Resiliency Assessment of the Power System Network to Cyber and Physical Attacks

Essam Al-Ammar, *student member, IEEE,* and Joseph Fisher

Abstract-- **Studies of fault tolerant of network can be modeled based on classical graph connectivity. This study is very basic yet it conveys succinct information on the degree of vulnerability of network topology in imbedded systems such as the electrical power system information and communication networks. In this paper, the degree of vulnerability of the North American Electric Reliability Council (NERC) power network to attacks is studied. The degree of vulnerability can be deemed as a measure of the resiliency of the network to attacks launched via cyber means or through physical means. New definition to calculate the Resiliency is proposed. The attacks are simulated either by 'killing' a node that is, by taking a processing element out of service and or by removing links (communication channels) out of service and identifying the overall resiliency of the system. Different cases are carried out. It is anticipated that the results would provide some quantitative measures in terms of the degree of network vulnerability and the resiliency of the network to attacks.**

Keywords-- **Data routing, Vulnerability, Graph connectivity, Resiliency, Power system communications.**

I. Introduction

A SUCCINCT representation of modeling an interconnection topology of multi-computer system is a graph

$$G = (V, E) \qquad (1)$$

where V is the set of vertices (nodes) representing the processing elements in the network and E is the set of edges representing the communication links. An edge between processing elements x and y can be represented by the equation

$$e = (x, y) \in E \qquad (2)$$

If the links are unidirectional, a direct graph would be used with an arc from processing elements say x to y represented as $(x \longmapsto y)$. Based on such model of an interconnection, the network characteristics of the system can be found from properties of the network which include such graph invariants as shortest path, minimum spanning tree, salesman problem, maximal flow and others which can provide a static and dynamic measure of the network.

The static measure as defined in [1] provides a measure of the size of the work, the connection costs which are measured in terms of weights assigned to each links which could be given in terms of distance, time delay, bit rate, or some other quantitative measures. The static measure can also be used to determine the communication delays between any two processing elements. In real time analysis, the dynamic measure is preferred in determining communication requests among processing elements to avoid congestions within the network.

Other significant features applied in the analysis of multi-computer network are the reliability and availability of the system components (processing elements and links) that give a measure of the network resiliency. In analyzing such features, two important measures are often applied which are the deterministic and probabilistic measures. These measures are based on different criteria for acceptable network operation. A network can be defined to be operable if there exist paths between any pair of processing elements in spite of faulty components (connectivity) that would not lead to large communication delays. When considering probabilistic criteria, a network is analyzed upon simulation of an attack or attacks, and determining the resiliency of the network to these attacks. Resiliency is a measure of network reliability, flexibility, and adaptability and can be achieved through optimal consolidation and distribution of computing resources, as well as the availability, security, and robustness of the network to attacks or threats. The calculations of the network resiliency are discussed later in the paper.

II. Analysis of Communication Networks

Communication networks comprises of nodes that are often referred to as processing elements, and communication links that interconnect the various processing elements. The processing elements are the routers and computers within the network and the links are the communication channels or transmission media. Fig. 1 illustrates a block diagram representation of computer network is depicted comprising processing elements and links that make up a power system network.

The link types represent the communication channels that link the processing elements within the network. The communication channel can be any of the type listed in Table I. Table I provides a comparison of various links used in communication systems.

Processing elements could comprise of any of the following devices:

Multiplexers-a device that allows several communication signals to be transmitted over a communication medium simultaneously.

Internet processors-which could include computers and any of the following:

Routers - a telecommunication processor that interconnects networks based on different rules or protocols, so a telecommunication message can be routed to its destination

Hubs - a post switching communications processor. It allows for sharing of network resources such as servers, LAN

Essam Al-Ammar is with the Department of Electrical Engineering, Arizona State University, Tempe, AZ, 85287, USA (ealammar@asu.edu)

Joseph Fisher can be reached at (Joseph.Fisher@asu.edu)

1-4244-0493-2/06/$20.00 ©2006 IEEE

workstations, and printers.

Gateways - a communication processor that connects networks that use different network architectures.

Switches- a communication processor that makes connection between telecommunication circuits in a network so that a telecommunication message can reach its intended destination.

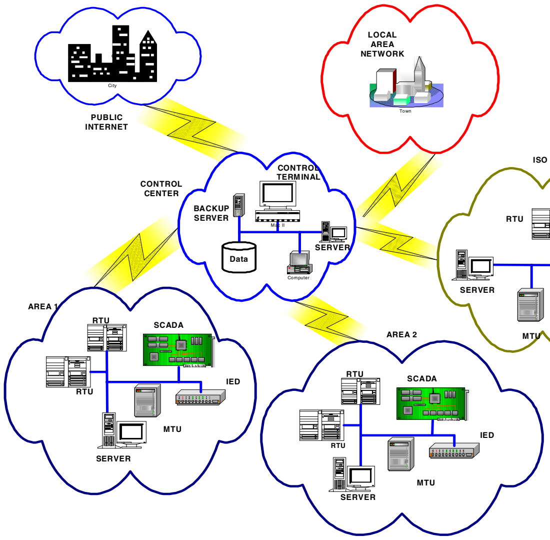

Fig. 1. Block diagram representation of computer network [3]

TABLE I
COMPARISON OF COMMUNICATION MEDIA

Communication medium	Data rate (Mbps)	Interference	Distance (mile)
Twisted pair	1-100	Electrical	100 mile (10 Mbps)
			up to 1 mile (1-2 Mbps)
			for 10 miles (2.4 kbps)
Coaxial cable	10	Electrical	2-3 miles
Optical fiber	400-500	Immune	20-30 miles
Microwave	200-300	Solid objects	20-30 miles
Satellite	1-2	Atmospheric conditions	

A switching device could comprise of any of the following:

Circuit switching - a link is established between the sender and the receiver, which remains in effect until the communication session is completed (an example would be the telephone session).

Message switching - a message is transmitted a block at a time from one switching device to another.

Packet switching - involves subdividing communications messages into fixed or variable group called packets. Typically packets are 128 characters long.

Cell switching - asynchronous transfer mode (ATM) switch which breaks voice, video, and other data into fixed cells, and routes them to their destination in the network.

Communication networks require switches and routers to be aware of other devices in the network in order to deliver data packets effectively. The only way this is possible is for all routers within the network to share knowledge on their network status with other devices within the network. With this shared knowledge, routers would have a fair understanding of the status of the network topology.

Routers determined the status of, or state of each link within the network by forwarding ‘hello’ packets on all their ports. In these packets, each router identifies itself so that upon receiving these packets, other routers establish connection to the router. That is, ‘hello’ messages are used to establish neighbor relationships to determine information exchange among other neighboring routers. Once a relationship is established, routers use such metrics as shortest path algorithm to map their destinations. This is accomplished by constructing a tree structure with each router at the ‘root’ of its own tree and the shortest paths to all other routers are mapped out. This allows for fast and efficient transfer of data within networks.

III. NERC POWER GRID CONNECTION

The trend in energy infrastructure deregulation in the United States and elsewhere into horizontally integrated systems is moving at a fast pace. For economic reasons most utilities are embracing the integration, consolidation, and dissemination of information systems and networks. Information or data traditionally used within a vertically integrated system now becomes very critical in a horizontally integrated system among such players as generating companies (gencos), transmission companies (transcos), distribution companies (discos), and independent system operators (ISOs) that are involved in the generation and transfer of energy. Transfer of information and data both inter- and intra-utilities has become vital to system operations. Despite the deregulation of power industry, the safety and reliability of the power system is regulated by North American Electric Reliability Council (NERC). The prime aim of the NERC as pointed out in [2] is to promote the reliability of the electricity supply of North America. As such the tasks of the NERC are to regulate the reliability operation of electric power systems in North America and to establish policies for reliable and secure operation of the entire power systems.

The electric power grid in North America comprises of three major interconnections which are the Western Interconnection - Western System Coordinating Council (WSCC), Electric Reliability Council of Texas (ERCOT)

Interconnections, and Eastern Interconnection. The Eastern Interconnection comprises other regional control areas such as the Florida Reliability Coordinating Council (FRCC), Mid Atlantic Area Council (MAAC), Mid America Interconnected Network (MAIN), Mid Continent Area Power Pool (MCAPP), Northeast Power Coordinating Council (NPCC), Southeastern Electric Reliability Council (SERC), East Central Area Reliability Coordinating Agreement (ECAR), and Southwest Power Pool (SPP). These regions are depicted in Figs. 2 and 3.

NERC comprises of about ten regional councils or control regions as depicted in Fig. 3. The members of the regional councils comprise all segments of the electric industry which include investor-owned utilities, independent power producers, independent power marketers, electric companies, and government entities. Each control area is bounded by some tie-line metering and telemetry control that monitors and controls the area power generation based on frequency control. This ensures dependable power is delivered to customers as well as controlling and monitoring interchange of power with neighboring control areas.

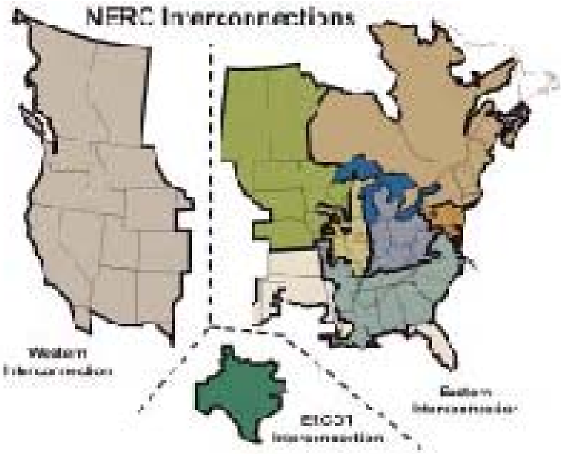

Fig. 2 NERC interconnection regions [2]

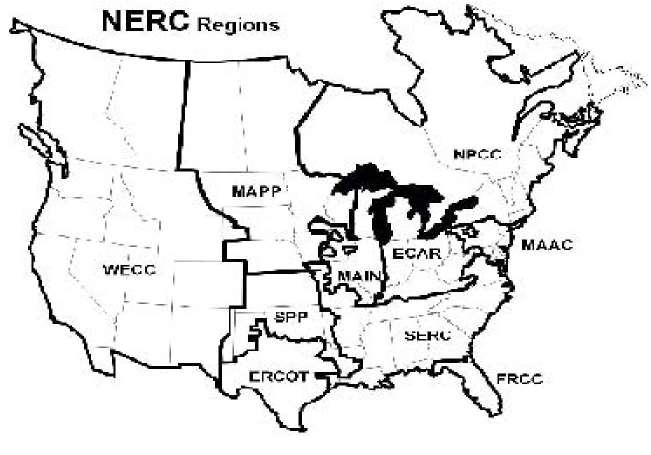

Fig. 3 NERC power regional interconnections showing regional control areas [2]

The criteria set by the NERC control areas as stipulated in [2] is that "…each control area shall have meters connected via communication links to facilitate exchange of information necessary to maintain interconnection reliability. The meters shall be installed on all tie-lines with adjacent control areas to record actual interchange of power (MW) in real time. The interchange meters shall be at a location common to both control areas, and provide identical values with opposite signs to both control areas. All control area interconnection points shall be equipped with common MWh meters, with readings provided hourly to the control centers of both control areas."

The entire NERC electric power system network depends on various information and communication elements to ensure proper functioning and reliability of the power grid. These elements are installed at all levels of the power network. At the lowest level are the supervisory control and data acquisition (SCADA) systems which are the central nerve systems that provide local level control of power systems. They provide supervisory control, data acquisition, alarm and process monitoring, energy accounting, and data management and report both normal and abnormal behavior of the information network.

At the level of power companies and regional control area information systems are the energy management systems (EMS) and the distribution management systems (DMS), which are simply the information systems that provide different functions related to power generation, transmission, and distribution applications. Some tasks performed by EMS programs include power generation and control, transmission control, network analysis, and contingency planning. DMS programs perform such tasks as display of real-time power network status, control of circuit breakers, and real-time power flow calculations within the network.

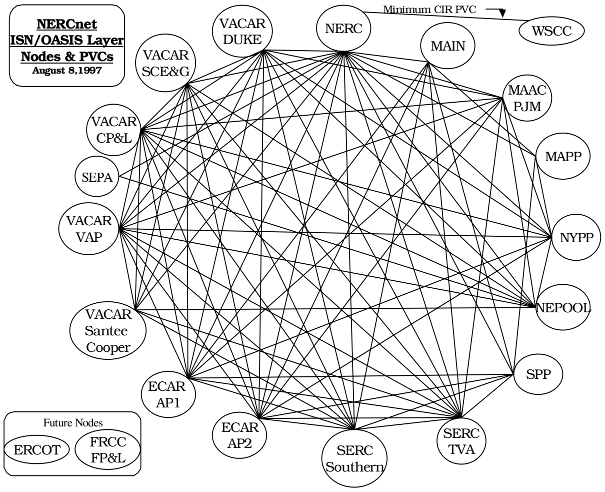

Fig. 4 NERC regional and interregional communication network [2]

A 1997-model of the NERC interregional structure at the level of power companies and regional control area information system is given in Fig. 4. The model comprises of the processing elements (nodes) and links forming a mesh network. The network provides interregional data exchange infrastructure that links the regional control areas. The interregional network is a near-real-time data exchange application for the purpose of sharing operational information pertaining to online operations of electrical power among pool members.

The interregional security nodes (ISN) as indicated in Fig. 4 reside primarily at Security Coordinator sites. Each control area is responsible for supplying their data to an ISN node for retrieval by any Security Coordinator or any other control area. Control areas will supply data to and retrieve data from their designated ISN.

The network structure is simply a collection of ISN nodes which communicate over a private frame relay system using inter-control center communications protocol (ICCP) to exchange the required power system data. A typical frame relay network is illustrated in Fig. 5.

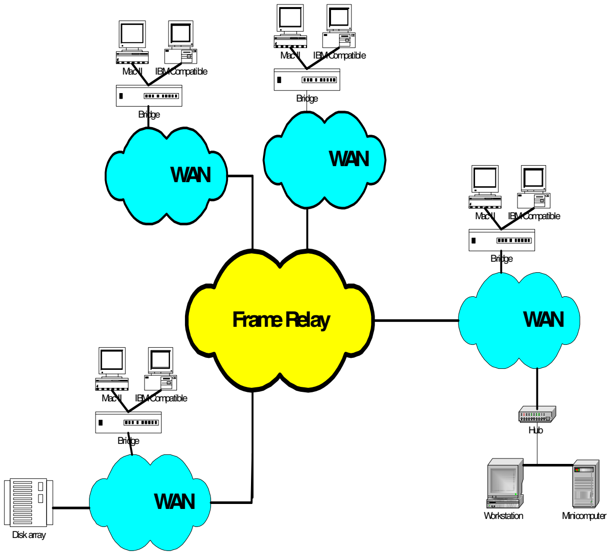

Fig. 5 A typical frame relay network [3]

A frame relay is simply a packet switched technology that is designed to solve communication protocol problems that other protocols lack [3]. That is, increased need for high speeds, increased need for large bandwidth efficiency, and the need to connect local area networks (LAN) and wide area networks (WAN) using intelligent networking devices with lower protocol processing time and at a lower costs than circuit switching over a leased line. These features make the frame relay technology an ideal communication protocol for complex embedded networks like the NERC power system networks with multiple WAN and unpredictable high volumes of data transfer and bursty traffic.

IV. NERC Network Simulations

It is impossible to prevent the occurrence of faults and attacks in a heterogeneously designed network such as the NERC communication and information network. This is because the system is so large and comprises of many sub-networks that the heterogeneity of the network design makes it inevitable to faults and failures. The overarching goal of this research is to forecast and estimate the presence, creation, and consequences of attacks and or faults on the network. The research explores the resiliency of the network to physical attacks, malicious security attacks, and incidental failures or faults. Resiliency as defined earlier, is a measure of network reliability, flexibility, and adaptability and can be achieved through optimal consolidation and distribution of computing resources, as well as the availability, security, and robustness of the network to attacks or threats.

Thus, the equation defining network resiliency is analogous to that of 'efficiency'. Efficiency is a measure of the ratio of system output to input correspondingly, resiliency gives a measure of the ratio of the weights of all nodes/links in service to that with certain nodes/links 'killed' or taken out of service. This is expressed mathematically as

$$\Re = \frac{\sum_{j=1}^{N}\left(\cos ts - certain\ nodes\ 'killed'\right)}{\sum_{j=1}^{N}\left(\cos ts - all\ nodes\ in\ service\right)} \qquad (3)$$

or

$$\Re = \frac{\sum_{j=1}^{N}\left(\cos ts - all\ links\ in\ service'\right)}{\sum_{j=1}^{N}\left(\cos ts - certain\ links\ 'killed'\right)} \qquad (4)$$

where $\Re$ is the resiliency, N is the number of nodes/links, and 'costs' are the accumulated weights which could be given in terms of distance, time delay, bit rate, or some other quantitative measures.

Dijkstra's algorithm [4] was applied to the network graph to determine the shortest route from a source to a destination point. Dijkstra's algorithm solves the single source shortest-path problem on a graph $G(V,E)$ provided all weights are nonnegative. That is, $\forall$ (i,j)$\in$ V: $w_{ij} \geq 0$. Starting at node s (source node), the algorithm finds the shortest path D_j from the source node s to every other permanently labeled node P in the graph as defined by the pseudo code in Fig. 6.

```
Initially $P = \{S\}$, $D_s = 0$,
Step 1: Find the adjacent nodes: Find $i \notin P$ such that
            $D_i = \min_{j \neq P} D_j$
Step2: Update the permanently label nodes and nodes' distances
            $P = P \cup \{i\}$
            $D_j = \min[D_j, D_i + d_{ij}]$
If $P$ contains all nodes then stop. Algorithm is complete.
Else go to Step 1.
```

Fig. 6 Pseudo code of Dijkstra's algorithm

V. Results and Discussion

Fig. 7 is a modified version of the NERC regional and interregional network under study. It is a mesh network with the various regional control areas depicted with the NERC node (node 1) at the hierarchy of the network and interlinks all other nodes. Neighboring regional and interregional nodes are interconnected to each other to allow interchange of data pertinent to online power operation among pool members within the regions.

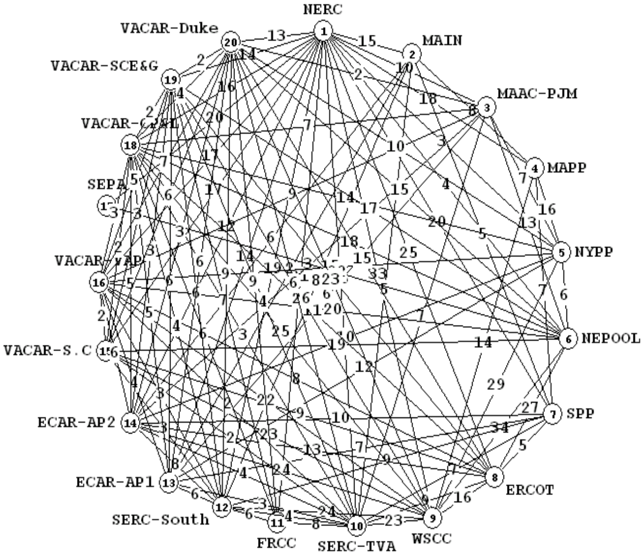

Fig. 7 Modified diagram of NERC communication network for simulation

The weights assigned to each links are given in the matrix in Fig. 8. For convenience, the weights are assigned according to the vulnerability of the link types. From Table I it is presumed that satellite links are the most secured of the listed links and as such are given lower weights compared to others.

$$\begin{bmatrix}
0 & 2 & 1 & 3 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 3 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 3 & 2 & 3 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 3 & 0 & 0 & 0 & 0 \\
0 & 3 & 3 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 3 & 0 & 4 & 0 & 0 & 0 \\
0 & 0 & 2 & 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 3 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 3 & 4 & 3 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 2 & 4 & 3 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 4 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 4 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 0
\end{bmatrix}$$

Fig. 8. Weight of each links

Several case studies were undertaken to assess the network resiliency to cyber and physical attacks that could result from such attacks as, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, buffer overflow attacks, and other similar attacks that could render the electrical power network inoperative. The processing elements or nodes such as computers or routers, and links (communication channels) can be 'killed' in two ways; by random removal of nodes and links, and by 'killing' of nodes and links based on calculated or motivated attack. The possible cases could be in many models, such as, incidental outages on the network, as well as determination of attacks carried out by attackers with ulterior motives such would be the case of terrorist attacks on a network

The following are the various case studies and scenarios that were investigated in the paper. Fig. 9 gives the shortest paths in terms of distance which is proportional to the time delay that would take for transmission of data to all nodes from the source node which is the NERC node (node 1). Only the shortest routes are indicated for convenience with other links removed. Fig. 10 shows the graphical representation of Fig. 9 with the various nodes and their corresponding shortest paths from the source node with all nodes and links in service (that is, no degradation). From Fig. 9 it is obvious that with node 1 taken out of service the performance of the system would be impaired as it is the main control node. A backup node would normally be required to maintain an effective network security and reliability.

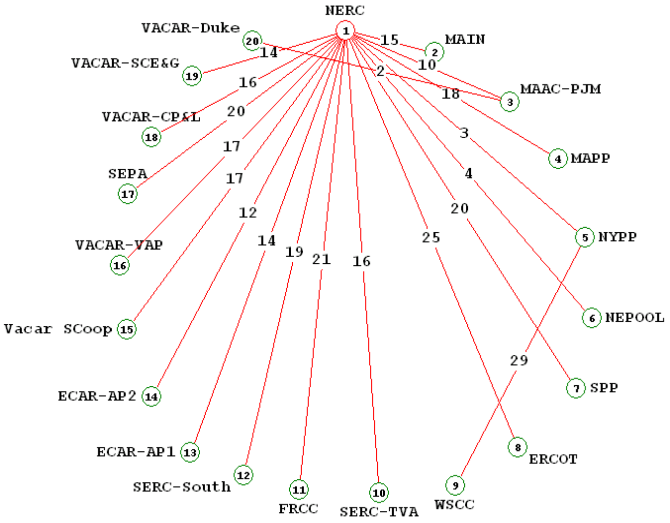

Fig. 9 Shortest paths to all nodes from NERC node (node 1) with all links and nodes in service

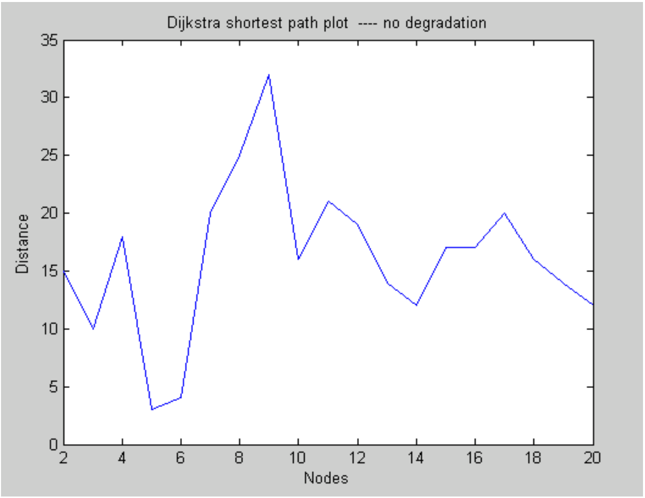

Fig. 10 Graphical representation of Fig. 9

In a DDoS attack, a hacker installs a program on a machine that would call on other system to participate in a distributed attack (from several machines) unlike DoS attack which is usually launched from a single machine. This would cause several machines to send bogus messages to the ultimate target of attack exhausting the network resources thus blocking or denying legitimate users access to the network resources. Such attacks on electric utilities would deny legitimate users such as control engineers and even protection engineers access to network data vital to online operation of power network.

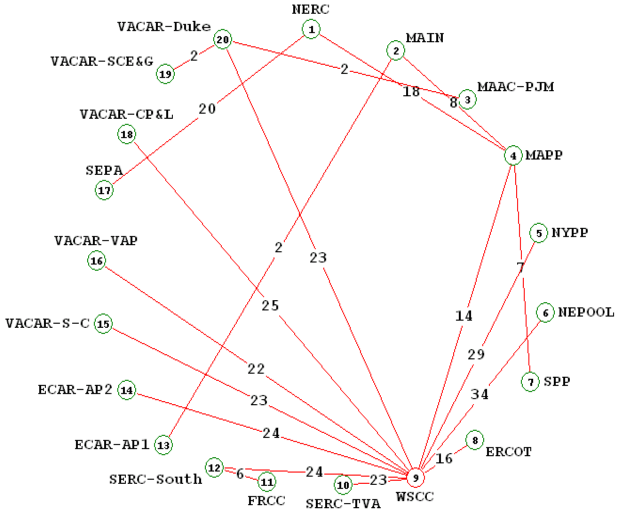

Fig. 11 Shortest paths from node 9 to all other nodes

TABLE II
RESILIENCIES OF THE NETWORK WITH THE WSCC NODE AS THE SOURCE

Node	Resiliency ($\Re$)
1	0.1019
2	0.0701
3	0.0796
4	0.0446
5	0.0924
6	0.1083
7	0.0669
8	0.0510
9	0
10	0.0732
11	0.0955
12	0.0764
13	0.0764
14	0.0764
15	0.0732
16	0.0701
17	0.1656
18	0.0796
19	0.0796
20	0.0732

Fig. 11 gives the shortest paths in terms of distance which is proportional to the time delay that would take for transmission of data to all nodes from the source node which is the WSCC node (node 9). Table II shows the resiliencies of the network with the WSCC node as the source and the corresponding resiliencies with each node 'killed'. The resiliencies are determined using Equation (3).

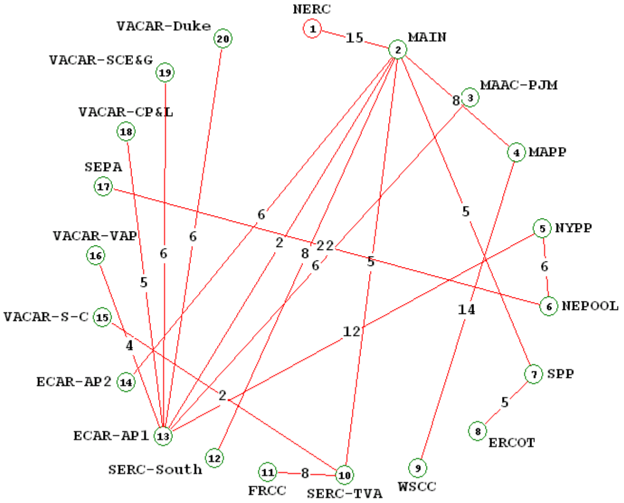

Fig. 12 Shortest paths to all links to node 1 'killed' except to node 2

Another case, where shortest paths (in term of distance) to all links to NERC node (node 1) 'killed' except to MAIN node (node 2) is proposed, as shown in Fig. 12. The results are also presented graphically in Fig. 13, with and without degradation. It is noted the distinction between the two degradation cases from the Fig. 13. The resiliencies of the network with all links to NERC node 'killed' except to MAIN node can calculated using Equation (4).

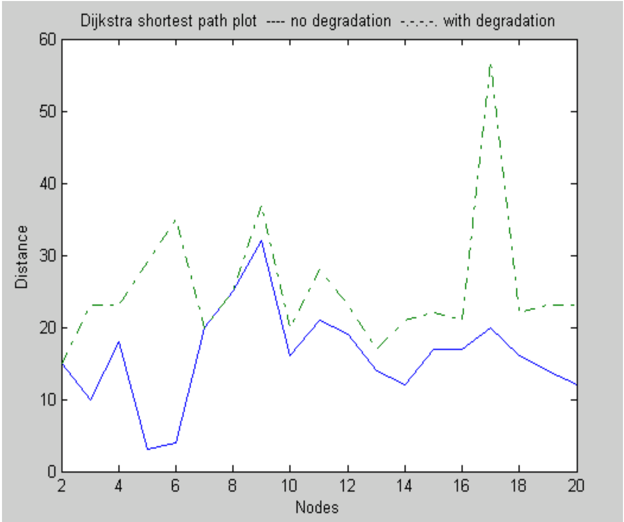

Fig. 13 Graphical representation of Fig. 12

VI. Conclusion

The presence, creation, and consequences of attacks and or faults on the network are forecasted and estimated. The resiliency of the network to physical attacks, malicious security attacks, and incidental failures or faults is explored and studied. New definition of the resiliency is proposed. The degree of vulnerability can be deemed as a measure of the resiliency of the network to attacks launched via cyber means or through physical means. New definition to calculate the Resiliency is proposed

Different cases were simulated and illustrated, in which the degree of vulnerability of the North American Electric Reliability Council (NERC) power network to attacks were studied. This ongoing research can have many cases and scenarios, which reserved for future publications.

It is anticipated that this research would provide some quantitative measures in terms of the degree of network vulnerability and the resiliency of the network to attacks.

VII. References

[1] P. Duggan, "A Mutual Alternative Routing Model for Circuit-Switched Networks," *IEEE Journal*, Electronics & Communication Engineering, Vol. 8, No. 4, August 1996, pp. 83 – 190.

[2] North American Electric Reliability Council (NERC), 1997 http://www.nerc.com/

[3] Black Box Corporation, 2002 http://www.blackbox.com/tech_docs/tech_overviews/frame_relay.html

[4] M. T. Goodrich and R. Tamassia, "Data Structure and Algorithms in Java," 2nd edition, Wiley Inc, 2001.