Design and Management of Survivable Network: Concepts and Trends

Myeong-Kyu Song
Department of Information Communication Engineering
Namseoul Univ., Cheonan, ChoongNam , Korea

ABSTRACT

The article first presents a broad overview of the design and management for survivable network. We review the concept of network survivability, various protection and restoration schemes. Also we introduce design architectures of Quantitative model and a Survivable Ad hoc and Mesh Network Architecture. In the other side of study like these(traditional engineering approach), there is the concept of the survivable network systems based on an immune approach. There is one sample of the dynamic multi-routing algorithms in this paper.

Keywords: *Network Survivability, Restoration, Protection, Fault management, Multi-routing algorithm*

1. INTRODUCTION

With the maturing of wavelength-division multiplexing (WDM) technology, one single strand of fiber can provide tremendous bandwidth (potentially a few tens of terabits per second) by multiplexing many non-overlapping wavelength channels (WDM channels). Each wavelength channel can be operated asynchronously and in parallel at any desirable speed (e.g., peak electronic speed of a few gigabits per second). In a wavelength-routed WDM network, an optical cross-connect (OXC) can switch the optical signal on a WDM channel from an input port to an output port without any optoelectronic conversion of the signal; thus, a light-path may be established from a source node to a destination node, and it may span multiple fiber links. A fiber cut usually occurs due to a duct cutl during construction or destructive natural events, such as earthquakes, etc. All the light-paths that traverse the failed fiber will be disrupted so a fiber cut can lead to tremendous traffic loss. Other network equipment (OXC, amplifier, etc.) may also fail. Table 1 shows some typical data on network component (transmitter, receiver, fiber link [cable], etc.) failure rates and failure repair times according to Bellcore (now Telcordia) [1].

Table 1. Failure rates and repair times (Telecordia [4])

Metric	Bellcore Statistics
Equipment MTTR	2 hrs
Cable-Cut MTTR	12 hrs
Cable-Cut Rate	Rate 4.39/yr/1000 sheath miles
Tx failure rate	10867/ 10^9 hrs (FIT)
Rx failure rate	4311/ 10^9 hrs (FIT)

In table 1, failure-in-time (FIT) denotes the average number of failures in 10^9 hours, Tx denotes optical transmitters, Rx denotes optical receivers, and MTTR means mean time to repair. With the frequent occurrence of fiber cuts and the tremendous traffic loss a failure may cause, network survivability becomes a critical concern in network design and real-time operation. As networks migrate from stacked rings to meshes because of the poor scalability of interconnected rings and the excessive resource redundancy used in ring-based fault management schemes, designing and operating a survivable WDM mesh network have received increasing attention [2–6]. Most of the research work on survivability in WDM networks focuses on recovery from a single link or node failure, where one failure is repaired before another failure is assumed to occur in the network. Nevertheless, as our knowledge on this subject has matured, the more realistic scenario of multiple near simultaneous failures should now be considered (e.g., more than one link may be affected when a natural disaster such as an earthquake occurs). Meanwhile, as our knowledge of resource management in survivable network design and real-time operation continues to mature, more and more researchers are shifting their attention to a service perspective. Naturally, how to provide a certain quality of service (QoS) per a customer's requirement and how to guarantee the service quality become critical concerns. The rationale behind this is as follows. A WDM mesh network may provide services for IP network backbones, asynchronous transfer mode (ATM) network backbones, leased lines, virtual private networks (VPNs), and so on. The QoS requirements for these services can be very different because of their diverse characteristics; for example, online trading, military applications, and banking services will require stringent reliability, while IP best effort packet delivery service may be satisfied without a special constraint on reliability. Service quality can be measured in many different ways such as signal quality, service availability, service reliability, restoration time, and service restorability. Signal quality is mainly represented by the optical signal-to-

* *Corresponding author. E-mail : mksong@nsu.ac.kr*
Manuscript received May. 20, 2009 ; accepted Jun. 23, 2009

noise ratio (OSNR), bit error rate (BER), and other factors, and is affected by the transmission equipment characteristics. This is a problem in all-optical networks, and is out of the scope of our current discussion. Our interest is in the availability of service paths in WDM mesh networks. Usually, availability is defined as the probability that the service or connection will be found in the operating state at a random time in the future [7]. Connection availability can be computed statistically based on the failure frequency and failure repair rate, reflecting the percentage of time a connection is "alive" or "up" during its entire service period. Although the problem of how connection availability is affected by network failures is currently attracting more research interest [1], [7]–[9], we still lack a systematic methodology to quantitatively estimate a connection's availability, especially when protection schemes are applied to the connection. In this review we shall discuss the rationale and challenges for availability analysis in WDM mesh networks. In particular, we shall present a framework for a generic connection provisioning problem with due consideration of network component failure characteristics so that all possible network failure scenarios and their effects can be incorporated.

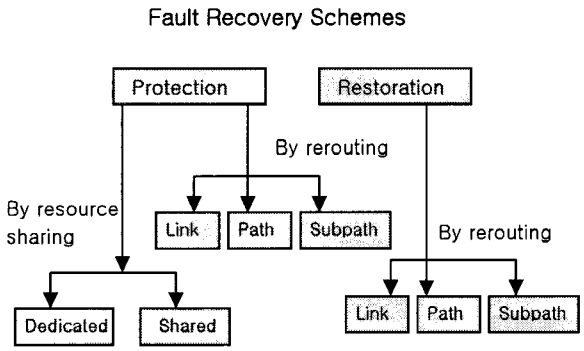

Fig. 1 Different protection and restoration schemes

2. CONCEPTS IN FAULT MANAGEMENT

The most general and important method of fault management for survivable network is fault recovery scheme. There are two types of fault recovery mechanisms [3]. If backup resources (routes and wavelengths) are pre-computed and reserved in advance, we call it a protection scheme. Otherwise, when a failure occurs, if another route and a free wavelength have to be discovered dynamically for each interrupted connection, we call it a restoration scheme. Protection schemes can be classified into ring protection and mesh protection. Ring protection schemes include Automatic Protection Switching (APS) and Self-Healing Rings (SHR). Both ring and mesh protection can be further divided into two groups: path and link protection. Figure 1 summarizes the classification of protection and restoration schemes. The following section describes basic concepts of these scheme.

2.1 Network survivability

There have been several accounted to research the survival or self-healing network. One of the widely known method is the LAN of having the dual Ring type. The FDDI and DQDB of MAN have this dual Ring structure. But the ring type of network is used in the restricted environment. Therefore we need to find the more general type of network having survivability. The mesh type network is more general. The network structure type may be to divide into 3 types. This is a section to consider the network survivability. There is in figure 2. In this figure, the second and third type (two connected topology and biconnected topology) have received attention for network survivability.

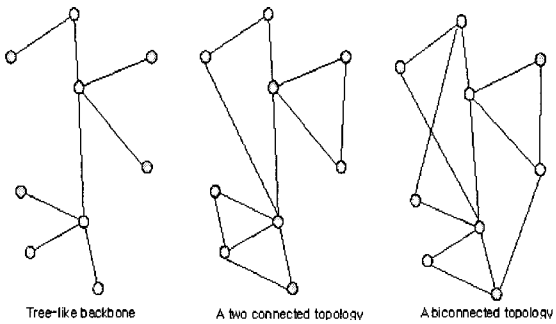

Fig. 2 The physical type of Network

If there are some faults in network Links, the first type is impossible to repair automatically. The others can be repaired by itself. Because they have dual routes. The second case is the Link-disjoint type(A). The third case is the Node-disjoint type(B). The B type has all characters of A type. But A type has not all characters of B type.

2.2 Management Concepts

2.2.1 Path protection/restoration

In path protection, backup resources are reserved during connection setup, while in path restoration, backup routes are discovered dynamically after the link failure. When a link fails [illustrated in Fig. 3(a)], the source node and the destination node of each connection that traverses the failed link are informed about the failure via messages from the nodes adjacent to the failed link, as illustrated in Fig. 4.

- **Dedicated-path protection:** In dedicated-path protection (also called 1:1 protection), the resources along a backup path are dedicated for only one connection and are not shared with the backup paths for other connections.
- **Shared-path protection:** In shared-path protection, the resources along a backup path may be shared with other backup paths. As a result, backup channels are multiplexed among different failure scenarios (which are not expected to occur simultaneously), and therefore, shared-path protection is more capacity efficient when compared with dedicated-path protection.

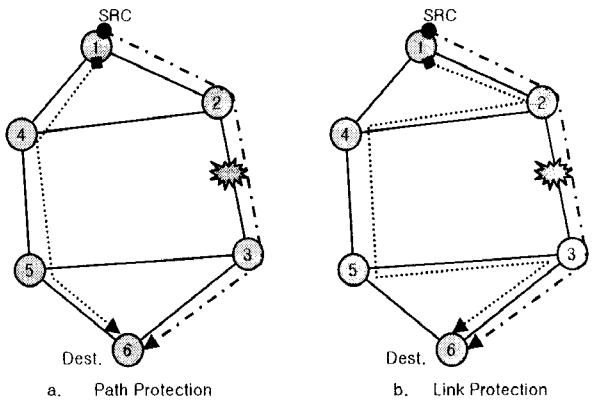

Fig. 3 Protection Types

• **Path restoration:** In path restoration, the source and destination nodes of each connection traversing the failed link participate in a distributed algorithm to dynamically discover an end-to-end backup route. If no routes are available for a broken connection, then the connection is dropped.

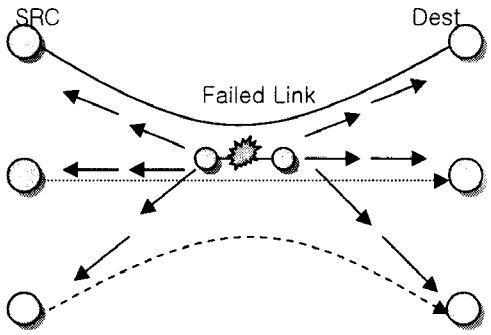

Fig. 4 Sending a failed Link Information

• **Path restoration:** In path restoration, the source and destination nodes of each connection traversing the failed link participate in a distributed algorithm to dynamically discover an end-to-end backup route. If no routes are available for a broken connection, then the connection is dropped.

2.2.2 Link protection/restoration

In link protection, backup resources are reserved around each link during connection setup, while in link restoration, the end nodes of the failed link dynamically discover a route around the link. In link protection/restoration [illustrated in Fig. 3(b)], all the connections that traverse the failed link are rerouted around that link, and the source and destination nodes of the connections are oblivious to the link failure.

• **Dedicated-link protection:** In dedicated-link protection, at the time of connection setup, for each link of the primary path, a backup path and wavelength are reserved around that link and are dedicated to that connection. In general, it may not be possible to allocate a dedicated backup path around each link of the primary connection and on the same wavelength as the primary path. For example, figure 5 shows a bidirectional ring network with one connection request between Node 1 and Node 5. The backup path around link (2,3), viz. (2,1,8,7,6,5,4,3), and the backup path around link (3,4), viz. (3,2,1,8,7,6,5,4), share links in common and hence cannot be dedicated the same wavelength.2 Since our experience indicates that dedicated-link protection utilizes wavelengths very inefficiently, we will not consider dedicated-link protection in this work.

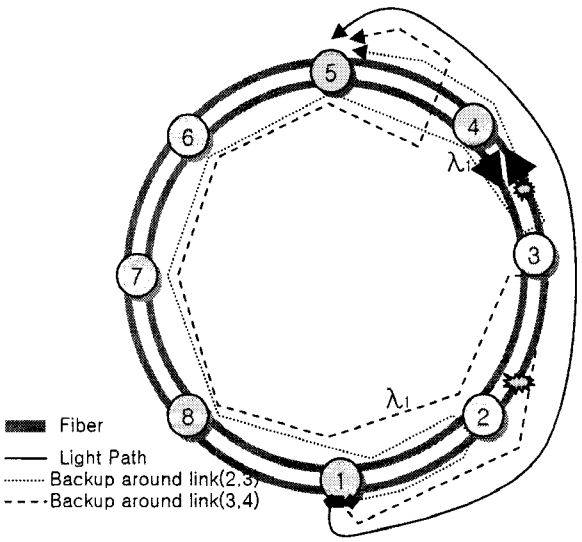

Fig. 5 A bidirectional ring network

• **Shared-link protection**

In shared-link protection, the backup resources reserved along the backup path may be shared with other backup paths. As a result, backup channels are multiplexed among different failure scenarios (which are not expected to occur simultaneously), and therefore shared-link protection is more capacity-efficient when compared with dedicated-link protection.

Link restoration: In link restoration, the end nodes of the failed link participate in a distributed algorithm to dynamically discover a route around the link. If no routes are available for a broken connection, then the connection is dropped.

2.2.3 Protection VS. Restoration

Survivable techniques can be categorized into two major groups: pre-planned protection and dynamic restoration techniques. Pre-planned protection techniques refer to the fact that protection resources, which are specified at the planning stage, protect system from failures. Since some of the resources and components are only used for protection in this technique, the network bandwidth utilization is dramatically reduced. However, recovery from failures is accomplished quickly and with a high probability. Two kind of protection are possible, namely dedicated and shared protection. In the dedicated case, a second copy of data is simultaneously transmitted on both working and protection paths. Accordingly, the network bandwidth utilization is narrow down to half in this case. However, 100% service recovery is guaranteed in the dedicated protection. In the shared case, a second copy of data is sent through a protection path only after detecting a failure. To be more bandwidth-efficient, the capacity of the protection path is shared among a group of working paths and is assigned to low priorities requests in the absence of failures. Then, the shared protection path is pre-emptied after a failure is detected. However, performing preempting procedures for optical networks requires buffering which is still the limitation of

optical networks. To overcome the drawbacks associated with pre-planned protection techniques, dynamic restoration protocols are introduced. Dynamic restoration implies discovering the unoccupied network capacities and assigning them to affected traffic. Dynamic restoration protocols are more resource-efficient than the counterpart since they do not require setting aside or adding protection resources. However, restoration time is usually longer. Furthermore, 100% service recovery cannot be guaranteed, as sufficient capacities may not be available at the time of failure.

2.2.4 Dynamic Restoration

Dynamic restoration mechanisms are based on three basic paradigms: disjoint path restoration; partially joint path restoration; link restoration. In disjoint path restoration, an S-D pair dynamically discovers an available alternate route, which is completely diverse form the primary path, to reroute the affected traffic. On the contrary, partially joint path restoration recovers the data through the shortest alternate path that usually have some common links with the affected path. Link restoration on the other hand, set up the shortest loop around the failed link. Accordingly based on the definitions, disjoint path restoration is an end-to-end scheme, link restoration is a point-to-point algorithm, and partially joint path restoration is a tradeoff between the two former mechanisms. Figure 6 contrasts disjoint path, partially joint path, and link restoration. Dotted lines show the affected paths and solid lines demonstrate restoration paths. Both path and link restoration perform efficiently if they occupy the available capacity of the shortest paths/loops. However, sometimes these two approaches end up with lengthy restoration paths/loops. As a result, the restoration processes become inefficient. Figure 7 compare efficient another type of dynamic restoration is achieved through partially joint path restoration. Since this approach keeps some of the working links in place, it is more efficient than disjoint path restoration.

However, it requires locating the failure in advance to avoid the failed link. Proposals are scarce in the literature and the existing ones are mostly linked to shared protection and segmented protection mechanisms. However, [10] proposes a novel method called Maximum Mutual Links- kth shortest path (MML) that leads to partially joint path restoration.

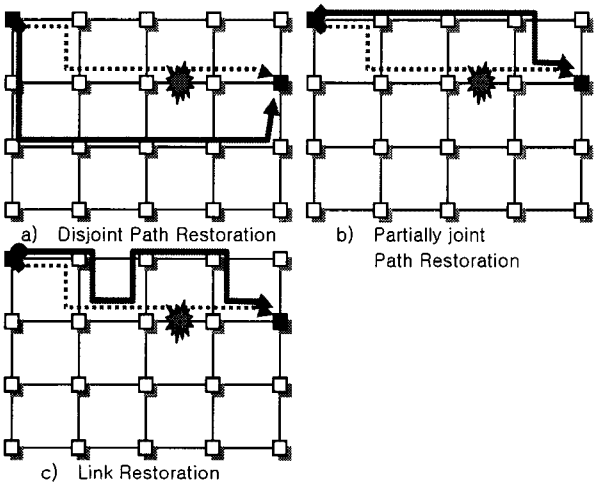

Fig. 6 Path & Link Restoration

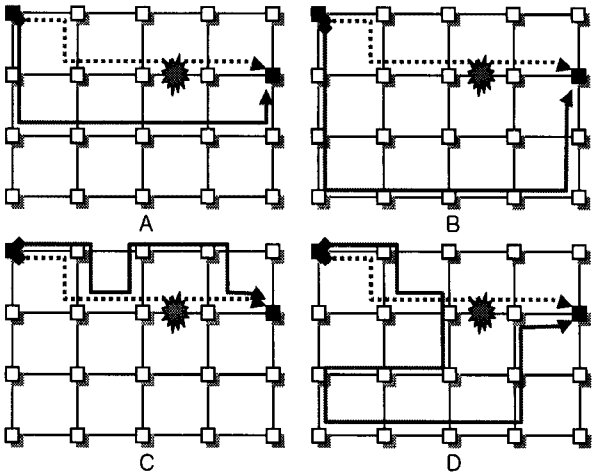

Fig. 7 Restoration Efficiency

A successful restoration path in MML satisfies two criteria: the number of tobe-configured (added) switches is minimized; the number of hops between the (source-destination) s-d pair is minimized (the kth shortest path is selected). Two weighting factors, namely length and switching factors are used to cover both criteria in chorus and reach a joint solution. Accordingly, the path that minimizes the overall weight is selected for partially joint path restoration. However, the weight assignment and comparison procedures increase the computational complexity. Like partially joint path restoration, link restoration is possible if the faulty link can be localized in advance. A protocol that is usually employed in WDM rings is Loop-back. In loop-back two nodes adjacent to the failure are responsible for switching the affected traffic to the restoration path [11]. Loop-back mechanism is also applicable to recovery from node failures but sometimes it leads to inefficient unnecessary examinations of all alternate loops. For mesh networks, Generalized Loop-back (GL) has been introduced [12]. This scheme finds a conjugate diagraph, called the secondary diagraph for the primary diagraph to flood the effected traffic with it. However, the flooding action with simultaneous failures can lead to complications and ultimately to performance degradations.

3. DESIGN ARCHITECTURE

We present two design architectures in this section. These architecture are SRLSQM(the quantitative model of spare resource limited survivability) and SAMNAR (Survivable Ad hoc and Mesh Network Architecture).

3.1 Quantitative model

3.1.1 Formulation of the quantitative model

This section presents a quantitative model of spare resource limited survivability(SRLSQM), based on the definition and four characteristic attributes of network survivability.[13]

We can find a quantitative model to achieve and improve spare resources limited survivability as illustrated in figure 8.

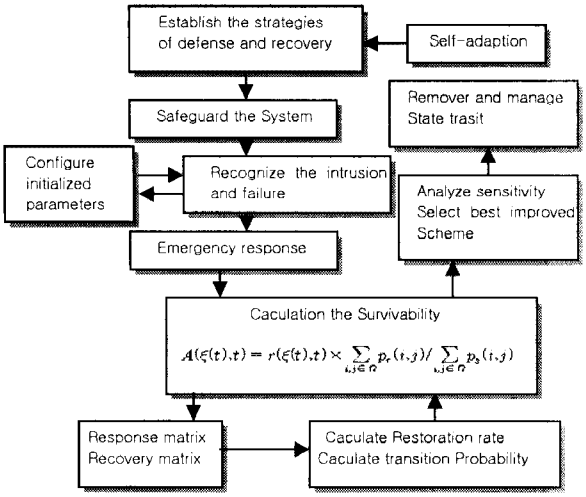

Fig. 8 A quantitative model

SRLSQM can be mainly depicted as follows: first, establish a series of safety strategies, including system defense and recovery strategies and the like. In order to ensure system security, some traditional static safety technique may be used, such as firewalls, encryption, authentication, and so on, which can drive up the doorsill of hacker attack technique to improve the network defense capability. According to the system information which has already been collected (like system environment information, input and output data, etc.), adopt detection technology to recognize the kind of future intrusion, and configure corresponding parameters. Second, response to the security leak or damage event, recognize the failed area and degree, set up corresponding emergency response scheme, including to give a alarm, inform administrator of updating configuration and the like. Third, establish the system response model(matrix) to these intrusion events, choose recovery strategy based on the damage degree, then compute recovery matrix according to it, and calculate system survivability with the arithmetic which will be put forward in the following text. Fourth, carry through the sensitivity analysis to find factors making great influence on the system and readjust parameters, then select best improved scheme. Finally, make recovery and management in order to continue system services after being attacked or destroyed. The last step also includes enhancing the capability of self-adaptation after being damaged.

3.1.2 Characteristic of the quantitative model

SRLSQM is in accordance with the definition of survivability which is presented by CMU/SEI research group[16],[17]and the four characteristic attributes proposed by Robert et al[18]. It is also exercisable, because we have quantified the response and recovery matrix, restoration rate and state transition in the model.

3.1.3 Executing process of the quantitative model

To enhance the maneuverability of SRLSQM, we design the executing process as follows:

Step1: read initialized parameters from database.

Step2: use event creating program to create original event at once, when the first attack occurs.

Step3: get defense strategy program from database according to the kind of created attack event.

Step4: compute the response matrix of the system.

Step5: turn to step 11 if the state of the system is normal, which shows the system has defended successfully, otherwise go along next step.

Step6: compute the recovery matrix of the system.

Step7: calculate survivability of the system.

Step8: find security leaks of the system and adjust parameters making great influence on it.

Step9: get corresponding recovery program.

Step10: go along next step if the state of the system has been improved, or else turn to step 12, which denotes administrator must modify recovery library.

Step11: turn to step 3, if here a new attack event occurs, otherwise go along next step.

Step 12: end.

3.2 SAMNAR Architecture

This section describes SAMNAR[14], a Survivable Ad hoc and Mesh Network Architecture which goal is to offer network operations or minimal service levels despite passive or active attacks. SAMNAR is based on the cooperation of the three defense lines, preventive, reactive and tolerant, and on the capability of network adaptation. In SAMNAR, preventive defenses, such as cryptography, firewalls and access control services, correspond the first obstacle to attacks. As these defenses block certain ones and are incapable of preventing others, reactive defenses as IDSs act to detect and stop them. However, reactive defenses also have limitations and some intruders can harm a giving node or the network. Thus, tolerant defenses work proactively to ensure the continuance of minimal service level by mechanisms as redundancy, until those preventive or reactive defenses can adapt them and take actions against attacks or intrusions. SAMNAR contains the survival, communication and collect modules. Fig. 1 illustrates them considering a network node/device. The survival module holds five independent components, being four ones related to SAMNAR properties, resistance, recovery, recognition and adaptability, and the control component. The properties represent respectively the network capability of repelling attacks; detecting attacks and evaluating the extent of damage; restoring disrupted information or functionalities; and quickly incorporating lessons learned from failures and adapting to emerging threats. The resistance component consists of preventive mechanisms such as firewall, access control, authentication and cryptography. This component works in a self-protection and self-adjusting fashion where preventive mechanisms and their configuration will be changed depending on the network or environment conditions. The rule of a distributed firewall, for instance, can be more rigorous in certain environments, while simpler rules can be applied in more secure environments. Another example is the cryptographic key size that can be larger depending on the environment. The recognition component comprehends reactive mechanisms to identify malicious behaviors such as IDSs, reputation systems, anti-malwares and anti-spammers. Recognition mechanisms can have also the capability of reacting and stopping intrusions. All the mechanisms will be reconfigured if necessary by the adaptation component. New

configurations such as IDS rules will depend on the network and environment figure 9: SAMNAR Architecture conditions.

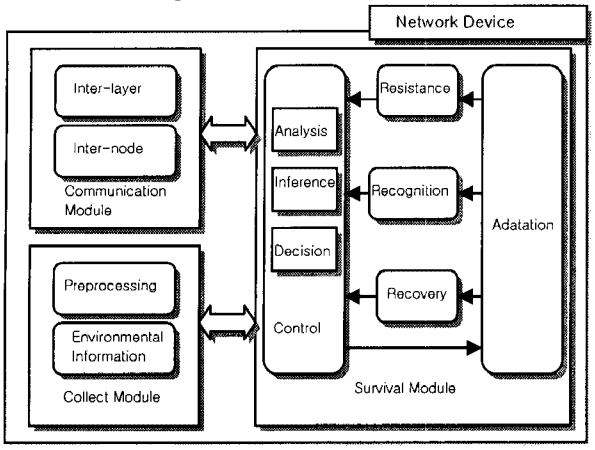

Fig. 9 SAMNAR Architecture

This component provides to the control component information about detections, trustworthiness of neighbor devices among others. The recovery component consists of mechanisms to enhance the attack tolerance of network essential services. Mechanisms to restore disrupted information or functionality such as replication or redundancy have been employed as tolerant mechanisms. The application of two cryptography algorithms successively and the replication of message pieces are examples of redundancy. Sending redundant message pieces by different routes increases the probability of the message to be received by the destination node and the possibility of message recovery in case of piece losses. However, redundant strategies should consider resource limitations as well as service and application requirements. The adaptation component complements the previous ones. It is responsible for adapting preventive, reactive and tolerant mechanisms as well as local or network configurations. It can replace a given protocol or a defense mechanism, such as changing a weaker cryptographic algorithm for a stronger one, depending on the necessities and requirements on time. Further, the adaptation component can change the key size of a cryptographic algorithm, the rules into an IDS or a firewall, the used route and others in accordance with the network condition or decisions taken by the control component. The control component manages and coordinates all modules in the architecture. It receives information from communication and collect modules as well as from the resistance, recognition and recovery components. The control component correlates and analyzes all information in order to make inferences and take decisions. All decisions are sent to the adaptation component that define and send satisfactory parameter values to other modules or components. Adaptation component learn with taken actions and later, it can take the same action if the node or network present a similar condition. The communication module is responsible by cross-layer and inter-node communications. The inter-layer component offers the exchange of information inter-layers. It supplies information from different network layers to control component so that it takes decisions based on all network layers and achieves the survivability for all of them. The inter-node component provides communication, exchange and synchronization of information among the nodes aiming to guarantee the survivability of the whole network. Example of this information is the node configuration or network intrusion detections. The collect module holds mechanisms to gather all data required by the survival module. It is out of the architecture scope to define the collection method. However, the survival module specifies adaptively which data and information must be collected following its requirements. The collect module is composed of the preprocessing component and the environmental information component. The first one is exploited when gathered data need to be treated before sending to the survival module. Normalizations, previous calculations and others are examples of preprocessing used to facilitate analyses and inferences of the survival module. The second component stores information gathered periodically about the network conditions, sending it to the survival module when required.

4. VARIOUS SURVIVABLE NETWORKS

In this section, there are two approaches for the survivable network. The one is related to the wireless sensor network and the other is a approach method using the immune concept. These mean that there are various researches for the survivable network.

4.1 Survivable and Secure Wireless Sensor Networks

A wireless sensor network (WSN) consists of battery operated sensor devices with computing, data processing, and communicating components. In WSNs, the sensor nodes can be deployed in controlled environment such as factories, homes, or hospitals; they can also be deployed in uncontrolled environment such as disaster or hostile area, in particular battlefield, where monitoring and surveillance is crucial. Clearly, security in WSNs is extremely important for both controlled environment (e.g., health-care, automation in the transportation, etc.) and uncontrolled and hostile environment (e.g., environmental monitoring, military command and control, battlefield monitoring, etc.). Moreover, the majority of the WSN applications should be run continuously and reliably without interruptions. Hence, survivability should also be taken into account in developing WSNs.

4.1.1 Reliability

In addition to the security concerns, the reliability of the network is also of special interest because many applications require the WSNs to be operating in uncontrolled environments. In such cases, some wireless sensor nodes may be failed, thus affecting the operation of the whole network. Reliability is the capability to keep the functionality of the WSN even if some sensor nodes are failed.

4.1.2 Availability

Availability ensures that services and information can be accessed at the time that they are required. In WSNs there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks. Lack of

availability may affect the operation of many critical real time applications. Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network. If a node serves as an intermediary or collection and aggregation point, what happens if the node stops functioning? The protocols employed by the WSN need to be robust enough mitigate the effects of outages by providing alternate routes. Energy Efficiency: WSN consists of battery-operated sensor devices with computing, data processing, and communicating components. Energy conservation is a critical issue in WSNs since batteries are the only limited life energy source to power the sensor nodes. Apparently, the battery life affects the reliability and availability of the WSN. Any protocols including security mechanisms designed for WSN should be energy aware and efficient. Evidently, there is a coupling between security, reliability, availability, and energy efficiency of WSNs. This motivates us to study the interactions of security and survivability of WSNs, so that we can effectively analyze and design secure and survivable WSNs.

4.2 Survivable network systems based on an Immune Approach

4.2.1 Organizing principles

In spite of there are several fundamental differences between the biology and network systems, a study of immune system reveals a useful set of organizing principles that we believe should guide the design of survivable network systems:

(1) Disreputability: Lymphocytes in the immune system are able to determine locally the presence of an infection, and no central coordination takes place. The human immune system provides a good example of a highly distributed architecture that greatly enhances robustness.

(2)Multi-layered: In immune system, no one mechanism confers complete survivability. Rather, multiple layers of different mechanisms are combined to provide high overall survivability. This is not a new concept in network survivability, but we believe it is important and should be emphasized in system design.

(3)Diversity: By making systems diverse, survivability vulnerabilities in one system are less likely to be widespread. There are two ways in which systems can be diverse: the protection systems can be unique or the protected systems can be diversified.

(4)Disposability: No single component of the human immune system is essential—that is, any cell can be replaced. Immune system can manage this because cell death is balanced by cell production. Although we do not currently have self-reproducing hardware, death and reproduction at the process level is certainly possible and would have some advantages if it could be controlled.

(5)Autonomy: The immune system does not require outside management or maintenance; it autonomously classifies and eliminates pathogens, and it repairs itself by replacing damaged cells. Although we do not expect (or necessarily want) such a degree of independence from our computers, as network and CPU speeds increase, and as the use of mobile code spreads, it will be increasingly important for computers to manage most security problems automatically.

(6)Adaptability: The immune system learns to detect new pathogens, and retains the ability to recognize previously seen pathogens through immune memory. A computer immune system should be similarly adaptable, both learning to recognize new intrusions and remembering the signatures of previous attacks.

(7)Dynamically changing coverage: Immune system makes a space/time tradeoff in its detector set: it cannot maintain a set of detectors (lymphocytes) large enough to cover the space of all pathogens, so instead at any time it maintains a random sample of its detector repertoire, which circulates throughout the body. This repertoire is constantly changing through cell death and reproduction.

(8)Anomaly detection: Immune system has an ability to detect pathogens that it has never encountered before, i.e. it performs anomaly detection. We believe that the ability to detect intrusions or violations is an important feature of any survivable system.

(9)Imperfect detection: By accepting imperfect detection, the immune system increases the flexibility with which it can allocate resources. For example, less specific lymphocytes can detect a wider variety of pathogens but will be less efficient at detecting any specific pathogen.

(10)The numbers game: Human immune system replicates detectors to deal with replicating pathogens. It must do so—otherwise, the pathogens would quickly overwhelm any defense. Computers are subject to a similar numbers game, by hackers freely trading exploit by computer viruses. For example, success of one hacker can quickly lead to compromise of thousands of hosts. Clearly, the pathogens in network survivability world are playing the numbers game—traditional systems, however, are not. These properties can be thought of as design principles for a survivable network system. Many of them are not new, and some have been integral features of survivable network systems; however, no existing survivable network system incorporates more than a few of these ideas. Although the exact biological implementation may

or may not prove useful, we believe that these properties of natural immune systems can help us design more survivable network systems.

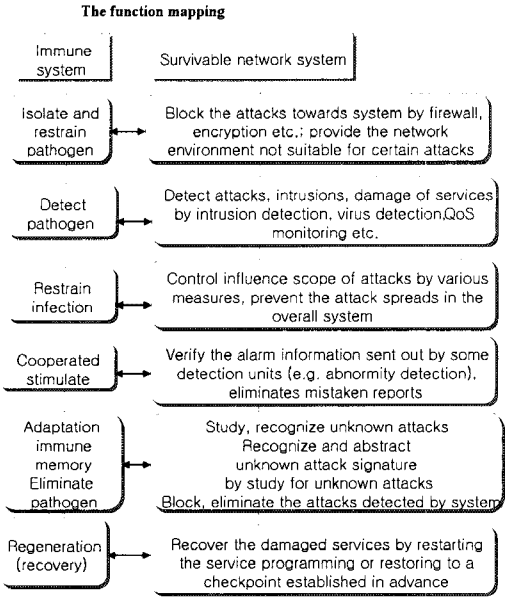

Fig. 10 The function mapping

4.2.2 Design for survivable network system

One approach to design survivable network system that incorporate the principles discussed in the previous section is to design systems based on direct mappings between immune system components and current network system architectures. The function mapping between the biological immunity system and the survivable network system is showed in figure 10. Various functions showed in figure 10 correspond to concrete modules structure. There exist 7 modules in the system structure, and we will illuminate as follows.

(1)Resistance module: isolates attack from the network system through establishing barrier, which has coped with the most attacks.

(2)Detection module: detects attack behavior, damage of services against the system, and sends out alarm information; the overall dynamic behavior of the system is driven by detection module.

(3)Adaptation module: studies and recognizes new attacks in the system, and automatically produce the patch procedure or attack signature used for filtering this kind of new attack and its simple variety, thus enhances flexibility of the system.

(4)Executive module: concrete execution unit of response and repair strategy, including recovery of control, block, elimination and its influence against attacks.

(5)Recovery module: Restores services which are damaged in the system, and it belongs to a part of response.

(6)Response and repair module: produces response and repair strategy with attack and system state information.

(7)Coordination control module: coordinates each unit in the system, and guarantees each kind of mechanism effective coordination

5. SURVIVABLE ROUTING : A SAMPLE[19]

In this section, the problem of survivable routing for overlapping segment protection is studied. Usually, the traffic in the backbone network is symmetric, thus we assume that each link is bidirectional. The problem is formally defined as follows. An undirected network is specified by $G = (N,L)$, where N is the set of nodes and L is the set of links in the network. The failure probability on link L_i is p_i. Nodes are assumed reliable. A source and a destination are given as, s, t N. The problem is to find a working path from s to t and backup paths, such that each link in a segment is covered by one or two backup paths and the end-to-end survivability is maximized. The problem is believed to be NP-Complete. To calculate survivability for the overlapping case, we consider each link that is protected by more than one backup path.

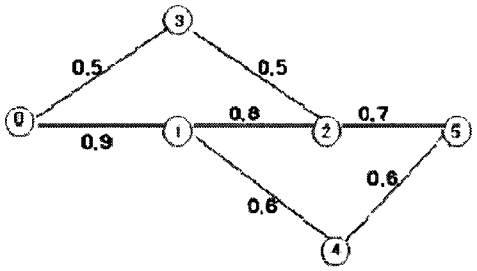

Fig. 11 An example for segment protection

We need to condition the end-to-end survivability on whether each overlapping link is failed or not. In the example of figure 11, only one overlapping link $L_{1,2}$ exists. Given that $L_{1,2}$ is not failed, the graph transformation is shown in figure 12.

The conditional survivability between node 0 and node 5 is, $(0.5 \times 0.5+0.9 / 0.5 \times 0.5-0.9)(0.6 \times 0.6 + 0.7 - 0.6 \times 0.6 \times 0.7) = 0.7474$. Given that $L_{1,2}$ is failed, the graph transformation is shown in figure 13.

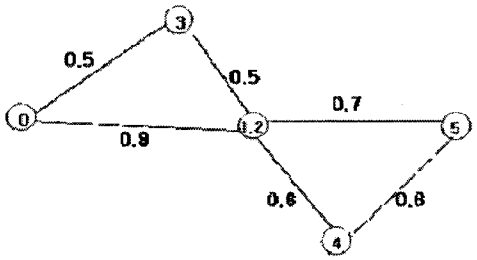

Fig. 12 Graph transformation if $L_{1,2}$ is not failed.

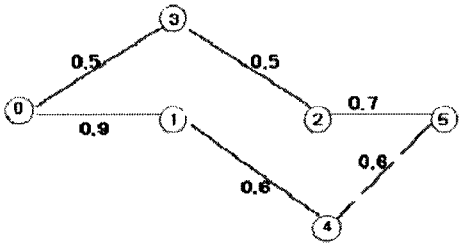

Fig. 13 Graph transformation if $L_{1,2}$ is failed.

The conditional survivability between node 0 and node 5 is,

(0.5 × 0.5 × 0.7 + 0.9 × 0.6 × 0.6 - 0.5 × 0.5 × 0.7 × 0.9 × 0.6 × 0:6) = 0.4423. Thus, the end-to-end survivability between node 0 and node 5 can be obtained by the total probability, 0.8 × 0.7474 + 0.2 × 0.4423 = 0.68638. If multiple overlapping links exist in the network, we need to consider all combinations of link states. If m overlapping links exist for a connection, the complexity of the survivability calculation is $O(|N|^{m})$. Usually, the number of the overlapping links is not excessive for overlapping segment protection. Thus, this method can be implemented for the survivability calculation. The end-to-end survivability may increase if there are more overlapping links covered by backup paths. More overlapping links mean more backup resources need to reserve for the working paths. In this paper, we will investigate the cost of achieving this higher survivability. Our heuristic is based on the shortest path algorithm. Since the shortest path algorithm takes costs to be additive, it cannot be applied to the problem directly. Thus, the first step is to take the logarithm of failure probability for each link. The end-to-end survivability can be improved by selecting the backup paths to cover each segment. A negative factor will be used on the working links to generate more backup paths. We now propose a heuristic algorithm, called Survivable Segment Protection Algorithm (SSPA).

Step1: Assign the weight $\log_q q_i$ for each bidirectional link L_i. $q_i = 1 - r_i$, is the probability with which link L_i will not fail. q is a constant, $0 < q < 1$.

Step2: Run the shortest path algorithm to find the first shortest path $P1$ from source s to destination t.

Step3: Remove all the links along the shortest path that are directed towards t and multiply the length of links in the reverse direction of the shortest path by a negative factor ϵ, $-1 \le \epsilon < 0$. ϵ is used here to generate overlapping links.

Step4: Run the shortest path algorithm again to find the second shortest path $P2$. If there are some overlapping links between $P1$ and $P2$, keep all the links on $P1$ and remove the overlapping links on $P2$ to obtain separate backup paths for $P1$. In SSPA, the complexity of Step 1 and Step 3 is $O(|L|)$. The shortest path algorithm implemented in Step 2 and Step 4 can be within $O(|L| lg(|N|))$. Thus, the overall computational complexity is $O(|L| lg(|N|))$.

6. CONCLUDING AND FUTURE WORKS

Designing and management of survivable networks is an important and exciting research area. This paper reviews the fault management for network survivability. We examine various protection and restoration schemes, network architectures, survivability for WSN and survivable network system using an immune approach. Also we review the sample of survivable routing. These concepts and methods work in specific network environments. But if we see the study of survivable network systems based on an Immune Approach, we know that there is no general and optimal solution yet. Therefore more study is required in designing and operating a survivable network to provide differentiated service and efficiently provide service quality guarantees.

REFERENCES

[1] M. To and P. Neusy, "Unavailability Analysis of Long-Haul Networks," *IEEE JSAC, vol. 12*, Jan. 1994, pp. 100–09.

[2] G. Ellinas, A. Hailemariam, and T. E. Stern, "Protection Cycles in Mesh WDM Networks," *IEEE JSAC, vol. 18*, Oct. 2001, pp. 1924–37.

[3] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM Mesh Networks," *IEEE/OSA J. Lightwave Tech., vol. 21*, Apr. 2003, pp. 870–83.

[4] G. Mohan, C. S. R. Murthy, and A. K. Somani, "Efficient Algorithms for Routing Dependable Connections in WDM Optical Networks," *IEEE/ACM Trans. Net., vol. 9*, Oct. 2001, pp. 553–66.

[5] R. Ramamurthy et al., "Capacity Performance of Dynamic Provisioning in Optical Networks," *IEEE/OSA J. Lightwave Tech., vol. 19*, Jan. 2001, pp. 40–48.

[6] O. Gerstel and R. Ramaswami, "Optical Layer Survivability – An Implementation Perspective," *IEEE JSAC, vol. 18*, Oct. 2000, pp. 1885–99.

[7] M. Clouqueur and W. D. Grover, "Availability Analysis of Span-Restorable Mesh Networks," *IEEE JSAC, vol. 20*, May 2002, pp. 810–21

[8] A. Fumagalli et al., "Shared Path Protection with Differentiated Reliability," *Proc. IEEE ICC*, Apr. 2002, pp. 2157–61

[9] J. Zhang et al., "Service Provisioning to Provide Per-Connection-Based Availability Guarantee in WDM Mesh Networks," Proc. OFC, Mar. 2003, *expanded version in ICC*, May 2003.).

[10] A. V. Sichani and H. T. Mouftah, "Maximum Mutual Links-kth Shortest Path Protocol, A Survivable Routing Scheme for WDM Mesh Networks," *Proceedings of IST'05*, pp. 109-116, Sep. 2005.

[11] M. Medard, S. G. Finn, and R. A. Barry, "WDM Loop-back Recovery in Mesh Networks," *Proceedings of IEEE INFOCOM*, pp. 752-759, March 1999.

[12] M. Medard, S. G. Finn, R. A. Barry, and W. He, and S.S. Lumetta, "Generalized Loop-Back Recovery in Optical Mesh Networks," IEEE Transactions on Networking,"*vol. 10, no. 1*, pp.153-164, Feb. 2002.

[13] Zhou Meng, Zhou Xueguang, Zhang huanguo , "Modeling and Calculation for Network System Survivability", *2008 Workshop on Knowledge Discovery and Data Mining IEEE Computer Society.*

[14] Michele N. Lima, Helber W. da Silba, "An Architecture for Survivable Mesh Network," *IEEE GLOBCOM 2008 Proceeding.*

[15] Huiqiang Wang, Guosheng Zhao, and Jian Wang "Survivable Network System: An Immune Approach,"*2008 International Conference on Internet Computing in Science and Engineering*, pp329~331.

[16] Knight J C, Strunk E A, Sullivan K J. Towards a Rigorous Definition of Information System Survivability[C]. *Proceedings of DARPA Information Survivability Conference and Exposition*, 2003, 1:78-89.

[17] Vickic R, Westmark. A Definition for Information System Survivability[C].*Proceeding of the 37th Hawaii Internal Conference on System Sciences (HICSS'04), Track* 9.

[18] Robert J Ellison, David A Fisher, Richard C Linger, et al. An Approach to Survivable Systems[OL]. *http://www.ccrt.org/ easel/natol.doc*

[19] Qingya She, Xiaodong Huang, and Jason P. Jue, "Survivable Routing for Segment Protection under Multiple Failures," *2006 Optical Society of America OCIS codes: ((060.4250) Networks; (060.4510) Optical communications.*

Myeong-Kyu Song

He received the B.S., M.S., Ph.D. in Electronics Engineering from Yonsei university, Korea in 1987, 1989, 1996 respectively. He has been a professor of Namseoul University in CheonAn, Korea since 1996. His main research interests include Network Design and Management.