Multipath Routing for Survivability of Complex Networks Under Cascading Failures

Preetha Thulasiraman
Department of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, CA, USA
pthulas1@nps.edu

***Abstract*—Complex infrastructure networks have been characterized as being scale-free and therefore maintain a heterogeneous node distribution. While scale free networks (SFN) have been investigated using vulnerability assessments, particularly that of cascading node failures, existing research has not dealt with the aftermath of these failures. This paper addresses the problem of discovering end to end paths in a SFN in the presence of cascading failures such that survivability is achieved for each source-destination pair. We first develop a model to capture cascading failures in SFNs while redistributing traffic load to neighboring nodes. Given the traffic distribution after the cascade of failures, we develop a routing algorithm such that backup connections are constructed for each source-destination pair. We formulate the routing algorithm by exploiting the multipath topology of SFNs and the different priorities of the traffic flows. We compare our routing approach in a SFN with that of a random network in which node distributions are homogeneous. We show that our routing algorithm performs well under intentional node attacks and efficiently considers the classification of the traffic when constructing alternate routing paths.**

Keywords – **scale free networks; multipath routing; cascading failures; load redistribution**

I. Introduction

Complex networks such as the Internet, electrical power grid and telecommunication and transportation systems are an essential part of the global society. These infrastructure networks are not random but rather known to be scale free, with some nodes having a tremendous number of connections, whereas others have only a few connections [1]. This highly heterogeneous node distribution has led researchers to prove that the degrees of the nodes in scale free networks (SFN) follow a power law distribution: the probability that any node is connected to k other nodes, $P(k)$, is proportional to $\frac{1}{k^n}$, where n is a parameter whose value is typically in the range $2 < n < 3$ [1]. Due to its topology, SFNs are robust against accidental failures (which tend to affect low degree nodes), but are vulnerable to coordinated attacks that target highly connected nodes in order to inflict maximum damage by disabling numerous connections.

The fragile properties of SFNs become more evident when the intrinsic dynamics of the network flows are taken into account. Specifically, due to the existence of many simultaneous traffic flows, the removal of a single, highly or moderately connected node can cause large scale cascading failures. This domino effect results in the interruption of traffic flow, service, and distribution of network resources. Thus, the vulnerability and reliability of SFNs in the face of attacks must be investigated.

The notion of survivability is an essential aspect of reliable communications. Survivability consists of the ability of the network to continue to deliver and preserve essential services in the presence of failures. These failures can occur due to natural faults and other unintentional errors or due to malicious adversaries. From the viewpoint of network resilience and survivability, a key question is whether a SFN can, in the face of dependent and correlated node failures, retain its functionality in terms of maintaining some sense of global communication. In this regard, traffic redistribution and robustness of routing policies for SFNs is a central problem which is gaining increased attention with a growing awareness to safeguard critical infrastructure networks.

A. Related Work and Motivations

Over the years, researchers have investigated the cascade based attack vulnerability of either specific infrastructure SFNs, such as the power grid [2], [3], or that of general SFNs with heterogeneous traffic load distributions [4], [5], [6]. In these works, different cascading failure models are analyzed to determine the best manner in which traffic load should be redistributed to maintain service. With advances in cyber based communication systems and their logical coupling to infrastructure networks [7], it is imperative that the vulnerabilities and consequences of node failures are studied from the perspective of network survivability [8], [9]. Survivability of networks depends on three key capabilities: resistance, recognition, and recovery [10]. While resistance repels failures from happening, recognition and recovery deal with and evaluate the failures to provide network restoration protocols. Thus far, the research on providing survivable network solutions to infrastructure networks has been tailored to focus on failure modeling and vulnerability assessments rather than network management [11], [12]. It is important not only to understand how to recognize faults and vulnerabilities but also how to recover from them.

Multipath routing has long been recognized as an effective strategy to increase reliability. To improve the transmission reliability, the multiple paths can be selected to be node disjoint. Disjoint multipath routing provides better robustness and a greater degree of fault tolerance than compared to the generic multipath routing scheme. Due to these advantages, disjoint multipath routing has been researched in order to enhance network survivability [13], [14].

SFNs are inherently highly connected, thus there always exists two or more paths between each source-destination pair. When a node fails in a SFN, potentially causing a cascade of node failures, the traffic flows that use the failed node should be maintained and the services they provide must be sustained. The aim of this paper is to ensure end to end survivability by bypassing failed nodes using efficient, robust multipath routing in the presence of cascading failures, while redistributing the corresponding traffic loads accordingly.

B. Contributions and Organization

The contributions of this paper are two-fold. First, we develop a local traffic redistribution model for a failed node by redistributing its load uniformly among its neighbors, taking into consideration that this redistribution can possibly overload the neighboring nodes, causing a series of cascading failures. Second, given the redistribution of the load, we establish survivable shortest disjoint multipath routes that bypass the failed node(s). The shortest disjoint paths are determined by the priority of the traffic flows; some flows, due to its service requirements, require backup paths that are more reliable than others (i.e., to ensure service availability). Therefore, the backup path for each traffic flow should be determined using local topological and connection information. In other words, the shortest paths for increasing traffic flow priority are those between a source and destination that cumulatively traverse the least number of highly connected nodes.

The rest of this paper is organized as follows: Section II discusses the system model. Section III discusses the load redistribution model based on cascading failures and Section IV develops the disjoint multipath route selection procedure based on traffic priority. We show our performance analysis using simulations in Section V and conclude the paper in Section VI.

II. System Model

The topology used in this paper is that of a SFN. The Barabasi-Albert (BA) model is used to generate SFNs with a power law degree distribution. The BA model is a well known algorithm for generating random SFNs using a preferential attachment mechanism [15]. Without loss of generality, for the purposes of this work, we construct the underlying network structure using the BA network model.

We consider a SFN consisting of N nodes ($n = 1, ..., N$) and A directed arcs ($a = 1, ..., A$). We assume that there are K ($k = 1, ..., K$) different traffic flows that are routed through the SFN, where a traffic flow is defined as a set of demands from a source to destination. Each traffic flow has a level of service that has to be maintained, therefore a certain amount of capacity is required along each arc of the route taken by a traffic flow, k. Within these K traffic flows, there are M classes of priority numbered from 0 to $M-1$, where Class 0 represents the highest class and $M-1$ represents the lowest class. Because highly connected nodes in a SFN are more vulnerable to outside attack, it is critical that high priority traffic flows route along paths that contain the least number of highly connected nodes to ensure end to end route survivability.

A manner in which node connectivity is measured is by the betweenness centrality (BC) parameter of SFNs. The BC is a measure of the number of shortest paths that go through a node n [1]. Nodes that occur on many shortest paths have higher betweenness than those that do not and are therefore more vulnerable to a coordinated attack. The BC of a node is denoted as

$$BC(n) = \sum \frac{\delta_n(p,q)}{\delta(p,q)} \tag{1}$$

where $\delta_n(p,q)$ is the number of shortest paths between nodes p and q and $\delta_n(p,q)$ is the number of shortest paths between p and q that run through node n. The BC parameter provides information about the physical connectivity of each node for the purposes of routing.

For the purpose of modeling network node failures, the actual traffic load of a node (the amount of traffic that each node processes) must be considered. The traffic load of a node is directly related to its BC; the higher the BC, the higher the traffic load that the node has to support. In this paper we assume that highly connected nodes are more susceptible to attacks than those that are not highly connected. Therefore, our proposed cascading failure model and routing algorithm are developed under the scenario that a highly connected node has failed and has caused a series of cascading failures.

III. Cascading Failure Model: Local Redistribution of Failure Load

Each source-destination pair in a SFN has an active path. This is the path on which a traffic flow is typically routed. Active paths often run through highly connected nodes and are thus exposed to attacks. In order to find active paths on a shortest path basis, a cost is defined, κ_a, of an arc a as

$$\kappa_a^m = \frac{m}{M-1} d_a + \frac{(M-1)-m}{M-1} BC(n) \tag{2}$$

where m is the current class of traffic flow, $m = 0, 1, 2, ..., M-1$, d_a is the length of arc a, and $BC(n)$ is the betweenness centrality parameter.

The active paths that are determined with the above cost are used as the default routing connection. However, when a node fails, the path that uses this node and its load has to be redistributed. The redistribution of the load may cause further node failures due to overload. Fig. 1 illustrates an example of a failed node's traffic being redistributed to its neighbors. Note that SFNs are always at least 2-connected, meaning that each node will have at least two disjoint paths to every other node in the network [16]. Not all the connections for each node to show 2-connectivity are shown in Fig. 1. The network of Fig. 1 is simply for illustration of the load redistribution concept.

Within a SFN, we assume that every node has a minimum load value, L_{min} and a maximum value, L_{max}. All nodes have

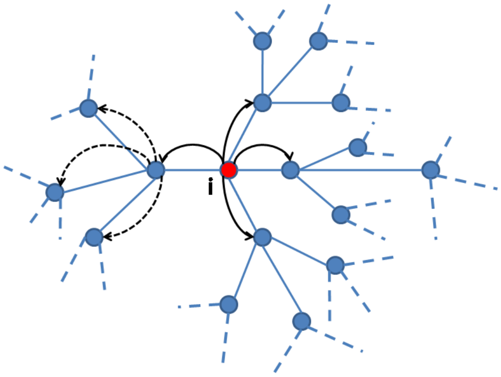

Fig. 1. Illustrates the load redistribution triggered by the failure of node i due to a coordinated attack. Node i is removed and its load is redistributed to the neighboring nodes

the same limit of operation, L_{fail}, beyond which they fail. To start the cascade, an initial disturbance causes the failure of a node. The algorithm for simulating the cascading failures proceeds in successive stages as shown in Fig. 2.

Cascading Failure Model

Step1: At stage $i = 0$, all N nodes are initially working under independent uniformly random initial loads $L_1, L_2, ..., L_N \; \forall \; [L_{min}, L_{max}]$, with $L_{max} < L_{fail}$.

Step2: An initial disturbance, causes a node to fail. This initial disturbance can either be a direct attack on the node itself or an overload.

Step3: The nodes' loads are incremented taking into account the neighboring topology of the failed node. Given that a node n has failed, $L*_n > L_{fail}$, its load $L*_n$ is spread uniformly among its neighbors. Each neighbor receives $\frac{L*_n}{d_n}$ portion of the load where d_n is the degree of the failed node. That is the total load of the failed node n is divided by the number of nodes to which node n is connected to in order to determine the amount of load each neighbor is incremented with.

Step4: If the neighborhood of the failed node is empty (i.e., if there are no functioning nodes connected to it), then the failure propagation comes to an end.

Fig. 2. Steps to model cascading failures given an initial disturbance

IV. Disjoint Multipath Survivable Routing under Cascading Failures

Once load is redistributed, the new topology configuration has to be considered when shortest paths are determined for each source-destination pair. When a node fails, the traffic flows that traverse that node need to be routed on alternate shortest paths that are disjoint from the original active paths. These backup paths allow for redistribution of end to end routing between nodes. The backup paths are determined based on the priority of the traffic flow. In this paper, our objective is to protect infrastructure networks against coordinated attacks on highly connected nodes. Therefore, high priority traffic must traverse the least number of highly connected nodes. This can deliver backup paths that are longer in length than other possible paths. Low priority traffic, if link capacities allow, can use backup paths with shortest hops as long as they are not taking away resources for high priority traffic. We formulate the discovery of backup paths as an integer linear program (ILP). We assume that a series of cascading failures does not partition the network, meaning that there will always exist at least one path between each pair of nodes in the network. The nomenclature used in the ILP formulation is shown in Table I.

TABLE I
Nomenclature Used in ILP

p_k - source node of a traffic flow k
q_k - destination node of a traffic flow k
λ_a - number of available channels on arc a
$\alpha^{\lambda}_{k,a}$ - takes value of 1 if channel λ of an arc a is used by an active path of traffic flow k; 0 otherwise
$\beta^{\lambda}_{k,a}$ - takes values of 1 is channel λ of an arc a is used by a backup path of traffic flow k; 0 otherwise
κ^m_a - cost of arc a (shown in Eq. 2)
$s_{k,a}$ - cost of an arc a calculated for traffic flow k on the backup path
C_a - capacity of an arc a
x - vector of all components of flows (variables)

Before developing the ILP, two boundary cases are worth mentioning. For Class 0, the highest priority class of traffic flow, the cost of an arc is calculated only on the basis of the $BC(n)$. This can be seen from Eq. 2. This results in finding backup paths that omit highly connected nodes. This causes the backup connections of Class 0 traffic to have a low probability of breaking. However, the backup paths may not be the shortest ones. For Class $M - 1$, the lowest priority traffic flow, the backup connections do not have to be guaranteed service continuity. For these flows, the cost of each arc is determined solely by the length of the arc, d_a. For all other classes of traffic flows, the cost of the arcs are determined using Eq. 2.

The ILP shown below finds backup paths while minimizing the linear cost of the paths.

Objective Function

$$\varphi(x) = \text{minimize} \quad \sum_{k=1}^{K} \sum_{a=1}^{A} \sum_{\lambda=1}^{\lambda_a} (\kappa^m_a \cdot \alpha^{\lambda}_{k,a} + s_{k,a} \cdot \beta^{\lambda}_{k,a}) \quad (3)$$

subject to the following constraints

a) Capacity constraints on the number of available channels on an arc a

$$\sum_{\lambda=1}^{\lambda_a} \sum_{k=1}^{K} (\alpha^{\lambda}_{k,a} + \beta^{\lambda}_{k,a}) \leq C_a, \forall a \in A \quad (4)$$

b) Flow balance constraints for each channel λ and for each demand k

For a source node of an active path

$$\sum_{a=(q_k,j),j\neq q_k} \alpha_{k,a}^{\lambda} - \sum_{a=(i,p_k),i\neq p_k} \alpha_{k,a}^{\lambda} = 1, \qquad \forall i,j \in N, \forall k \in K, \forall a \in A, \forall \lambda \in \lambda_a \tag{5}$$

For a destination node of an active path

$$\sum_{a=(q_k,j),j\neq q_k} \alpha_{k,a}^{\lambda} - \sum_{a=(i,p_k),i\neq p_k} \alpha_{k,a}^{\lambda} = -1, \qquad \forall i,j \in N, \forall k \in K, \forall a \in A, \forall \lambda \in \lambda_a \tag{6}$$

For intermediate nodes of an active path

$$\sum_{a=(i,j),i,j\neq q_k,i,j\neq p_k} \alpha_{k,a}^{\lambda} - \sum_{a=(i,j),i,j\neq q_k,i,j\neq p_k} \alpha_{k,a}^{\lambda} = 0, \qquad \forall i,j \in N, \forall k \in K, \forall a \in A, \forall \lambda \in \lambda_a \tag{7}$$

For a source node of a backup path

$$\sum_{a=(q_k,j),j\neq q_k} \beta_{k,a}^{\lambda} - \sum_{a=(i,p_k),i\neq p_k} \beta_{k,a}^{\lambda} = 1, \qquad \forall i,j \in N, \forall k \in K, \forall a \in A, \forall \lambda \in \lambda_a \tag{8}$$

For a destination node of a backup path

$$\sum_{a=(q_k,j),j\neq q_k} \beta_{k,a}^{\lambda} - \sum_{a=(i,p_k),i\neq p_k} \beta_{k,a}^{\lambda} = -1, \qquad \forall i,j \in N, \forall k \in K, \forall a \in A, \forall \lambda \in \lambda_a \tag{9}$$

For intermediate nodes of a backup path

$$\sum_{a=(i,j),i,j\neq q_k,i,j\neq p_k} \beta_{k,a}^{\lambda} - \sum_{a=(i,j),i,j\neq q_k,i,j\neq p_k} \beta_{k,a}^{\lambda} = 0, \qquad \forall i,j \in N, \forall k \in K, \forall a \in A, \forall \lambda \in \lambda_a \tag{10}$$

c) Constraints to ensure node disjointness of active and backup paths.

$$\sum_{\lambda=1}^{\lambda_a} \sum_{a=(i,j),j\neq i,i\neq p_k} (\alpha_{k,a}^{\lambda} + \beta_{k,a}^{\lambda}) \leq 1, \qquad \forall i,j \in N, \forall a \in A, \forall k \in K \tag{11}$$

$$\sum_{\lambda=1}^{\lambda_a} \sum_{a=(i,j),j\neq i,j\neq p_k} (\alpha_{k,a}^{\lambda} + \beta_{k,a}^{\lambda}) \leq 1, \qquad \forall i,j \in N, \forall a \in A, \forall k \in K \tag{12}$$

The constraint given in Eq. 4, assures that the total number of channels, reserved for survivable connections on an arc a, will not exceed the capacity of this arc. For each channel and each demand, flow balance for the active paths is assured by Eqs. 5-7. Eq. 7 simply states that the intermediate nodes do not store traffic. Eqs. 8-10 describe the flow balance constraints for backup paths. Eqs. 11 and 12 reflect the requirement that the active and backup paths be node disjoint.

V. Performance Evaluation

In this section, we evaluate the performance of our cascading failure model and end to end survivable routing algorithm via simulations. We consider a SFN generated by the BA model [15] and compare it to a random graph generated by the algorithm given in [17]. For fairness, the number of nodes and number of links in both are randomly set to be 1470 and 3131, respectively. The number of nodes and links chosen generate networks that are at least two connected to ensure disjoint paths can be obtained for each node in the face of a cascading failure. The BA model follows the power law degree distribution, while the degree distribution of a random graph is Poisson. Unlike a SFN, the random graph is a homogeneous network, in which there is no node with an enormous number of connections. In each network, we randomly generate 4000 traffic flows (i.e., K=4000). The source and destination nodes for each flow are chosen randomly. Once a source-destination pair is chosen, a shortest path between them is determined using the cost metric given in Eq. 2. The capacity of the links in the network are determined by the traffic loads. Intuitively, links from highly connected nodes need larger capacity since more traffic loads go through them. Thus, the capacity of an arc (i, j) is given as

$$C_{ij} \propto BC(i) + BC(j) \tag{13}$$

where C_{ij} is the capacity of the arc, which is proportional to the sum of the betweenness of node i and node j. Comparing the definition of betweenness with the routing rule of the traffic flows, it can be concluded that the betweenness characterizes the average traffic load of a node [18]. In addition, each directed arc in the networks have 8 channels (i.e., $\lambda_a = 8$) available to them and are of equal length (i.e., d_a = 175km).

A. Simulation Results and Discussion: Cascading Failure Model

Given a network, to start a cascade, an initial disturbance is imposed on a node in the form of an extra load, D, which results in the failure of that node due to overload. This failure occurrence leads to the redistribution of the load to neighboring nodes, which may cause further failures. As the nodes become progressively more loaded, the cascade continues. The cascade propagation algorithm is embedded in a Monte Carlo simulation framework implemented in Matlab version 7.11.0. The damage caused by the cascades for any initial load, $[L_{min}, L_{max}]$, is quantified in terms of the number of nodes that have failed on average. This is referred to as the cascade size, S. It is assumed that each node operates in such a manner that the initial node loads are normalized between the range $L_{min} = 0$ to $L_{max} = L_{fail} = 1$. Large load values represent highly loaded nodes where each node is on average operating close to its limit capacity, $L_{fail} = 1$. The range of load conditions is normalized from 0 to 1 so that the model for cascading failures is not limited to the propagation of failures in specific applications. As the simulation is repeated for different ranges of initial load, $[L_{min}, L_{max}]$, with $L_{max} = 1$ and $L_{min} \in [0, 1]$ the pair (L, S) is recorded.

Fig. 3 portrays the effect of propagation of failure. The analysis is performed for values of D that span the entire feasibility range $D \in [0, 1]$. Eight different initial disturbance values are used $D \in [0.8, 0.6, 0.4, 0.2, 0.1, 0.01, 0.001, 0.0001]$. The results reflect the simulation of the generated SFN.

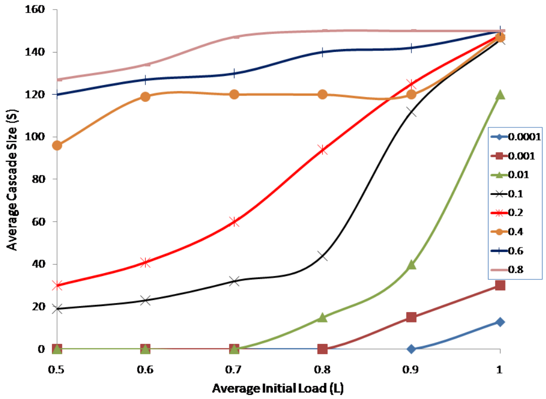

Fig. 3. Illustrates the average cascade size, S, versus the average initial load, L, for eight different values of the initial disturbance D. Each point is averaged for the same range of initial load $[L_{min}, L_{max}]$

From Fig. 3, it can be seen that a low D value causes almost no cascading failures, thus as D increases, the number of failures also increases. This intuitively makes sense since the value of D determines the strength of the disturbance.

B. Simulation Results and Discussion: Disjoint Multipath Survivable Routing Algorithm

To evaluate the performance of our disjoint multipath routing algorithm, we adopt the following performance metrics:

- Restoration time: restoration time is defined as the amount of time needed by the algorithm to construct an alternate path after the failure of a node.
- Bandwidth utilization ratio: the utilization ratio of the bandwidth is the total bandwidth used by the backup path to the total bandwidth provided (capacity) for different classes of traffic. This metric describes how well the backup paths use the bandwidth for different classes of traffic.

The routing algorithm was implemented using Matlab 7.11.0 and IBM's ILOG CPLEX optimizer. In these simulations we do not consider any route signalling mechanisms. We first look at the average restoration time of broken connections due to node failure as a function of the class of service. The results are shown in Fig. 4. We assume that there are 5 traffic classes, with Class 0 being the highest and Class 5 the lowest. The results shown were averaged over 10 simulation trials in which each trial has a different node failing, thereby causing a different cascading failure sequence and load distribution. It can be seen that the proposed multipath routing algorithm leads to a significant reduction in the restoration time for high traffic classes versus lower priority traffic. Thus, our routing algorithm efficiently takes into consideration the priority of the connection when constructing a backup path between a source-destination pair. Given the limited published research in routing for networks with cascading failures, the restoration time of our approach can not be compared at this time with existing fast recovery techniques.

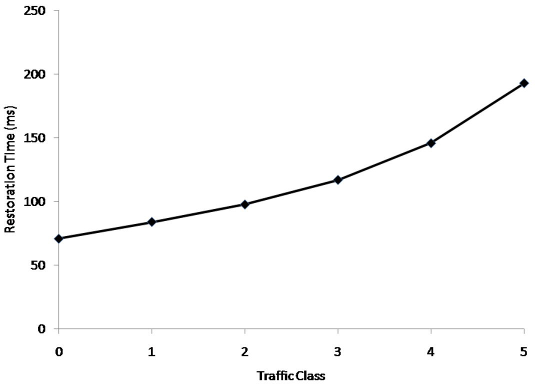

Fig. 4. Illustrates the average restoration time in milliseconds for 6 classes of traffic

We next look at the bandwidth utilization ratio for different classes of traffic versus the total capacity available. Fig. 5 shows the performance of the SFN network generated by the BA algorithm for a random failure and intentional failure (i.e., highly connected node removed) compared to the utilization for the original intact network for Class 0 traffic. The random attack curve in Fig. 5 overlaps with the original one, whereas the intentional attack curve is approximately 14% lower in terms of bandwidth utilization. The utilization ratio of the bandwidth decreases as the total capacity rises, which means that a higher percentage of bandwidth is wasted. The results obtained for Class 5 traffic are shown in Fig. 6. It can be seen that the bandwidth utilization for Class 5 traffic is higher than the Class 0 traffic results. This difference in utilization ratio results from the backup paths being longer for lower priority connections and therefore using more bandwidth. The results of both Figs. 5 and 6 indicate that the BA generated SFN is robust under random attack but fragile under intentional attack.

By contrast, Fig. 7 shows the results for a randomly generated graph. It can be seen that the random graph is robust to both random and intentional attacks; both curves perform similarly to the original curve. There is only a slight decline in utilization ratio when the network is intentionally attacked. Because the random graph is homogeneous, the traffic is well distributed among all the nodes. Therefore, the attack on one node (no matter randomly or intentionally) has little effect on the traffic performance of the whole network. Due to space limitations, only the results for Class 0 traffic are shown for the random graph. Similar results were obtained for lower traffic

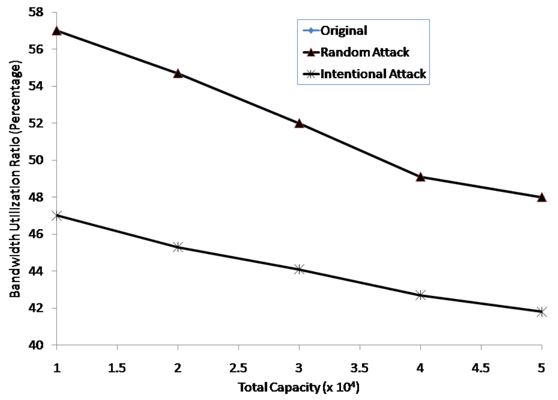

Fig. 5. Utilization ratio of the bandwidth in a BA generated SFN for Class 0 traffic (highest priority)

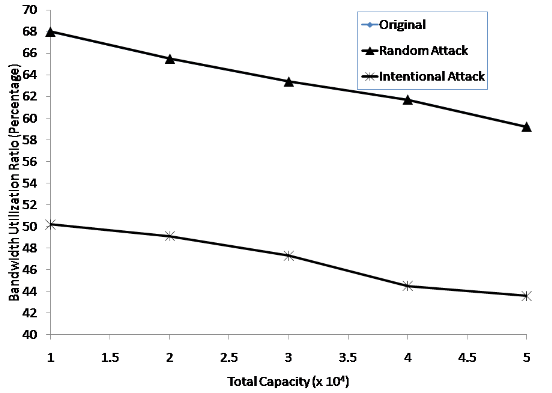

Fig. 6. Utilization ratio of the bandwidth in a BA generated SFN for Class 5 traffic (lowest priority)

classes.

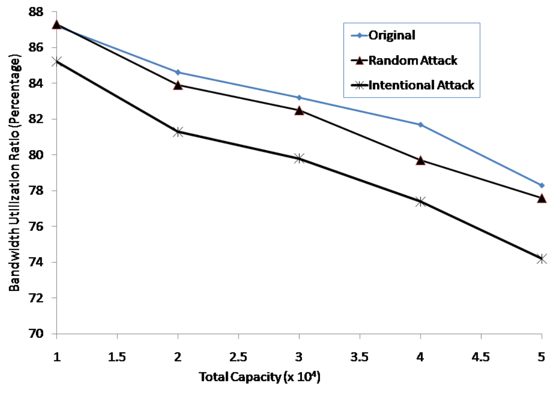

Fig. 7. Utilization ratio of the bandwidth in a randomly generated network for Class 0 traffic (highest priority)

VI. Conclusion

In this paper we have developed an end to end disjoint multipath survivable routing algorithm for SFNs in the presence of cascading node failures. We show that our algorithm effectively constructs alternate paths in a SFN considering the priority of the different traffic classes. We also show that our routing algorithm fares well when an intentional attack occurs. In our future work, we will look at improving the cascading failure model by redistributing load onto neighboring nodes based on the capacity of the nodes rather than using a uniform distribution. We will also introduce resource allocation mechanisms into the cascading failure routing scheme.

Acknowledgement

This work was funded by the Research Initiation Program (RIP) at the Naval Postgraduate School, Monterey, CA, USA.

References

[1] A. Laszlo and E. Bonabeau, “Scale free networks,” *Scientific American*, pp. 50–59, May 2003.

[2] I. Dobson, B.A. Carreras, V.E. Lynch, and D.E. Newman, “Complex systems analysis of series of blackouts: Cascading failure, critical points and self-organization,” *Chaos, American Institute of Physics*, vol. 17, no. 2, pp. 1–13, June 2007.

[3] J.-W. Wang and L.-L. Rong, “Cascade-based attack vulnerability on the US power grid,” *Safety Science (Elsevier)*, vol. 47, no. 10, pp. 1332–1336, December 2009.

[4] H.J. Sun, H. Zhao, and J.J. Wu, “A robust matching model of capacity to defense cascading failure on complex networks,” *Physica A (Elsevier)*, vol. 387, no. 25, pp. 6431–6435, November 2008.

[5] X. Wang, S. Guan, and C.H. Lai, “Protecting infrastructure networks from cost-based attacks,” *New Journal of Physics*, vol. 11, no. 3, pp. 1–9, March 2009.

[6] J.-W. Wang and L.-L. Rong, “A model for cascading failures in scale-free networks with a breakdown probability,” *Physica A (Elsevier)*, vol. 388, no. 7, pp. 1289–1298, April 2009.

[7] J. Kopylec, A. D’Amico, and J. Goodall, *Visualizing Cascading Failures in Critical Cyber Infrastructures*, Springer, 2007.

[8] R. Zimmerman, “Decision-making and the vulnerability of interdependent critical infrastructure,” in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, 2004, pp. 4059–4063.

[9] R. Zimmerman and C. Restrepo, “The next step: Quantifying infrastructure interdependencies to improve security,” *International Journal of Critical Infrastructures*, vol. 2, no. 23, pp. 215–230, February 2006.

[10] “Survivable mobile wireless networks: Issues, challenges, and research directions,” in *Proceedings of ACM Workshop on Wireless Security*, 2002, pp. 31–40.

[11] Y.Y. Haimes, B.M. Horowitz, J.H. Lambert, J.R. Santos, C. Lian, and K.G. Crowther, “Inoperability inputoutput model for interdependent infrastructure sectors,” *Journal of Infrastructure Systems*, vol. 11, pp. 67–709, June 2005.

[12] Y. Xia and D.J. Hill, “Attack vulnerability of complex communication networks,” *IEEE Transactions on Circuits and Systmes-II: Express Briefs*, vol. 55, no. 1, pp. 65–69, January 2008.

[13] X. Huang and Y. Fang, “Multiconstrained qos multipath routing in wireless sensor networks,” *Wireless Networks*, vol. 14, no. 4, pp. 465–478, 2008.

[14] P. Thulasiraman, J. Chen, and X. Shen, “Multipath routing and max-min fair qos provisioning under interference constraints in wireless multihop networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 716–728, 2011.

[15] A.-L. Barabasi and R. Albert, “Emergence of scaling in random networks,” *Science*, vol. 286, no. 5439, pp. 509–512, October 1999.

[16] P. Thulasiraman, S. Ramasubramanian, and M. Krunz, “Disjoint multipath routing to two distinct drains in a multi-drain sensor network,” in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2007, pp. 643–651.

[17] P. Erdos and A. Renyi, “On the evolution of randome graphs,” in *Mathematical Institute of Hungarian Academy of Sciences*, 1960, pp. 17–60.

[18] K.-I Goh, B. Kahng, and D. Kim, “Universal behavior of load distribution in scale free networks,” *Physical Review Letters*, vol. 87, no. 27, pp. 278–281, December 2001.