of issues," IETF Draft, Mar. 2001.

[15] M. Kodialam and T. V. Lakshman, "Dynamic routing of locally restorable bandwidth guaranteed tunnels using aggregated link usage information," Proc. of IEEE Infocom 2001, pp. 902-911, Apr. 2001.

[16] C. Qiao and D. Xu, "Distributed partial information management (DPIM) schemes for survivable networks – Part I," Proc. of IEEE Infocom 2002, June, 2002.

[17] H. Wang, E. Modiano and M. Medard, "Partial path protection for WDM networks: end-to-end recovery using local failure information," Proc. of IEEE ISCC, July 2002.

[18] L. Li and A. K. Somani, "Dynamic wavelength routing using congestion and neighborhood information," IEEE/ACM Transactions on Networking, Vol. 7, pp. 779-786, Oct. 1999.

[19] S. Tomic, B. Statovci-Halimi, and A Halimi, "ASON and GMPLS-Overview and Comparison," Photonic Network Communications, 7:2, pp. 111-130, 2004.

[20] A. Elwalid, C. Jin, S. Low and I. Widjaja, "MATE: MPLS adaptive traffic engineering,'' Proc. of IEEE Infocom 2001, Apr. 2000.

[21] J. Yates, "Wavelength converters in dynamically-reconfigurable WDM networks,'' IEEE Communications Surveys, Second Quarter 1999.

[22] S. Subramaniam, M. Azizoglu and A.K. Somani, "On optimal converter placement in wavelength-routed networks,'' IEEE/ACM Transactions on Networking, vol. 7, pp. 754-766, Oct. 1999.

[23] R. Guerin and A. Orda, "QoS routing in networks with inaccurate information: theory and algorithms,'' IEEE/ACM Transactions on Networking, vol. 7, pp. 350-364, June 1999.

[24] K.S. Lui and K. Nahrstedt, "Topology aggregation and routing in bandwidth-delay sensitive network," Proc. of IEEE Globecom 2000, San Fransicisco, CA, Nov.-Dec., 2000.

[25] F. Hao and E. Zegura, "On scalable QoS routing: performance evaluation of topology aggregation," Proc. of IEEE Infocom 2000, Tel Aviv, Israel, Mar. 2000.

[26] S. Nelakuditi, Z.L. Zhang and R. P. Tsang, "Adaptive proportional routing: a localized QoS routing approach," IEEE/ACM Transactions on Networking, vol. 10, pp. 790-804, Dec. 2002.

[27] C. Ji, V. Chan and G. Liu, "Network management information for light-path assessment," Proc. of IEEE ISIT 2002, Lausanne, Switzerland, June 2002.

[28] G. Liu, C. Ji and V. Chan "Network management information for light-path assessment," Proc. of IEEE Infocom 2003, Apr. 2003.

[29] R. O. Duda and P. E. Hart, Pattern Classification, Wiley, New York, 2001.

[30] L. Rabiner, "A tutorial on hidden markov models and selected applications in speech recognition", Proceedings of the IEEE, 77 (2), 1989.

[31] H. Cramer, "Mathematical Methods of Statistics," Princeton University Press, 1946.

[32] M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security issues in all-optical networks," IEEE Network, Vol. 11, No. 3, pp. 42-48, May/June 1997.

[33] T. Wu and A. K. Somani, "Cross-talk attack monitoring and localization in all-optical network," IEEE/ACM Transactions on Networking, Vol. 13, No. 6, pp. 1390-1401, Dec. 2005.

[34] M. Medard, S. R. Chinn, and P. Saengudomlert, "Node wrappers for QoS monitoring in transparent optical nodes," Journal of High Speed Networks, Vol. 10, pp. 247-268, 2001.

[35] "Secure Optical Networks," Cisco Systems, White Paper, Copyright 1999-2005.

[36] R. Bergman, M. Medard, and S. Chan, "Distributed algorithms for attack localization in all-optical networks," Network and Distributed System Security Symposium, Session 3, paper 2, 1998.

[37] J. K. Patel, S. U. Kim, D. H. Su, S. Subramaniam, and H-A Choi, "A framework for managing faults and attacks in WDM optical networks," Proc. of the DAPRA Information Survivability Conference and Exposition, 2001.

[38] S. Stanic, S. Subramaniam, H. Choi, G. Sahin, and H-A Choi, "Efficient alarm management in optical network," Proc. of the DAPRA Information Survivability Conference and Exposition, 2003.

[39] C. M. Machuca, I. Tomkos, and O. K. Tonguz, "Failure location algorithm for transparent optical networks," IEEE Journal on Selected Areas in Communications, Vol. 23, pp. 1508-1519, Aug. 2005.

[40] P. Smyth, D. Heckerman, and M. I. Jordan, "Probabilistic independence networks for hidden markov probability models," Neural Computation, 9, pp. 227-270, 1997.

[41] R. G. Cowell, A. P. Dawid, S. L. Lauritzen, and D. J. Spiegelhalter, "Probabilistic networks and expert systems," Springer-Verlag, New York, 1999.

[42] S. Geman and K. Kochanek, "Dynamic programming and the graphical representation of error-correcting codes," IEEE Transactions on Information Theory, 47, pp. 549-568, 2001.

[43] F. R. Kschischang, B. J. Frey, and H-A Loeliger, "Factor graph and the sum-product algorithm," IEEE Transactions on Information Theory, Vol. 47, No. 2, pp. 498-519, 2001.

[44] J. Zhou, R. Cadeddu, E. Casaccia, C. Cavazzoni, and M. J. O'Mahony, "Crosstalk in multiwavelength optical cross-connect networks," IEEE Journal of Lightwave Technology, Vol. 12, pp. 1423-1435, June 1996

[45] A Tzanakaki, I. Zacharopoulos, and I. Tomkos, "Broadband building blocks," IEEE Circuits and Devices Magazine, pp. 32-37, Mar./Apr. 2004.

[46] T. Deng and S. Subramaniam, "An analysis of optical amplifier gain competition attack in a point-to-point WDM link," Proc. of Opticomm, pp. 249-261, July 2002.

[47] S. Zachary and Ilze Ziedins, "Loss networks and Markov Random Field," Journal of Applied Probability, No. 2, pp. 403-414, 1999.

[48] K. Gummadi, R. Gummadi, S. Gribble, S. Ratnasamy, S. Shenker, and I. Stoica, "The impact of DHT routing geometry on resilience and proximity," Proc. of SIGCOMM 2003, Karlsruhe, Germany.

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

[50] 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.

[51] G. Liu and C. Ji, "Graphical Models for Resilience of All-Optical Networks under In-Band Crosstalk Attacks," Technical Report, School of ECE, Georgia Insitute of Technology, 2005.

[52] H. Zhu, H. Zang, K. Zhu, and B. Mukherjee, "A novel generic graph model for traffic grooming in heterogeneous WDM mesh networks," IEEE/ACM Transactions on Networking, Vol. 11, No. 2, pp. 285-299, Apr. 2003.

[53] M. Steinder and A. S. Sethi, "Probabilistic fault localization in communication systems using belief networks," IEEE Transactions on Networking, No. 5, pp. 809-822, Oct. 2004.

[54] 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.

[55] A. T. Ihler, J. W. Fisher III, R. L. Moses, and A. S. Willsky, "Nonparametric belief propagation for self-localization of sensor networks," IEEE Journal on Selected Areas in Communications, Vol. 23, pp. 809-819, Apr. 2005.

[56] M. Paskin, C Guestrin, and J. McFadden, "A robust architecture for distributed inference in sensor networks," Proc of Information Processing in Sensor Networks, 2005.

[57] Y. Mao, F. R. Kschischang, B. Li, and S. Pasupathy, "A factor graph approach to link loss monitoring in wireless sensor networks," IEEE Journal on Selected Areas in Communications, Vol. 23, pp. 820-829, Apr. 2005.

[58] J. Barros, M. Tuchler, and S. P. Lee, "Scalable source/channel decoding for large-scale sensor networks," Proc. of IEEE International Conference on Communications, 2004.

[59] S. Jeon and C. Ji, "Nearly optimal distributed configuration management using probabilistic graphical model," Proc. of Workshop on Resource Provisioning and Management in Sensor Networks, pp. 219-226, MASS 2005.

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

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

[62] N. F. Maxemchuk, I. Ouveysi, and M. Zukerman, "A quantitative measure for telecommunications network topologies design," IEEE/ACM Transactions on Networking, Vol. 13, No. 4, pp. 731-742, Aug. 2005.

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

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

[65] 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.

[66] 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.

[67] B. Sanso and F. Soumis, "Communication and Transportation Network Reliability Using Routing Models," IEEE Transactions on Reliability, Vol. 40, 1991.

[68] 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.

[69] 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.

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

[71] V. Tamilraj and S. Subramaniam, "A Comparison of Optical Network Topologies," Forty-First Annual Allerton Conference on Communication, Control and Computing, Oct. 2003.

[72] A. Girard and B. Sanso, "Multicommodity flow models, failure propagation, and reliable loss network design," IEEE/ACM Transactions on Networking, Vol. 6, No. 1, pp. 82-93, Feb. 1998.

[73] E. Modiano, A. Narula-Tam, "Survivable light-path routing: a new approach to the design of WDM-based networks," IEEE Journal on Selected Areas in Communications, Vol. 20, No. 4, pp. 800-809, May 2002.

[74] A. Nucci, B. Sanso, T. G. Crainic, E. Leonardi, and M. A. Marsan, "Design of fault-tolerant logical topologies in wavelength-routed optical IP networks," in Proc. GLOBECOM 2001 San Antonio, TX, Nov. 2001.

[75] S. Kandula, D. Katnabi, and J. Vasseur, "Shrink, a tool for failure diagnosis in IP networks," Minenet 2005.

[76] 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.

[77] Y. B. Yoo and N. Deo, "A comparison of algorithms for terminal-pair reliability," IEEE Transactions on Reliability, Vol. 37, No. 2, pp. 210-215, June 1988.

[78] K. Sivarajan and R. Ramaswami, "Lightwave networks based on de Bruijin graphs," IEEE/ACM Transactions on Networking, Vol. 2, pp. 0-79, Feb. 1994.

[79] D. L. Jagerman, "Some properties of the Erlang loss function," Bell Systems Technical Journal, Vol. 53, pp. 525-551, 1974.

[80] W. Whitt, "Blocking when service is required from several facilities simultaneously," AT&T Technical Journal, Vol. 64, No. 8, pp. 1807-1855, Oct. 1985.

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

[82] 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.