Resiliency Assessment of the Global Internet Infrastructure System

Mayada Omer Roshanak Nilchiani Ali Mostashari

m.omer@stevens.edu roshanak.nilchiani@stevens.edu ali.mostashari@stevens.edu

Center for Complex Adaptive Sociotechnological Systems (COMPASS)
Stevens Institute of Technology
Castle Point on Hudson,
Hoboken NJ 07030-5991
USA

Abstract. Resilience is the ability of the system to both absorb shock as well to recover rapidly from a disruption so that it can return back to its original service delivery levels or close to it. Recent manmade and natural disasters such as 9/11 incident and Hurricane Katrina have introduced an increasing interest in infrastructure resilience. The global submarine fiber optics cable network that serves as the backbone of the internet is a particularly critical infrastructure system that is vulnerable to both natural and man-made disasters. In this paper, we propose a model to measure the base resiliency of this global network, and explore the node to node and global resiliency of the network using existing data demand, capacity and flow information. The base resiliency of the system can be measured as the value delivery of the system after a disruption to the value deliver of the system before a disruption. We further demonstrate how the resiliency of the global internet infrastructure is enhanced through reducing the network vulnerability and increasing its adaptive capacity.

Introduction

In the aftermath of 9/11 and hurricane Katrina, the ability of Infrastructure systems to withstand the impact of natural and man-made disruptions is a topic of increasing interest to decision-makers (John A. McCarthy, 2007). In particular with regards to the global internet infrastructure, the Asian tsunami of 2006 (Yasuichi Kitamura et al., 2007) and the Middle East and South Asia internet outage of 2008 (International Herald Tribune, 2006) have highlighted the need for incorporating resiliency into the global submarine cable infrastructure to prevent the loss of billions of dollars of global information flow. We define resiliency as the ability of the system to both absorb shock as well to recover rapidly from a disruption. The concept of resiliency is also closely entangled with vulnerabilities that exists in a system and also the amount of adaptive capacity that the system has in face of major shocks. Therefore, incorporating resiliency into any infrastructure system does not only makes the infrastructure less susceptible to disruptions, more ready to recover, but also reduces the wider impact on socioeconomic continuity and security.

In this paper, first we begin by looking at the vulnerability of the Global Submarine Cable Infrastructure and its node-to-node and network resiliency in the face of major natural and man-made disasters. Resiliency is measured through the identification of the most vulnerable point in the network, and evaluation of the losses in terms of resiliency. Then we propose a

methodology and a network model that can also be used to measure the resiliency of the global submarine cable through vulnerability reduction and through increasing the adaptive capacity of the system. This resiliency model can also be used for other types of networked infrastructures, since a large number of key infrastructures such as telecommunications, transportation, electric power grids, and water supply systems are network based. Next, the results of the model and the case study are presented and discussed. The paper is concluded by limitations and future research direction suggestions.

Literature Review

The concept of resiliency in capsules many different topics ranging from Ecology to child psychology and psychiatry to engineering systems (Simoncini, L. 2007). In Ecology it is defined as the process of moving from one stable domain to another in which the system develops evolution tolerance. In psychiatry, it is process by which individual learns how to be more resilient to future situations. In material science it is the capacity of a material to absorb energy when it is elastically deformed. In engineering, one definition of resiliency is the ability of the system to return to a stable state after a perturbation. A resilient system has also be been defined as a system that will return to an equilibrium state, more resilient systems have multiple equilibrium points. Burneau et al. (2003) define a resilient system to have reduced failure probability, reduced consequences from failure and reduced time to recover (Fiksel, J. 2003).

Dalziell et al. (2004) define resiliency to be composed of two elements; these are vulnerability and adaptive capacity. They define vulnerability to be the ease by which an individual or an organization move from one stability equilibrium to another, while adaptive capacity is the degree to which they are able to cope with that change.

There have been a substantial number of studies focused on defining the concept of resiliency for infrastructures and the quantification of resiliency metrics. Little (2002) looks into the types of failures that could occur due to interdependencies between infrastructures. Little also suggests that complex adaptive system models may provide an understanding of the events that occur and how to react when a disruption occurs.

In Networked Infrastructures, Burneau et al. (2007) proposed a metric for measuring resiliency that measures the size of expected degradation in the quality of an infrastructure and identified robustness, redundancy, resourcefulness and rapidity to be properties of a resilient system. Garbin and Shortle (2007) outline an approach by which to quantative measure the resilience of the network. The proposed resiliency metrics are the percentage of links damaged versus the network performance and the percentage of nodes damaged versus the network performance, they also emphasize the concept of shared risk group when measuring network resiliency. Studies by Soo Kim et al. (2006) have also shown that the resiliency of a network is improved by changing the network topology.

However there are very few studies that have focused on the resiliency and vulnerability of the global sub-marine infrastructure system as a whole, looking at the vulnerability of the physical infrastructure enabling the internet.

Threats and Vulnerabilities in the Global Submarine Cable Infrastructure

Problem Definition

Internet traffic has become a part of everyday telecommunication and undersea cable systems are increasingly becoming the most favored solution for information transfer across the oceans, the demand for the fiber optic cables has been increasing continuously over the past few decades. Fiber optic cables are considered as a very reliable and secure means of data transfer as they are harder to eavesdrop than satellites. In addition to that, fiber optic cables can be easily installed and upgraded. The Global Submarine Cable Infrastructure is made up of fiber optic cables that lie on the ocean floor, supporting a continuously increasing demand for internet data traffic.

However disruptions to the global fiber optic network could result in significant commercial damage (Insurance and Technology, 2008). Since the optical fibers lie on the ocean floor, they are vulnerable to damages caused by humans and nature. There are many causes for damage to fiber optic cables. The most common cause is the damage caused by anchors dropped by ships, as recently highlighted by a major outage due to this cause in the Persian Gulf in 2008 (Fox News, 2008). Additionally, natural disasters can also damage fiber optic cables. The earthquake in Taiwan in 2006 caused significant damages to the Asia Pacific undersea cables (Kitamura et al. 2007). Dredging fishing nets have also been reported to cause cable damages. Undersea life itself poses a threat to the cable systems as fish often eat their way through a fiber optic cable, AT& T suffered from crocodile shark damages on their first deep sea submarine cables between the Canary Islands in 1985 (Marra, 1989). Faulty equipment is another factor that could result in a disruption.

Given all the information and facts on vulnerabilities of the underwater fiber optic internet infrastructure systems, there is a critical need for creating resiliency in this infrastructure system which in turn creates a need for measures and metrics of resiliency in this infrastructure system and also a network model of this infrastructure system. By creating this model, hypothetical disruptions can be introduced in the infrastructure system and the effect of disruption can be studied. By network modeling of this infrastructure system in combination with resiliency metric, we can provide the opportunity for the stakeholders to look at different resiliency improvement strategies and measure and compare the effectiveness and value of several solutions to the resiliency of the system.

Network Model of Resiliency in the Global Submarine Cable System

There are several view points of the global submarine infrastructure; one view point is the physical network that makes up the infrastructure which shows the details of the physical connections between the regions. We can also look at the logical network where the world regions make up the nodes of the network and the connections are the links. The following sections describe the physical and logical networks of the internet infrastructure in more detail.

Physical Network of the Submarine Cable Map

Currently, there are more than 70 submarine cable systems; this number is on the increase as the demand is still increasing. The cable systems have different capacities depending on the regions that they are connecting. The cable system Apollo, which connects North America to Europe has a capacity of 1400 Gbps is considered the biggest. The fiber optic cables also known as optical fibers are made up of a glass fiber core that is covered in Cladding; a layer of buffer coating covers the coating to protect the fiber from damage and moisture. The information travels down the length of the glass fiber by total internal reflection. The cables are terminated by landing stations that pass the signal from the cable to the terrestrial system at each end. Several repeaters are used along the length of the cable to boost and correct the signal. The physical submarine cable map by Telegeography is shown in Figure 1 (Telegeography, 2009).

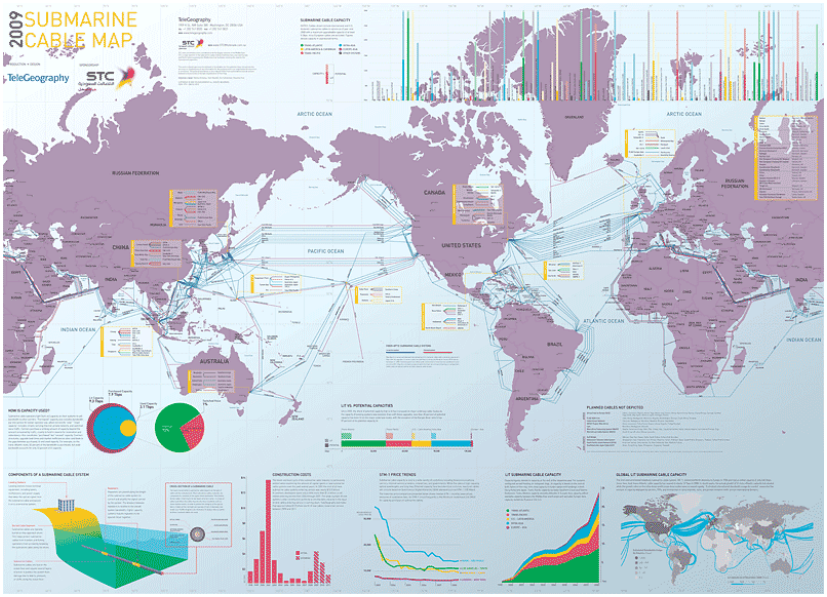

Figure 1. 2008 Submarine Cable Map

(will change to 2009 map)

Logical Network of the Submarine Cable Map

In order to model the resiliency of the global submarine fiber optics cable network, we will address it as a logical network made up of nodes (geographic regions) connected by links (the fiber optic cables). The network used for the model development is based on the actual 2008 submarine cable map Figure 1 shows the physical connections between the world continents.

Figure 2 (Telegeography, 2008) and Figure 3 show the global submarine cable infrastructure as a physical and as a logical Network. Table 1 contains the link capacities.

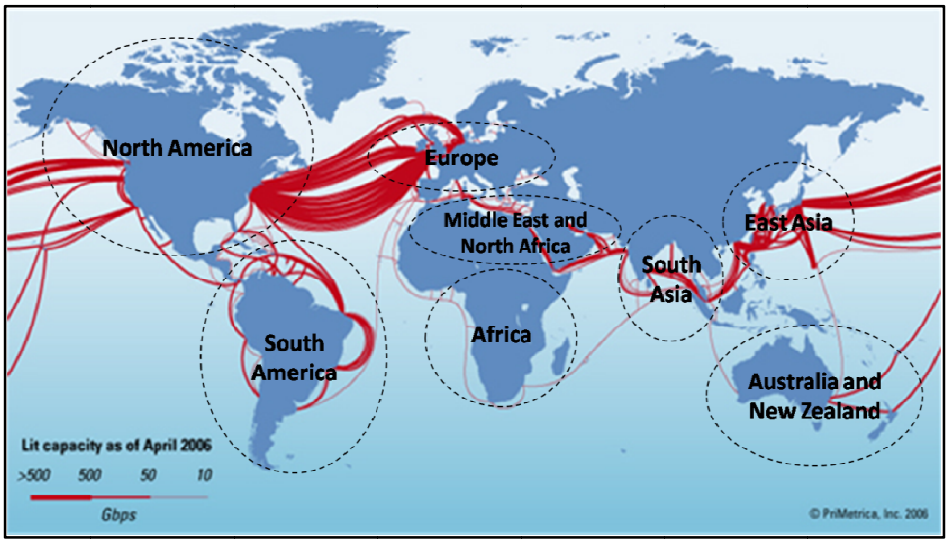

Figure 2. Physical Network of the Global Submarine Cable System

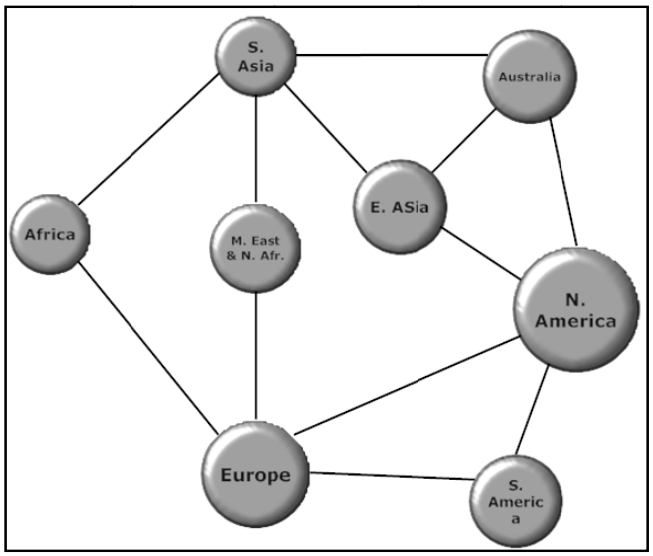

Figure 3. Logical Network of the Global Submarine Cable System

Base Resiliency calculation

We define the *base resiliency* of the network as the ratio of the value delivery of the network after a disruption to the value delivery of the network before a disruption. This is shown in Equation 1.

$$Res_{network} = \frac{V_{init} - V_{loss}}{V_{init}} \quad (1)$$

The initial value delivery of the internet network V_{init} is the total amount of information that needs to be carried through network. The loss in value delivery V_{loss} is the information loss as a result of cable damages.

The *node to node resiliency* is the ratio of the value delivery between the two nodes after a disruption to the value delivery between the two nodes before a disruption. The node to node resiliency measured is shown in Equation 2.

$$Res_{node} = \frac{V_{init\_node} - V_{loss\_node}}{V_{init\_node}} \quad (2)$$

Where V_{init_node} is the total demand of the node and V_{loss_node} is the total information loss taking into consideration the information routed by the extra network capacities.

Using these resiliency measures, we can evaluate the damage when a link or a node is partially or completely down. We then look into different resiliency strategies that would minimize the losses caused by a disruption.

Formulating the Network Problem

In order to analytically quantify the network, three parameters have to be taken into consideration; the node demand, link capacity and traffic flow of the network.

The demand is the information in mega bytes per second that has to be transported from source to destination. The total demand of a node is the total information that needs to be carried through the network to the node. The total node demand is calculated based on the total number of people in any region using the internet and the average number of megabytes downloaded per person. Table 1 shows the demand figures for every region as calculated by the Internet World Stats (Internet World Stats, 2008).

Table 1. Demand Values

Region	No. People Using Internet	Mega bytes per day	Total Demand (MBps)
Africa	51,065,630	50.00	29,551.87
Middle East & N. Africa	41,939,200	70.00	33,978.52
South Asia	348,474,324	90.00	362,994.09
Europe	384,633,765	120.00	534,213.56
N. America	248,241,969	120.00	344,780.51
Australia	20,204,331	90.00	21,046.18
East Asia	230,063,933	90.00	239,649.93
South America	139,009,209	80.00	128,712.23

The links capacity information for the model is based on the figures provided by Telegeography for internet submarine cable capacities for 2006. The numbers are a close approximation of the current cable capacities. The link Capacity Information is shown in Table 2.

Table 2. Link Capacities

Link	Capacity (Gbps)
Africa - South Asia	150
Africa - Europe	120
Middle East & N. Africa – South Asia	410
Middle East & N. Africa - Europe	360
South Asia - Australia	160
South Asia - East Asia	5190
Europe - North America	19770
Europe - South America	160
North America - Australia	320
North America - East Asia	2760
North America - South America	1200
Australia - East Asia	640

The links in the network are both access links and backbone links, as they are used to connect source and sink nodes as well as a source or sink node to a network nodes. The capacity of the link is the collective capacity of the fiber optic cables that are between the two nodes, the capacity is also measured in mega bytes per second. In the real network, there may be more than one fiber optic cable systems between two nodes.

The traffic flow is determined by the demand and the link capacities, the traffic flow in the internet infrastructure is asymmetric as there are different upload and download rates for every region, for example a country in Africa might access websites hosted by the United States more than the other way around. For this reason, capacity allocation protocols are used for distributing the cable bandwidth between the IP traffic flows in both directions.

The flow through the links is determined by the demand of any one node from the rest of the nodes.

The problem can thus be formulated as a network optimization problem, where flow disruptions change the link flows limited by link capacities. Also the internet information traffic flow is asymmetric, since the upstream and downstream flows are not symmetric. For instance, North Africa downloads more content from North America than the reverse case. Therefore that needs to be taken into consideration when distributing the flow. Equation 3 shows the formulation of the network optimization using linear and mixed integer programming.

Max V_{init}

Subject to the constraints

$$\sum_{i=1}^{n} x_{ji} + s_i \leq D_i$$

$$x_{ij} + x_{ji} \leq \alpha_{ij} c_{ij} \qquad (3)$$

V_{init} is the total information through the network, x_{ij} is the flow going into node i from the node j, x_{ji} is the flow going out of node i to other nodes, n is the number of nodes connected to node I and D_i is the demand of node i and. s_i is a parameter used to measure the amount of

information lost when the capacity c_{ij} of any link is reduced. The capacity degradation is controlled by the coefficient α_{ij}

The value delivery between two nodes is the total amount of information that flow in the link connecting the two. Using the resiliency metric we can measure the resiliency when a link or a node is partially or completely down.

Using Equation 3, the total information loss when a link is down is calculated. We are able to determine the node to node resiliency of the network and the overall network resiliency using Equation 4.

$$V_{loss} = \sum_{i=1}^{k} s_i \qquad (4)$$

Where k is the total number of nodes and s_i is the coefficient that captures the amount of information lost due to a capacity reduction.

Network Resiliency

For the overall network resiliency, the value delivery is the total information flow in the network. The resiliency is measured by Equation 1.

$$Res_{network} = \frac{V_{init} - V_{loss}}{V_{init}}$$

Node to Node Resiliency

The node to node resiliency is the resiliency between two nodes when the link between them is disrupted. It is measured as the ratio between total information flow between the nodes after a disruption to the total information between the nodes prior to a disruption. The node to node resiliency measured is shown in Equation 2.

$$\boldsymbol{Res_{node} = \frac{V_{init\_node} - V_{loss\_node}}{V_{init\_node}}}$$

Critical Link Identification

The vulnerability of the network is evaluated by identifying the links in the network that would lead to greater damage than others when disrupted.

Some links have a much bigger capacity than others and are more central to the network and are hence more critical. Identification of this link will enable us to identify the structural vulnerabilities of the network as enforcing these links would increase the whole system's resiliency. These links can be identified by gradual degradation of capacity; the critical links will result in the most value loss when their capacity is reduced. The link capacity in the network model is controlled by the coefficient α_{ij}.

Increasing Resilience through Usage of Other Links

When a cable cut occurs in the network, the remaining link capacity may not be sufficient for the whole flow. One vulnerability reduction strategy is to use the extra capacity of the other links in the network to transfer the information between the nodes when the link between them is down. The maximum flow theory is used to determine the maximum amount of information that can be transferred between the two nodes

The nature of the internet information traffic flow is asymmetric, since the upstream and downstream flows are not different. For instance, North Africa downloads more content from North America than the reverse case. The ratio of the flow from node i to node j and vice versa should be kept the same as the original ration when re-routing the information over the residual capacities of the network. The demand ratio is given by (6).

$$\beta_{ij} = \frac{x_{ij}}{x_{ij}+x_{ji}} \tag{6}$$

The maximum flow of the network is the sum of the information that is transferred in both directions Equation 7 and Equation 8 are used to determine the maximum flow from node i to node j and vice versa.

Max $\beta_{ij}V_{Loss}$
subject to:

$$\sum_{j=1}^{n} y_{ji-} \sum_{j=1}^{n} y_{ij} = \begin{cases} -\beta_{ij}V_{Loss} & for\ i = s \\ 0 & otherwise \\ \beta_{ij}V_{Loss} & for\ j = t \end{cases}$$

$$y_{ij} + y_{ji} \leq \beta_{ij} c\_res_{ij} \tag{7}$$

Where

$\beta_{ij}V_{Loss}$ is the total information that needs to be routed from node i to node j, y_{ij} is the flow from node i to other nodes connected to it, y_{ji} is the flow into node i, n is the total number of nodes connected to node i. c_res_{ij} is the residual capacity of the links, s is the source node and t is the destination node. β_{ij} is used to maintain the flow ratio in both directions. Equation (9) specifies i to be the source node and j to be the destination node and (10) ensures that the flow in any link does not exceed the allocated portion of the capacity.

Since β_{ij} is the ratio from node i to node j, the ratio γ_{ij} from node j to node is given by (8)

$$\gamma_{ij} = 1 - \beta_{ij} \tag{8}$$

Max $\gamma_{ij}V_{Loss}$
subject to:

$$\sum_{j=1}^{n} z_{ji-} \sum_{j=1}^{n} z_{ij} = \begin{cases} -\gamma_{ij}V_{Loss} & for\ i = s \\ 0 & otherwise \\ \gamma_{ij}\ V_{Loss} & for\ j = t \end{cases}$$

$$z_{ij} + z_{ji} \leq \gamma_{ij} c\_res_{ij} \tag{9}$$

The total information loss from node j to node i is $\gamma_{ij}\ V_{Loss}$, z_{ij} is the flow from node i to other nodes connected to it, z_{ji} is the flow into node i, n is the total number of links connected to node i. c_res_{ij} is the residual capacity of the links, s is the source node and t is the destination node.

Increasing Resilience through Adaptive Capacity

The adaptive capacity of the system is determined by the speed by which the system applies responses to problems. It is how fast the system can resume normal operation after a disruption. Typically, the system is repaired gradually over time. The adaptive capacity is measured over the length of time the system is still suffering from the disruption. That is, from the time the disruption occurs until full functionality has been recovered.

$$V_{init\_ac} = V_{init} \times t_{loss} \quad (9)$$

$$V_{loss\_ac} = \sum_{i=1}^{n} Vloss_i \times t_{loss\_level} \quad (10)$$

The initial value delivery of the system V_{init_ac} is calculated as the value delivery V_{init} multiplied by the number of days with reduced functionality t_{loss}. The loss in value delivery is calculated by summing up the product of the loss levels and the total time at that particular loss level where n is the number of time periods at a particular loss level. The system's base resiliency can then be measured by applying Equation (1)

Case Study Results

Using Equation 3, the demand and capacity data given in Table 1 and Table 2 were used to determine the system's resiliency under normal circumstances using, i.e. when the network links operate at 100% capacity. The results showed that the resiliency of the network has a value of 1 for all the links which indicates that all the links in the network are able to support the total demand. This also indicates that the node to node resiliency has a value of 1.

Disruptions on cables caused by undersea earthquakes, fish bites or ship anchors will result in a reduction in the capacity of the cable under attack, which in turn will result in a reduction of the overall link capacity. The effect of such a disruption is modeled by reducing the available link capacity using the coefficient α_{ij}. The capacity of each link, one link at a time, was reduced to 80% , in order to measure the impact of reducing the capacity of the individual links on the overall network resiliency. A resiliency enhancement strategy is to reduce the system's vulnerability; this could be done by fully utilizing the resources available by the network. Some of the links have residual capacities even after the node demands has been satisfied, these residual capacities can be used to re-route the information that would otherwise be lost. Equations 6 and 7 were used to re-route the information over the residual capacities of the other links in the network. Figure 4 shows a comparison of the resiliency values for each link when the lost information is routed over the residual capacities of the network links

The results show that reducing the capacity of the Middle East – South Asia link to 80%, reduces the network resiliency to 0.996, It can be seen from the graph that routing the information over residual capacities gives a network resiliency of 1, which means that all the information is being transferred from source to destination. The biggest impact on resiliency is made by the North America – South America link where the network resiliency is reduced to 0.992, rerouting the information increases the resiliency value to 0.997 which implies that some information will be lost even though a resiliency strategy has been deployed. The rest

of the links have little or no impact on the network resiliency as the remaining capacity of the links is able to handle the node demands.

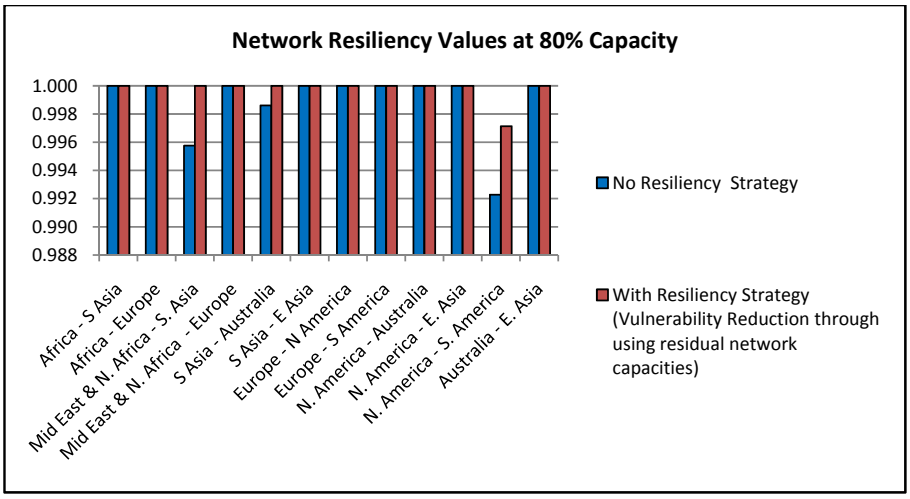

Figure 4. Network Resiliency at 80% link Capacity

The impact of using the residual capacities of the network on the network resiliency is more dramatic when a link capacity is completely disrupted, that is, it has a capacity of 0. The graph in Figure 5 shows the impact of a link at 0% capacity on the network resiliency when no resiliency strategy is used and when the lost information is re-routed over the residual network capacities.

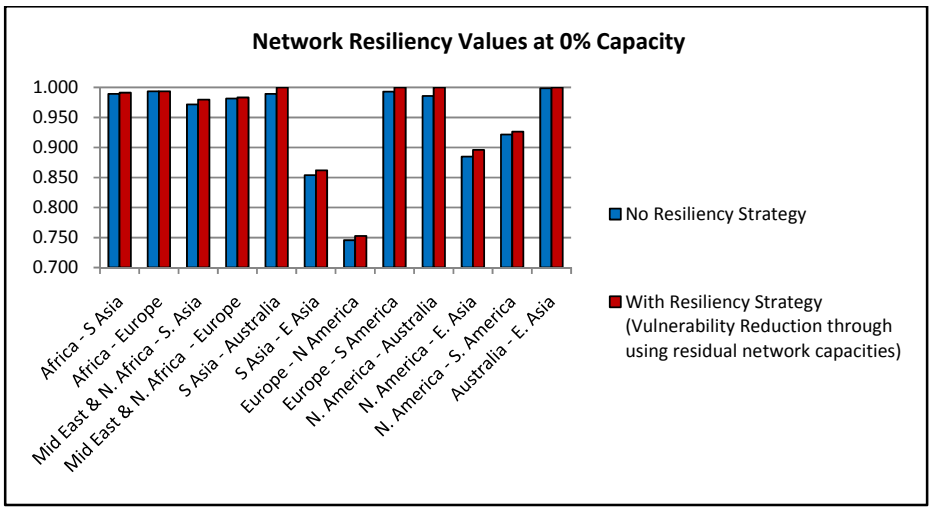

Figure 5. Network Resiliency at 0% link Capacity

It can be seen from figure 5 that reducing the Europe – North America link or South Asia – East Asia link capacity to 0 has a huge impact on the network resiliency. The re-routing capabilities of the network are only as good as the re-routing capability of the link with the least capacity. The addition of redundant capacities to the links that create these bottlenecks will result in a dramatic increase in the amount of information that the network is able to re-route which will in turn further improve the network resiliency. In addition to that, depending on the severity of the disruption, the amount of information loss could be beyond the re-routing capabilities of the network.

Figure 6 shows the *node to node resiliency* between East Asia – South Asia link when the link capacity is gradually reduced to 0% of the original network capacity. As previously mentioned, re-routing the information over the other links in the network has a very slight improvement in the node-to-node resiliency because the network does not have sufficient residual capacity. Node-to-node resiliency can be improved by adding redundant capacity to those links in the network that pose the biggest bottlenecks. The most critical links were identified to be the links connecting Australia to North America and Australia to South Asia. Doubling the capacity of those links had a big impact on the node-to-node resiliency values.

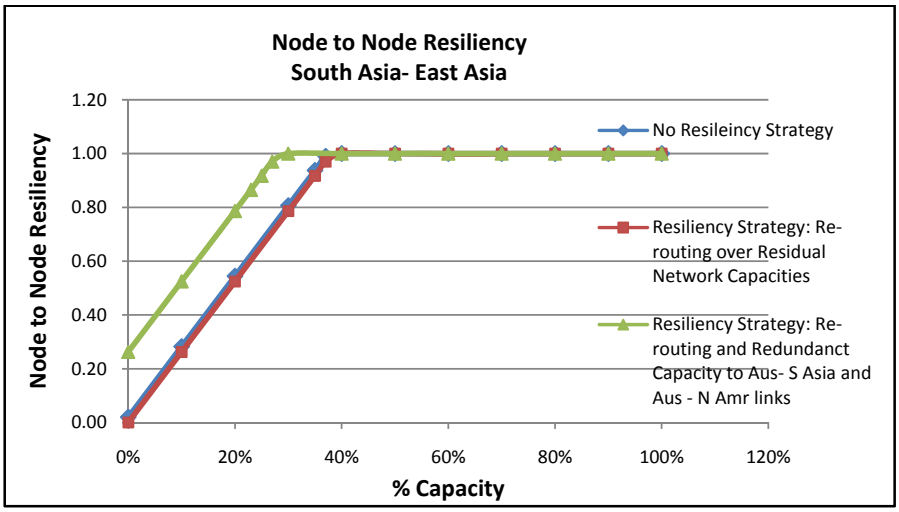

Figure 6. Node to Node Resiliency of South Asia – East Asia Link

Node-to-node resiliencies are different for every case. Figure 8 shows the node-to-node resiliency of Middle East & N. Africa – South Asia link. In this case, adding redundant capacity to the Middle East & North Africa – Europe link, which is a link in the re-routing path helps to maintain a resiliency value of one even if the link between Middle East & N. Africa –Europe link is completely destroyed.

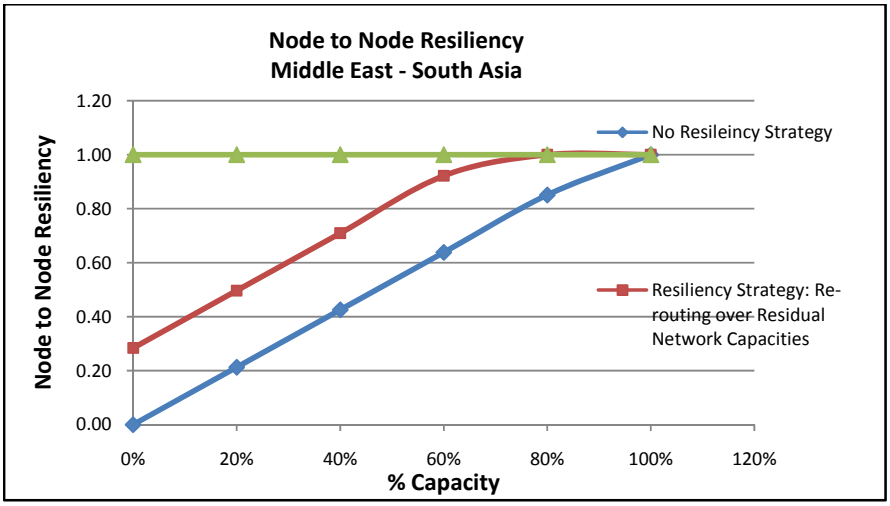

Figure 7. Node to Node Resiliency of Middle East & N. Africa – S. Asia Link

It often takes several days or even weeks to locate and repair a faulty cable, the longer the repair efforts take the lower the system's resiliency is. Figure 8 shows an example of an

initial disruption of 80% in the Middle East & North Africa – Europe link which causes the link capacity to drop down to 72Gbps, the graph shows a comparison of recovery speed, the first graph shows the repair being carried out gradually over the days until the full functionality is achieved by the end of day 7. Equations 9 and 10 the value delivery and the loss in value delivery in terms of adaptive capacity are used to calculate the resiliency, the resiliency for a slow repair is 0.62. The dotted line in Figure 8 shows that when full functionality is achieved by the end of the second day, the node to node resiliency over the same time has a value of 0.78. A speedy recovery has a positive impact on the resiliency value.

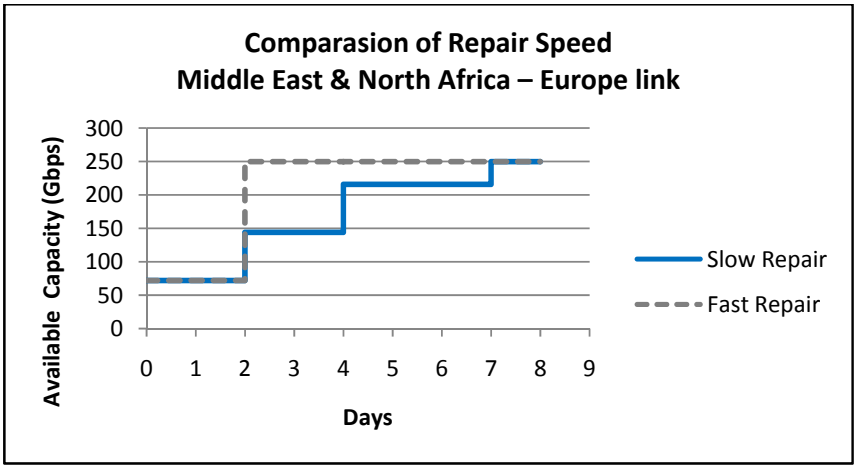

Figure 8. Comparison of Repair Speed

Conclusion and Future Research

Recent events such as the undersea cable disruptions near Alexandria (Egypt) in 2008 and the Asian Tsunami in 2006 have highlighted the vulnerability of the global undersea infrastructure. Analyzing and implementing resiliency into an infrastructure system is a way of mitigating the consequences of such disruptions as well as it prepares the infrastructure system in the face of these threats. Reducing the vulnerability of the system will improve the system's resiliency. Resiliency can be measured as the ratio of the value delivery of the system after a disruption to the value delivery before a disruption. The two aspects of network resiliency discussed in this paper are the base network resiliency and the node to node resiliency. In this paper, we propose a model for measuring the resiliency of networked infrastructure systems and showed that after the occurrence of a disruption, reducing the system's vulnerability through re-routing and redundant capacities will result in a more robust resilient infrastructure.

So far, we have looked into the network resiliency when a link is partially or fully disconnected. The next step of the research will investigate the impact of a node being partially disrupted and the impact of the disruption on the whole network. The research will also investigate the impact of the proposed vulnerability reduction strategies and other vulnerability reduction strategies such as parallel systems and new alternative routes and the additional cost for implementing these parallel strategies. The model can be used as a tool for decision makers to choose between the different resiliency strategies.

References

Ahuja, R. K., Magnanti, Thomas L., Orlin and James B. 1993. *Network Flows: Theory, Algorithms, and Applications.* New Jersey: Prentice Hall.

Anthony O'Donnell. 2008. Undersea Cable Failure Demonstrates Internet's Vulnerability**.** *Insurance and Technology*, March 05.
`http://www.insurancetech.com/distribution/showArticle.jhtml?articleID=206901887`

Barabási, A. 2003. *Linked: How Everything Is Connected to Everything Else and What It Means.* Cambridge: Plume.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., and von Winterfeldt, D. 2003. A framework to quantitatively assess and enhance the seismic resilience of communities, *Earthquake Spectra* 19 (4): 733–752.

Burneau , M. and Reinhorn, A. 2007. Exploring the concept of seismic resilience for acute care facilities. *Earthquake Spectra* 23(1): 41–62.

Cohen, R. Erez, K. and Ben-Avraham, D. 2001. Breakdown of the internet under intentional attack. *Physical Review Letters* 86(16): 3682-3685.
`http://ory.ph.biu.ac.il/~cohenr/publications/attack_prl.pdf`

Dalziell, E. and McManus, S. 2004. Resilience, vulnerability, and adaptive capacity: Implications for system properties. *Proceedings of the First International Forum on Engineering Decision Making*. Stoos, Switzerland.

Dolev, D. Jamin, S. Mokryn, O. and Shavitt, Y. 2006. Internet resiliency to attacks and failures under BGP policy routing. *Computer Networks: The International Journal of Computer and Telecommunications Networking* 50 (16): 3183-3196.
`http://portal.acm.org/citation.cfm?id=1225830.1225842`

Fiksel, J. 2003. Designing Resilient, Sustainable Systems. *Environmental Science and Technology* 37(23): 5330-5339

Garbin, D.A. and Shortle, J.F. 2007. Measuring Resilience in Network-Based Infrastructures. Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resiliency. Critical Infrastructure Protection Program. Discussion Paper Series.
`http://cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf`

Hibernia Atlantic, Submarine Cable Infrastructure
`http://www.hiberniaatlantic.com/pdf/MR1395appi.pdf`

Hoffman, J. and Nilchiani, R. 2008. Assessing Resilience in the US Energy Infrastructure. White Paper, COMPASS.
`http://www.socio-technical.org`

Internet World Stats
http://www.internetworldstats.com/stats.htm

McCarthy, J.A. 2007. Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resiliency. Critical Infrastructure Protection Program. Discussion Paper Series.

http://cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf

Kitamura,Y. Lee, Y. Sakiyama, R. and Okamura, K. 2007. Experience with restoration of Asia Pacific network failures from Taiwan earthquake. *IECE Transactions* E90-B(11): 3095-3103

Little, R. G.2002. Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems. *Proceedings of the 36th Hawaii International Conference on System Sciences.* -9

Marra, L.J. 1989. Sharkbite on the SL Submarine Lightwave Cable. *IEEE Journal of Oceanic Engineering* 14(3):230-237

Park, S. Khrabrov, A. Pennock, D. Lawrence, S. Giles, C.L. and Ungar, L.H. 2003. Static and dynamic analysis of the internet's susceptibility to faults and attacks. *In Proceedings of the IEEE INFOCOM* 3: 2144-2154.

Simoncini, L. 2007. Resilience for survivability in IST. Joint Workshop on Teaching Resilient Computing. Erlangen, Germany

http://resist.isti.cnr.it/JWTRC/slideshow/Simoncini.pdf

Soo Kim, Heejo Lee, WanYeon Lee. 2006. Improving Resiliency of Network Topology with Enhanced Evolving Strategies. *The Sixth IEEE International Conference on Computer and Information Technology CIT' 06.* 149-149

Telegeography Research
http://www.telegeography.com/maps/index.php

———. 2006. Asia slowly bounces back from one of region's biggest telecom outages. *International Herald Tribune*, December 28.
http://www.iht.com/articles/ap/2006/12/28/asia/AS_GEN_Asia_Telecom_Crisis.php

———. 2008. Third internet cable cut in Middle. *Fox News*, February 1.
http://www.foxnews.com/story/0,2933,327588,00.html

———. 2008. Undersea Cable Failure Demonstrates Internet's Vulnerability. Insurance and Technology. http://www.insurancetech.com/distribution/showArticle.jhtml?articleID=206901887

Biographies

Mayada Omer is a graduate student at the Stevens Institute of Technology pursuing a Ph.D. in Systems Engineering. Her current research is focused on Infrastructure Resiliency. She has work experience with Infineon Technologies where she worked first as an SRAM/ROM Development Engineer and later on as a Hardware Engineer for the Ferrari Formula 1 race car. Mayada obtained a Bachelor of Engineering from Reading University (UK) in 1999 and a Master of Science in Digital Electronics from the University of Sussex and the University of Brighton (UK) in 2000.

Dr. Roshanak Nilchiani is an Assistant Professor at the School of Systems and Enterprises at Stevens Institute of Technology. She is currently working on physical and mathematical modeling of systems' response to change. Her research interests include Risk-Based Complex Engineering Systems Design and Operations, System of Systems Design, Resilient Infrastructure Systems, and Agile Systems and Enterprises. During her time at MIT, Dr. Nilchiani performed research on flexible designs for DARPA's Orbital Express system, direct broadcasting satellites and next generation Mars rovers. In addition she has served as a mission analysis and design consultant for 4Frontiers, a commercial space travel company. Dr. Nilchiani received her Ph.D. in Aerospace Systems from the Massachusetts Institute of Technology in 2005 and is an associate member of the New York Academy of Sciences, and a member of the American Institute of Aeronautics and Astronautics.

Dr. Ali Mostashari is the Director of the Complex Adaptive Sociotechnological Systems (COMPASS) Research Center and an Associate Professor of Systems Engineering at the School of Systems and Enterprises at Stevens Institute of Technology. His research focuses on the application of complexity science to systems engineering, and to sociotechnological systems analysis and design. He currently serves as a senior strategy consultant for the United Nations Development Programme's Knowledge Management 2.0 strategy. Dr. Mostashari was selected as a Asia 21 Young Leader, and was nominated by the UNDP Assistant Secretary General for Africa for the World Economic Forum's Young Global Leaders 2008 award. In 2004, he was selected as a top finalist of UNDP's Leadership Development Programme from over 7000 applicants from 78 countries worldwide. Dr. Mostashari holds a Ph.D. in Engineering Systems from MIT, a Master's in Civil Engineering from MIT, a Master's in Technology and Policy from MIT, a Master's in Chemical Engineering from the University of Nebraska and a Bachelor's in Chemical Engineering from Sharif University of Technology