How to cite this paper:

Mariam Wajdi Ibrahim (2018). Level of resilience measure for communication networks. *Journal of Information and Communication Technology* (JICT), *17* (1), 115-139.

LEVEL OF RESILIENCE MEASURE FOR COMMUNICATION NETWORKS

Mariam Wajdi Ibrahim

School of Applied Technical Sciences
German Jordanian University, Jordan

mariam.wajdi@gju.edu.jo

ABSTRACT

Our daily life applications have come to depend on communication networks to deliver services in an efficient manner. This has made it possible for an attacker to sabotage its operation. Network resiliency is concerned with the degree the network is able to bounce back to a normal operation in the face of attacks. This paper introduced a new resiliency measure, called Levelof-Resilience (LoR) for communication networks, determined by examining: (a) the Level-of-Stability-Reduction (LoSR), as measured by percentage of "IP traffic dropped", (b) the eventual Level-of-Performance-Reduction (LoPR), as captured by the percentage of reduction in the application Quality-of-Service (QoS), namely latency and (c) Recovery-Time (RT), which is the time the network takes to detect and recover from an attack or a fault, as measured by convergence duration. Previous resiliency measures may only consider one aspect of the above parameters, while this measure is a composite of them. This paper showed that network topology can affect the network resilience, as indicated by the LoR metric. This measure is illustrated by comparing the resiliency level of two communication networks that served the same traffic, but differed in their network topology, under three different attack scenarios.

Keywords: Level-of-resilience, stability, quality-of-service, convergence.

Received: 14 June 2017 Accepted: 7 September 2017

LEVEL OF RESILIENCE MEASURE FOR COMMUNICATION NETWORKS

Mariam Wajdi Ibrahim

School of Applied Technical Sciences
German Jordanian University, Jordan

mariam.wajdi@gju.edu.jo

ABSTRACT

Our daily life applications have come to depend on communication networks to deliver services in an efficient manner. This has made it possible for an attacker to sabotage its operation. Network resiliency is concerned with the degree the network is able to bounce back to a normal operation in the face of attacks. This paper introduced a new resiliency measure, called *Level-of-Resilience* (*LoR*) for communication networks, determined by examining: (a) the *Level-of-Stability-Reduction* (LoS_R), as measured by percentage of "*IP traffic dropped*", (b) the eventual *Level-of-Performance-Reduction* (LoP_R), as captured by the percentage of reduction in the application *Quality-of-Service* (*QoS*), namely latency and (c) *Recovery-Time* (*RT*), which is the time the network takes to detect and recover from an attack or a fault, as measured by convergence duration. Previous resiliency measures may only consider one aspect of the above parameters, while this measure is a composite of them. This paper showed that network topology can affect the network resilience, as indicated by the *LoR* metric. This measure is illustrated by comparing the resiliency level of two communication networks that served the same traffic, but differed in their network topology, under three different attack scenarios.

Keywords: Level-of-resilience, stability, quality-of-service, convergence.

Received: 14 June 2017 Accepted: 7 September 2017

INTRODUCTION

An adverse event can affect both networks' stability and performance, and whose recovery time is also another important figure of merit. Therefore, when designing a network, it is crucial to choose the best design utilizing the given set of resources (of nodes and connectivity). Doing so, can affect the network's resiliency, i.e. its ability to withstand adverse events. Hence, this paper tackled the problem of measuring how resilient the network is against adverse events (link, or node failures).

Various measures of networks' resilience have been investigated throughout the literature. For instance, Farid (2015) proposed *static* resilience measures (number of service paths that realized a service, before and after a disruption) for *large flexible engineering systems* based upon an axiomatic design model which specifically considered the allocation of the system processes to system resources. Such processes and resources may be defined at any level of abstraction or decomposition at successive stages of the engineering design.

Menth, Duelli, Martin, and Milbrandt (2009) assigned reasonable probabilities to failure scenarios, abnormal traffic matrices of the network for ingress-egress pairs and to overload on links. Then statistical measures for unavailability and overload in the network are derived. Baroud, Ramirez-Marquez, Barker, and Rocco (2014) introduced stochastic temporal metrics of resilience against a disrupted network. These are time to total system restoration, time to full system service resilience, and time to a specific %α resilience.

The network resilience measure is given by Shi & Fonseka (1997) as the percentage of lost traffic due to physical link failures. The scalability of network resilience is defined as the growth rate of this measure with respect to the physical topology, the failure probabilities, the protection schemes and the network layer traffic (Liu & Ji, 2009).

The integration of the area under the quality curve with values representing varying degrees of system operability is labeled with Resilience *R* by O'Rourke (2007). Moreover, the expected loss in the quality of communications, as modeled by a random variable, is proposed by Shirazi et al. (2013) as a resilience measure. The quality measure can be in terms of bandwidth, latency, throughput, or some other observable variables of interest, when the adversary takes out a number of nodes.

A series of experiments were conducted by CAIDA (2016) to infer topological resilience of complex networks to breakdowns or attacks, by estimating the percentage of the network that remains reachable when nodes with the largest out-degrees are removed, or by removing nodes with the smallest average distance to the rest of the network. A similar resilience measure is introduced by Matta (2014), namely Vertex Attack Tolerance (*VAT*). *VAT* represents the worst case scenario of the proportionally smallest number of vertices that must be attacked in order to disconnect the largest number of vertices from the network.

A comprehensive set of network characteristic parameters that affect the performance and the resilience of the network were identified by Mohammad, Hutchison, and Sterbenz (2006). These parameters were classified by density, mobility, channel, node resources, network traffic, and derived properties. A network metric is a function of these parameters. Then, mathematical expressions are defined for network states in terms of network operational metric (e.g. normal operation, partially degraded, and severely degraded), and also in terms of network performance (e.g. acceptable, impaired and unacceptable).

A two-dimensional classification framework for network resilience metrics was presented by ENISA (2010). The first dimension was incidence-based classification, where resilience metrics were grouped over three different times: the preparedness phase, the service delivery phase, and the recovery phase. The second dimension was domain-based classification, covering areas such as security, dependability and performability. In the preparedness phase, the number of links removed are varied, while measuring the network performance (e.g. bandwidth, packet loss) either empirically or via simulation. Using the data collected, an envelope were determined, which was confined by the best case curve (the upper boundary of the performance) and the worst case curve (the lower boundary of the performance) for a given number of link/node failures.

A quantitative framework based on using a measure analogous to availability through the dependence on the up and down times was proposed by Kwasinski (2015) for measuring and characterizing resiliency for communication networks power supply. The degree of dependency

of a communications facility from the electric power grid or of components of a communications site could be measured based on a *primary dependent resiliency* R_L.

Heck, Kieselmann and Wacker (2016) measured the network connectivity within extensive simulations for different structured overlay network configurations to determine the resilience of self-organizing cyber-physical systems. The network resilience *r* is given by the number of nodes that can fail without loss of communication.

Conceptual frameworks for performance testing and network optimization that would enable operators in Thailand to optimize their network performance was developed by Chimmanee & Jantavongso (2016). This involved the *QoS* measurements of the services (e.g. latency, user data rates, and speed test measurements) by the 3G operators and on 850/900MHz and 2100MHz bands respectively.

The main contribution in this paper is to introduce the notion of Level-of-Resilience (*LoR*) for communication networks as a way to measure their resiliency. To quantify resiliency, the following are considered: (a) Level-of-Stability-Reduction (LoS_R), as measured in terms of the percentage of *IP* traffic dropped, (b) Level-of-Performance-Reduction (LoP_R), as measured in terms of percentage of reduction in the application Quality-of-Service (*QoS*) latency parameter, and (c) the amount of Recovery-Time (*RT*) it takes for a network to recover from an adverse event in terms of convergence duration. Two communication networks with the same users and applications, but with different topologies were analyzed using the *Optimized Network Engineering Tools* (*Opnet Modeler*), a software tool for computer network modeling and simulation (RTI, 2016). The collected data from the simulation were used to compare the Level-of-Resilience for these two networks under three different attack scenarios.

COMMUNICATION NETWORKS LEVEL-OF-RESILIENCE

Communication Networks Stability

Traditionally, networks have been viewed as being a relatively stable layer over which traffic is routed. The traffic flows and the routing updates have been seen as sources of instability (Clayman, Clegg, Galis, & Manzalini, 2012). The level of path stability defined by Kuipers & Van Mieghem (2005), has a direct relation to the number of updates that are necessary to maintain an accurate view of the network state of information. If a small change in the network state does not affect the shortest path between network nodes, then such a change need not be distributed throughout the network.

Stability refers to the property of keeping the amount of traffic (number of packets) in the network to remain always bounded over time (Alvarez, Blesa, & Serna, 2011). Beyond such a bound, a network would incur packet drops/

losses, and therefore, the level of stability of a network is measured in terms of the percentage of *IP* traffic dropped.

The attack model presented here includes link or node failures (the latter also implies a set of link failures). Certainly a network must be endowed with layers of security (such as authentication, encryption, firewalls and detection) to cope with false/corrupted traffic, but those are viewed to be the resiliency properties of the security layer, and the network resilience is viewed to arise out of its topological and networking redundancy in coping with link/node compromises (Salles & Jr, 2011). This work examined the network resilience against link failures in terms of losses in level of stability and performance (i.e. the application latency *QoS* **parameter) while recovery time as measured by convergence duration was another figure of merit.**

Level-of-Resilience Formulation

Given a sequence of *m* faults/attacks, and the corresponding rerouting/recovery actions, suppose the resulting network configurations (also referred to here as modes) are denoted by $N_0 \rightarrow N_1 \rightarrow \ldots \rightarrow N_m$, where N_0 is the initial mode, while N_i is the mode after the i^{th} fault and reconfiguration (*i=1, ..., m*). The amount of *IP* traffic dropped in those configurations is denoted as: $IP_0 \rightarrow IP_1 \rightarrow \ldots \rightarrow IP_m$. Then, as mentioned above, the Level-of-Stability-Reduction (LoS_R) is measured by the percentage of *IP* traffic dropped.

Definition 1. *Given the sequence of mode switches:* $N_0 \rightarrow N_1 \rightarrow \ldots \rightarrow N_m$, *(under an attack scenario A), the corresponding sequence of amount of IP traffic dropped:* $IP_0 \rightarrow IP_1 \rightarrow \ldots \rightarrow IP_m$,*, and the total amount of IP traffic sent,* IP_s, *the Level-of-Stability-Reduction,* LoS_R, *is given by,*

$$LoS_R := [(IP_m - IP_0)/ IP_s]\%. \tag{1}$$

For the following definition, a factor is added, which is the Level-of-Performance-Reduction (LoP_R) in the application Quality-of-Service (QoS), namely network latency.

Definition 2. *Given the sequence of mode switches:* $N_0 \rightarrow N_1 \rightarrow \ldots \rightarrow N_m$, *(under an attack scenario A), the Level-of-Performance-Reduction,* LoP_R, *in the Quality-of-Service, QoS, Latency parameter, L, of a network application, is given by Maximum-Loss-in-Performance, MLiP:*

$$LoP_R :=[(L_m - L_0) / L_0]\%. \tag{2}$$

Another aspect of the resiliency metric is Recovery-Time (*RT*), which is the time network takes to detect and recover from an attack or a fault, as measured by convergence duration. This duration tells how much time it takes for a network that goes to failure condition to come back to normal condition (Shah & Waqas, 2013).

Using Definitions 1 and 2, the following definition can be used to compare the Level-of-Resilience of two or more networks under an attack scenario: A network is more resilient if it incurs a smaller loss of stability, or otherwise, a smaller loss of performance, or otherwise a smaller level of recovery-time.

Definition 3. *Given two networks CN_1 and CN_2, and an attack scenario A, we say that $LoR(CN_1, A) > LoR(CN_2, A)$ if:*

$[LoS_R(CN_1, A) < LoS_R(CN_2, A)]$

Ú $[[LoS_R(CN_1, A) = LoS_R(CN_2, A)]$

Ù $[LoP_R(CN_1, A) < LoP_R(CN_2, A)]]$

Ú $[[LoS_R(CN_1, A) = LoS_R(CN_2, A)]$

Ù $[LoP_R(CN_1, A) = LoP_R(CN_2, A)]$

Ù $[RT(CN_1, A) < RT(CN_2, A)]]$.

Example Networks to Illustrate LoR

To illustrate this approach, a pair of communication networks with identical users and applications/services (Email, FTP, and Video) were considered, but with different topologies, as shown in Figures 1 (a) and (b). For the 1st communication network, CN_1, three routers; R_1, R_2, and R_3 were configured with Routing Information Protocol (*RIP*), and were connected with each other. In addition to that, R_1 was connected to three Local Area Networks (*LAN*s); LAN_1, LAN_2, and LAN_3, where each *LAN* had ten users. R_2 was connected to LAN_4, which had ten users as well. Router R_3 had three more links, which connected it respectively, to an Email server through the Internet, an FTP server, and a Video workstation. The 2nd communication network, CN_2, had the same users and applications/services as CN_1, but possessed a different topology, in which LAN_1 was connected to R_3 as opposed to R_1.

The application configurations, the node models in use, and link models in use for the two networks are tabulated in Appendix, Tables 10-12. For Email and FTP services, the latency corresponded to the download time, whereas for the Video application, it was measured as the packet delay variation. This work demonstrates through analysis that while the two networks served the same set of users/demands, and were served by the same set of servers/workstations, they had different resilience to the same attack due to their topological difference.

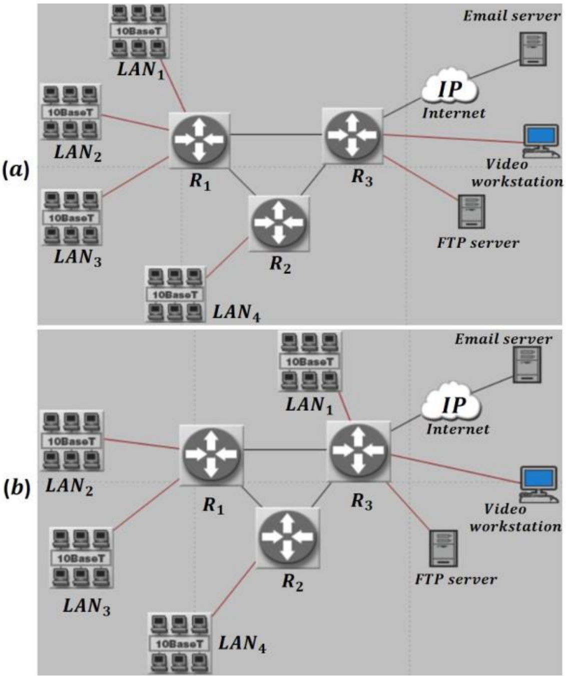

Figure 1. (a) Network CN1, and (b) Network CN2.

EXPERIMENTAL COMPARISON OF LoR

In this section, three different attack scenarios for two different communication networks CN_1 (Figure 1 (a)) and CN_2 (Figure 1 (b)) were simulated, with identical users, and applications/services (Email, FTP, and Video), but with different topologies. For each scenario, the *LoR* for each network was evaluated and compared.

In the first attack scenario A_1, two links were compromised in the sequence: $L_{13} \rightarrow L_{23}$. For CN_1, the initial pre-fault average *IP* traffic dropped was: 0.0516 *packets/sec*, which was the average *IP* datagrams dropped by all nodes in the network (Sethi & Hnatyshin, 2013). A fault was applied at link L_{13} between routers R_1 and R_3 at time 540 *sec*. For *RIP*, a distance vector routing protocol which offered hop count as a routing metric for path selection, the traffic was rerouted through a redundant path (if it existed). By default, the routing updates are broad-casted or multi-casted every 30 *sec,* with a maximum of 15 hops count from source towards the destination (i.e. *RIP* provides loop-free routing) (CAN, 2016). In general, the rerouting time is dependent on the routing protocol in use. Here, both networks that were analyzed, were configured with the same routing protocols, (i.e., *RIP*). After rerouting the traffic through a redundant path, (i.e. for the traffic communicated among *LAN*s: LAN_1, LAN_2, and LAN_3 and the servers/workstations, the traffic was rerouted through $R_1 \leftrightarrow R_2 \leftrightarrow R_3$), the average *IP* traffic dropped converges to post-fault steady state of 0.3269 *packets/sec*. The total *IP* traffic sent was 39975.6 *packets/sec,* and the corresponding Level-of-Stability-Reduction (LoS_R), was given by 0.7×10^{-3}%. If a second fault was applied at link L_{23} between routers R_2 and R_3 at time 3600 *sec*, then, traffic communicated among the *LAN*s, LAN_1, LAN_2, LAN_3, and LAN_4 and the servers, had no redundant path to be rerouted through. Hence, the average *IP* traffic dropped grew unbounded as shown in Figure 2 and the network was no longer stable.

The same attack sequence A_1 was simulated for the second communication network, CN_2, shown in Figure 1 (b), where the initial pre-fault average *IP* traffic drop was: 0.0496 *packets/sec*. A fault was applied at link L_{13} between routers R_1 and R_3 at time 540 *sec*. Accordingly, the traffic communicated among the *LAN*s, LAN_2, LAN_3 and the servers, was rerouted through $R_1 \leftrightarrow R_2 \leftrightarrow R_3$. The post-fault steady state *IP* traffic dropped was 0.2497 *packets/sec*. The total *IP* traffic sent was 36921.6 *packets/sec*, and the corresponding Level-of-Stability-Reduction (LoS_R) was given by 0.5×10^{-3}%. After that, a second fault was applied at link L_{23} between routers R_2 and R_3 at time 3600 *sec*. Then, the traffic communicated among the *LAN*s, LAN_2, LAN_3, LAN_4 and the servers, had no redundant path to be rerouted through. Hence, the average *IP* traffic dropped grew unbounded as shown in Figure 3 and the network was no longer stable.

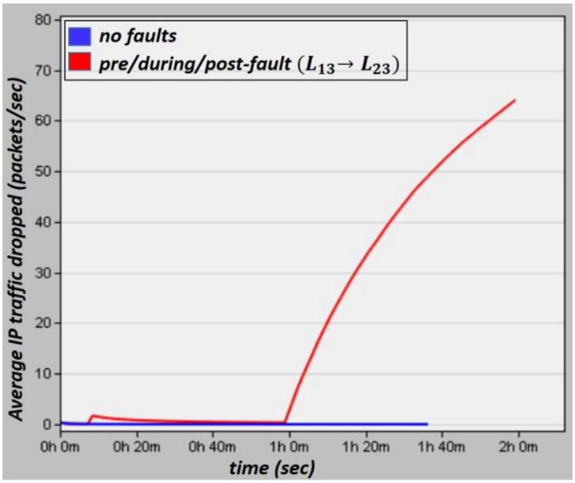

Figure 2. CN1 average IP traffic dropped under A1.

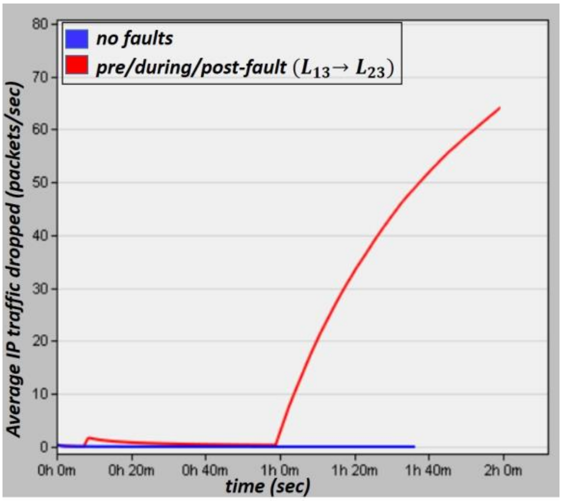

Figure 3. CN2 Average IP Traffic Dropped Under A1.

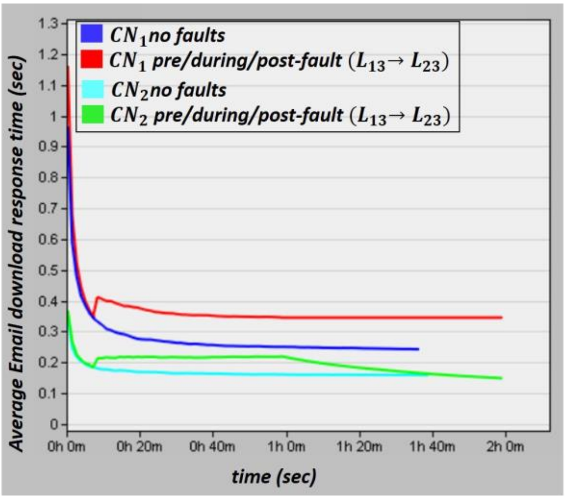

Figure 4. CN1 (respectively, CN2) average email download response time under A1.

The LoP_R associated with each mode of configuration was measured by the Maximum-Loss-in-Performance (*MLiP*), following Equation (2), of the coressponding latency of the Email, FTP, and Video services. Figure 4 shows the Email latency for CN_1 and CN_2, respectively. It is given by the average download response time under A_1. Here, it can be noticed that for CN_2 under the second fault at link L_{23}, only LAN_1 was served (connected) with a *MLiP* of 34.63%, whereas for CN_1, no *LAN* is served and with an infinite download response time (i.e. $LoP_R=\infty$). In this case, the *Opnet Modeler* marked the same data collected at the time step preceding the current infinite (undefined) value (Sethi & Hnatyshin, 2013), (i.e. the value of 0.3455 *sec* generated at time 3528 *sec* was continuosly repeated for the remaining time of simulation as shown in red in Figure 4.)

Similar observations can be made regarding the FTP latency, which is given by the average download response time. LAN_1 was configured with Email and FTP applications. Hence, under the second fault at link L_{23}, LAN_1 was served (connected) in CN_2, while it was no longer served (connected) in CN_1, making the eventual LoP_R for CN_2 = 13.20%, whereas, the eventual LoP_R for CN_1 was infinite (i.e. infinite download response time), and is given by Opnet as the data preceding the current infinite (undefined) value, (i.e. the value of 0.9539 sec was continuously repeated after the second fault, as shown in red in Figure 5.)

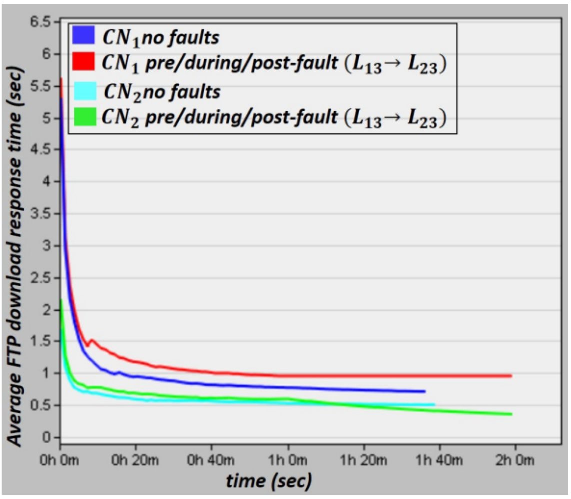

Figure 5. CN1 (respectively, CN2) average FTP download response time under A1.

For Video application, Figure 6 shows the average in packet delay variation as a latency parameter for CN_1 and CN_2 respectively, under A_1. It can be seen that after the 2nd fault at link L_{23}, both CN_1, and CN_2 no longer serve the Video application, (i.e. both have an infinite delay variation, which is given by the

Opnet values of 0.0407 for CN_1, and 0.0079 for CN_2), as LAN_2 and LAN_3 are not connected to the networks. Hence, $LoP_R=\infty$ for both CN_1, and CN_2.

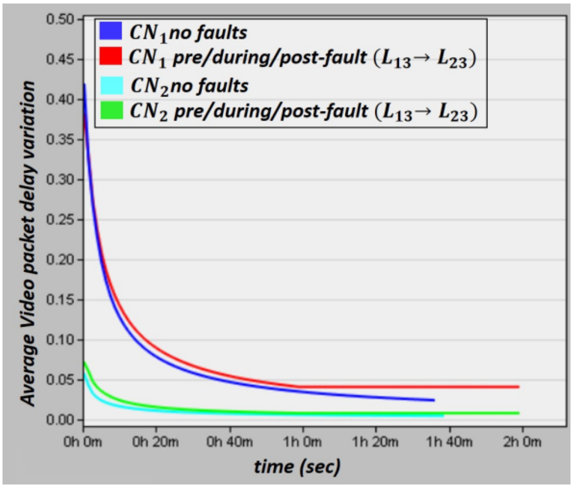

Figure 6. CN1 (respectively, CN2) average video packet delay variation under A1

Figure 7 shows the average *IP* convergence duration for CN_1 and CN_2 respectively, under A_1. It can be seen that CN_2 took less time (7.53 *sec* on average) to converge as compared to CN_1 (7.69 *sec* on average).

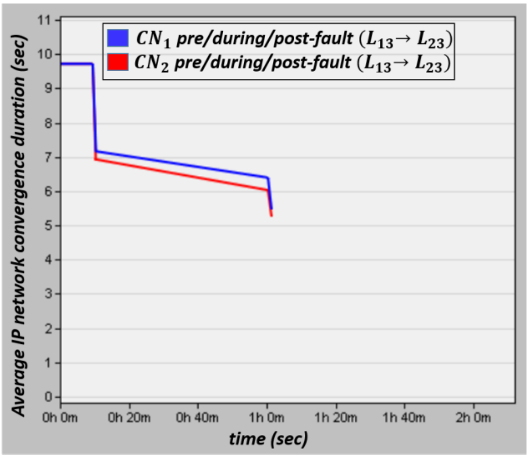

Figure 7. CN1 (respectively, CN2) average IP convergence duration under A1.

Tables 1 and 2 show the data collected for the average Email (respectively, FTP) download response time, D. While, Table 3 shows the data for Video packet delay variation, V, of each network at t = 540 sec, and t = 3600 sec, respectively, and the eventual LoP_R under A_1, following equation (2). For CN_1, the LoP_R for the three applications. Email, FTP, and Video was ∞, while for CN_2, Email LoP_R = 34.63%, FTP LoP_R = 13.20%, and Video LoP_R = ∞. Hence, CN_1 had higher LoP_R than CN_2 over all applications. Moreover, CN_1 had higher LoS_R (0.7×10^{-3}%) as opposed to CN_2 (0.5×10^{-3}%). In addition, the RT of CN_1 was greater than the RT of CN_2 , so $LoR(CN_2, A_1) > LoR(CN_1, A_1)$. Thus, CN_2 was more resilient to attack scenario A_1 as compared to CN_1.

Table 1

Average Email Download Response Time, D of Each Network (sec) and LoP_R (%) Under A_1

A_1	D_0, t = 540 sec	$D_{(L13)}$, t = 540 sec	D_0, t = 3600 sec	$D_{(L23)}$, t = 3600 sec	LoP_R
CN_1	0.3316	0.4117	0.2504	∞	∞
CN_2	0.1804	0.2137	0.1608	0.2165	34.63

Table 2

Average Ftp Download Response Time, D of Each Network (sec) and LoP_R (%) Under A_1

A_1	D_0, t = 540 sec	$D_{(L13)}$, t = 540 sec	D_0, t = 3600 sec	$D_{(L23)}$, t = 3600 sec	LoP_R
CN_1	1.1858	1.5230	0.7704	∞	∞
CN_2	0.6863	0.7760	0.5251	0.5944	13.20

Table 3

Average Video Packet Delay Variation, V of Each Network and LoP_R (%) Under A_1

A_1	V_0, t = 540 sec	$V_{(L13)}$, t = 540 sec	V_0, t = 3600 sec	$V_{(L23)}$, t = 3600 sec	LoP_R
CN_1	0.1411	0.1556	0.0344	∞	∞
CN_2	0.0180	0.0265	0.0058	∞	∞

Similarly, under a second attack scenario, A_2: $L_{13} \rightarrow L_{12}$, the average *IP* traffic dropped (respectively, Email download response time, FTP download response time, and Video packet delay variation) for both CN_1 and CN_2 as shown in Figures 8-12.

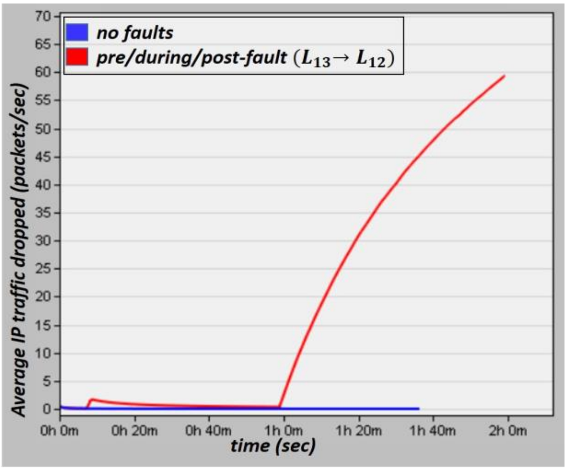

Figure 8. CN1 average IP traffic dropped under A2.

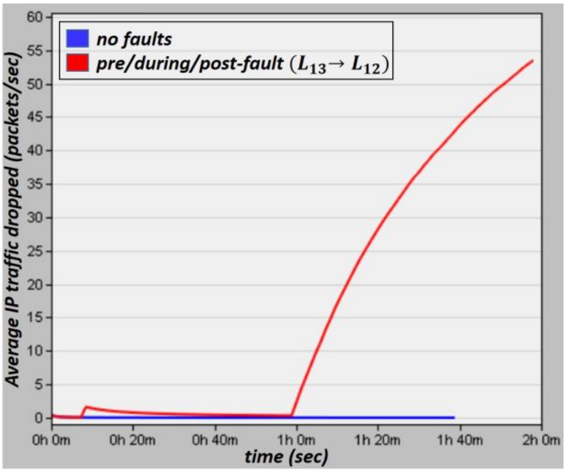

Figure 9. CN2 average IP traffic dropped under A2.

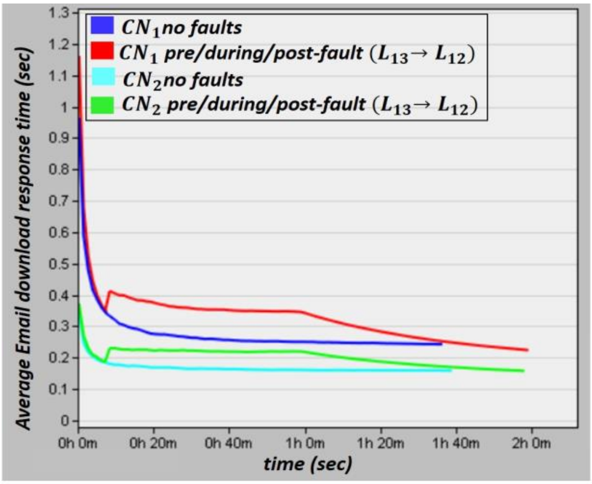

Figure 10. CN1 (respectively, CN2) average email download response time under A2.

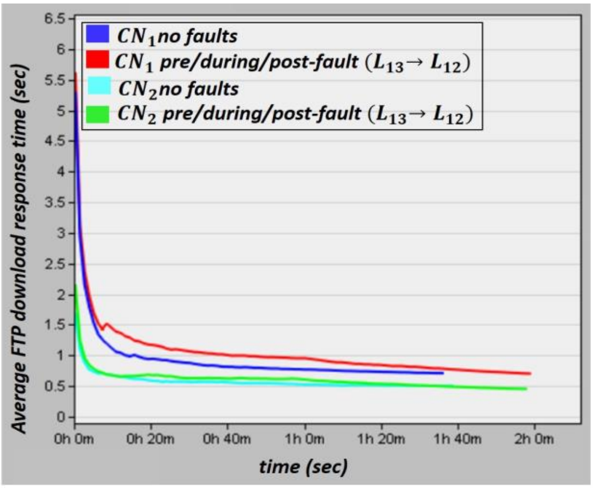

Figure 11. CN1 (respectively, CN2) average FTP download response time under A2.

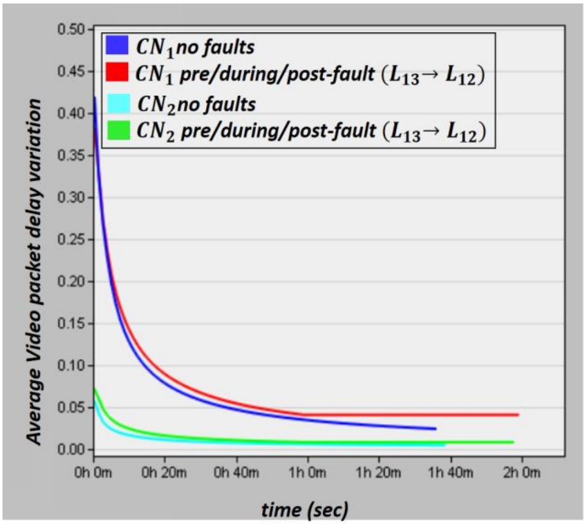

Figure 12. CN1 (respectively, CN2) average video packet delay variation under A2

Figure 13 shows the average *IP* convergence duration for CN_1 and CN_2 respectively, under A_2. It is clear that CN_2 took less time (7.44 *sec* on average) to converge as compared to CN_1 (7.70 *sec* on average).

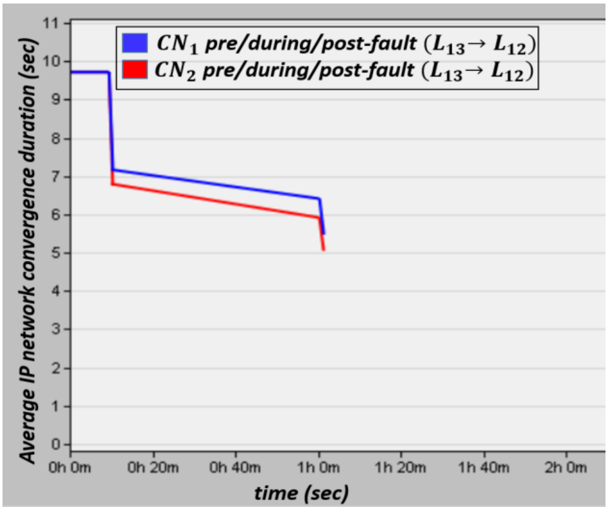

Figure 13. CN1 (respectively, CN2) average IP convergence duration under A2.

Tables 4 and 5 show the data collected for the average Email (respectively, FTP) download response time, D. Table 6 shows the data for Video packet delay variation, V, of each network at t = 540 sec, and t = 3600 sec, respectively, and the eventual LoP_R under A_2, following equation (2). For CN_1, Email LoP_R = 36.58%, FTP LoP_R = 23.82%, and Video $\text{LoP}_\text{R} = \infty$. On the other hand, for CN_2, the Email LoP_R = 35.57%, FTP LoP_R = 15.61%, and Video $\text{LoP}_\text{R} = \infty$. Hence, CN_1 had higher LoP_R than CN_2 over all applications. Moreover, both CN_1 and CN_2 had the same LoS_R (0.7×10^{-3}%). Also, the RT of CN_1 was greater than the RT of CN_2, so $\text{LoR}(\text{CN}_2, \text{A}_2) > \text{LoR}(\text{CN}_1, \text{A}_2)$.

Table 4

Average Email Download Response Time, D of Each Network (sec) and LoP_R (%) Under A_2

A_1	**D_0, t = 540 sec**	**$D_{(L13)}$, t = 540 sec**	**D_0, t = 3600 sec**	**$D_{(L12)}$, t = 3600 sec**	**LoP_R**
CN_1	0.3316	0.4117	0.2504	0.3420	36.58
CN_2	0.1804	0.2301	0.1608	0.2180	35.57

Table 5

Average Ftp Download Response Time, D of Each Network (sec) and LoP_R (%) Under A_2

A_1	**D_0, t = 540 sec**	**$D_{(L13)}$, t = 540 sec**	**D_0, t = 3600 sec**	**$D_{(L12)}$, t = 3600 sec**	**LoP_R**
CN_1	1.1858	1.5230	0.7704	0.9539	23.82
CN_2	0.6863	0.6897	0.5252	0.6072	15.61

Table 6

Average Video Packet Delay Variation, V of Each Network and LoP_R (%) Under A_2

A_1	**V_0, t = 540 sec**	**$V_{(L13)}$, t = 540 sec**	**V_0, t = 3600 sec**	**$V_{(L12)}$, t = 3600 sec**	**LoP_R**
CN_1	0.1411	0.1556	0.0344	∞	∞
CN_2	0.0180	0.0266	0.0058	∞	∞

A third attack scenario A_3, was also simulated, A_3: L_{12} → L_{23}. The average IP traffic dropped (respectively, Email download response time, FTP download response time, and Video packet delay variation) for both CN_1 and CN_2 as shown in Figures 14-18.

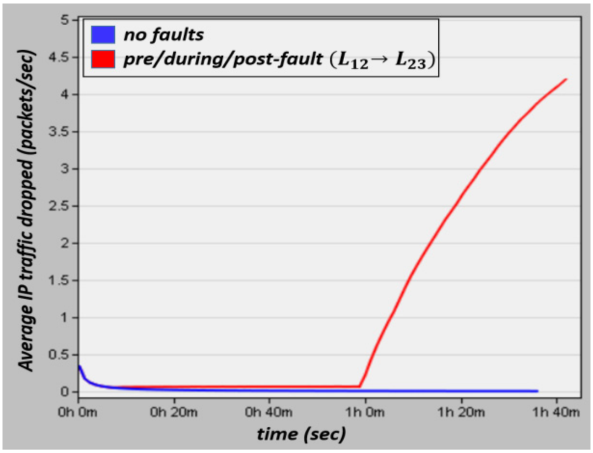

Figure 14. CN1 average IP traffic dropped under A3.

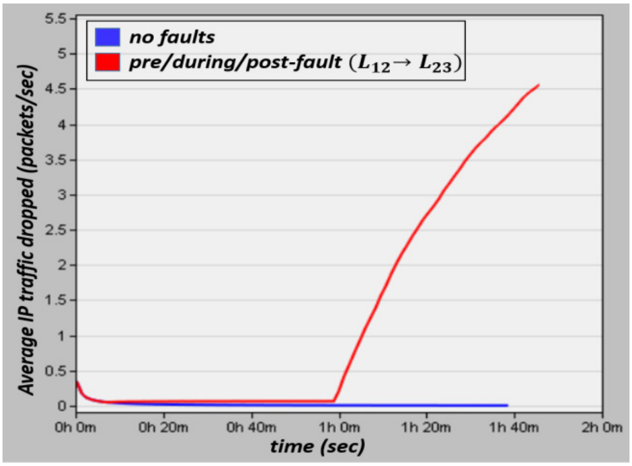

Figure 15. CN2 average IP traffic dropped under A3.

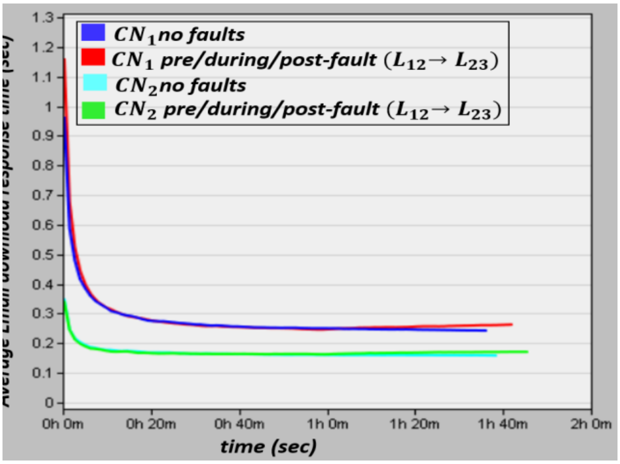

Figure 16. CN1 (respectively, CN2) average email download response time under A3.

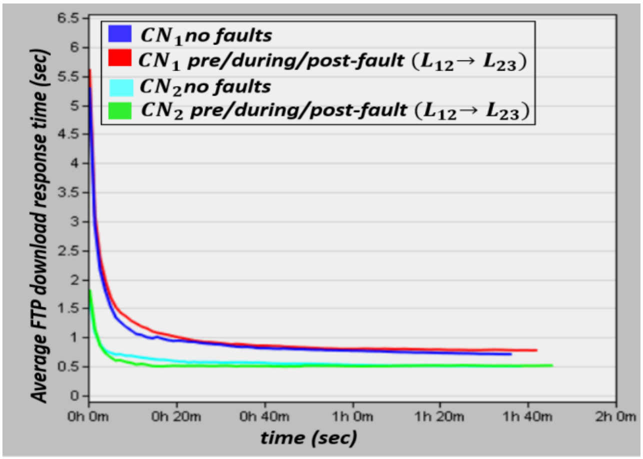

Figure 17. CN1 (respectively, CN2) average FTP download response time under A3.

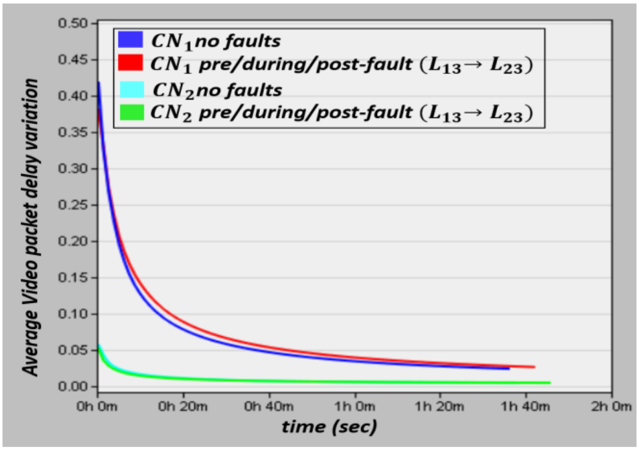

Figure 18. CN1 (respectively, CN2) average video packet delay variation under A3.

Figure 19 shows the average *IP* convergence duration for CN_1 and CN_2 respectively, under A_3. It is clear that CN_2 took less time (7.58 *sec* on average) to converge as compared to CN_1 (7.94 *sec* on average).

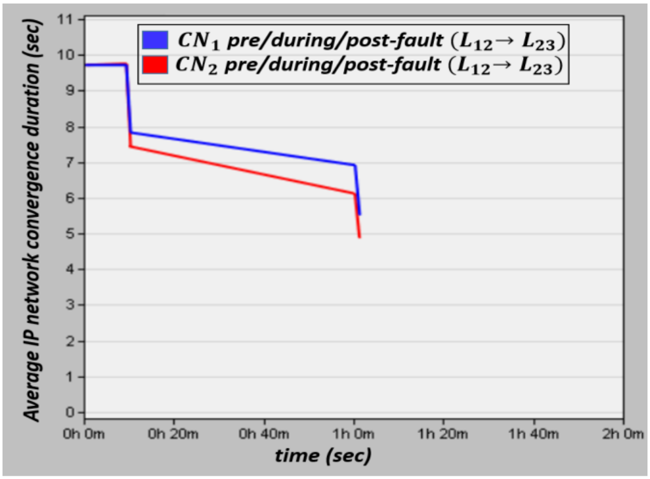

Figure 19. CN1 (respectively, CN2) average IP convergence duration under A3.

Tables 7 and 8 show the data collected for average Email (respectively, FTP) download response time, *D*. Table 9 shows the data for Video packet delay variation, *V,* of each network at t = 540 *sec*, and t = 3600 *sec*, respectively, and the eventual LoP_R under A_3, following equation (2). For CN_1, Email LoP_R = 26.11%, FTP LoP_R = 4.78%, and Video LoP_R = 14.83%. On the other hand, for CN_2, the Email LoP_R = 7.50%, FTP LoP_R = 1.29%, and Video LoP_R = 3.45%. Hence, CN_1 had higher LoP_R than CN_2 over all applications. Moreover, both CN_1 and CN_2 had almost the same LoS_R (CN_1 LoS_R = 3.84×10^{-5}%, and CN_2 LoS_R = 4.55×10^{-5}%). Also, the *RT* of CN_1 was greater than the *RT* of CN_2 , so $LoR(CN_2, A_2) > LoR(CN_1, A_2)$, implying that topology CN_2 was more resilient as compared to CN_1, under the three attack scenarios.

Table 7

Average Email Download Response Time, D of Each Network (sec) and LoP_R *(%) Under* A_3

A_3	D_0, t = 540 *sec*	$D_{(L12)}$, t = 540 *sec*	D_0, t = 3600 *sec*	$D_{(L23)}$, t = 3600 *sec*	LoP_R
CN_1	0.3316	0.3340	0.2429	0.2611	26.11
CN_2	0.1804	0.1788	0.1587	0.1706	7.50

Table 8

Average Ftp Download Response Time, D of Each Network (sec) and LoP_R *(%) Under* A_3

A_3	D_0, t = 540 *sec*	$D_{(L12)}$, t = 540 *sec*	D_0, t = 3600 *sec*	$D_{(L23)}$, t = 3600 *sec*	LoP_R
CN_1	1.1858	1.3649	0.7682	0.8049	4.78
CN_2	0.6863	0.5793	0.5045	0.5110	1.29

Table 9

Average Video Packet Delay Variation, V of Each Network and LoP_R *(%) Under* A_3

A_3	V_0, t = 540 *sec*	$V_{(L12)}$, t = 540 *sec*	V_0, t = 3600 *sec*	$V_{(L23)}$, t = 3600 *sec*	LoP_R
CN_1	0.1411	0.1556	0.0344	0.0395	14.83
CN_2	0.0180	0.0157	0.0058	0.0060	3.45

The experimental results show that while both CN_1 and CN_2 had same users, and services, yet, following ***Definition 3.*** CN_2 was more resilient as compared to CN_1 under the three attack scenarios, owing to their topological difference. Hence a network designer may suggest to use CN_2 design as opposed to CN_1.

CONCLUSION

In this work, a new measure for comparing Level-of-Resilience (*LoR)* for communication networks was proposed. This measure was based on examining Level-of-Stability-Reduction (LoS_R), as measured by percentage of *IP* traffic dropped, Level-of-Performance-Reduction (LoP_R), as measured by percentage of reduction in application Quality-of-Service (*QoS*) latency parameter, and the network Recovery-Time (*RT*), as measured by convergence time, under various attack scenarios. Future work could involve a model-based approach for generating such attack scenarios. Examples were illustrated to compare the *LoR* of two different communication network topologies under three different attack scenarios. While *RIP* was implemented here as a routing protocol, other dynamic routing protocols such as OSPF and EIGRP could be introduced. Each of these protocols has its own routing process and hence, may incur different *LoR* for same topology and attack sequence. It was shown that the placement of network resources could affect the network resilience, as indicated by the *LoR* metric. Thus, using this metric, alternate network designs could be analyzed and evaluated to achieve a best-case resilience utilizing the given set of resources (of nodes and connectivity).

APPENDIX

In this appendix, the modeling data for the communication networks CN_1 **and** CN_2 **that were used as running examples are provided.**

Table 10

Applications Configuration for both CN_1 and CN_2

Traffic type	Supported LANs	Application attributes	Traffic size (byte)
FTP	LAN_1, LAN_2, LAN_3, LAN_4	download inter arrival time (seconds) exponential (with mean 360)	Constant (50000)
Email	LAN_1, LAN_3, LAN_4	Send/receive inter arrival time (seconds) exponential (with mean 10)	Constant (2000)
Video conferencing	LAN_2, LAN_3	Incoming/outgoing stream inter arrival time (seconds) exponential (with mean 4)	Incoming/ outgoing stream frame size constant (17280)

Table 11

Node Models in Use for Both CN_1 and CN_2

Nodes	Model
3 routers (with RIP protocol)	Eathernet_4_slip8_gtwy node
4 LANs	10BaseT_LAN
1 Internet (IP)	ip32_cloud
2 servers (FTP, Email)	Ethernet_server
1 video workstation	Ethernet_wkstn

Table 12

Link Models in Use for Both CN_1 and CN_2

Nodes	Model	Bandwidth
Among routers; to IP and Email	PPP_DS1	1.544 Mbps
Other links	Ethernet 10baseT	10Mbps

REFERENCES

Alvarez, C., Blesa, M., & Serna, M. (2011). The robustness of stability under link and node failures. *Theoretical Computer Science*, *412*, 6855-6878. Elsevier.

Barker, K., & Ramirez-Marquez, J. E. (2016). *Infrastructure network resilience.* Retrieved from EPFL International Risk Governance Center website: https://www.irgc.org/riskgovernance/resilience/

Baroud, H., Ramirez-Marquez, J. E., Barker, K., & Rocco, C. M. (2014). Stochastic measures of network resilience: Applications to waterway commodity flows. *Risk Analysis*, *34* (7), 1317-1335.

Center for Applied Internet Data Analysis (CAIDA). (2016). *Topological resilience in ip and as graphs*. Retrieved from http://www.caida.org/research/topology/resilience/

Chimmanee, S., & Jantavongso, S. (2016). The performance comparison of third generation (3g) technologies for internet services in Bangkok. *Journal of Information and Communication Technology (JICT)*, *15* (1), 1-31.

Cisco Networking Academy (CNA). (2016). *Routing protocols and concepts*. Retrieved from https://www.netacad.com/web/about-us/ccna-exploration

Clayman, S., Clegg, R., Galis, A., & Manzalini, A. (2012). Stability in dynamic networks. *Future Network and Mobile Summit*.

European Network and Information Security Agency (ENISA). (2010). *Measurement frameworks and metrics for resilient networks and services*: *Technical report*.

Farid, A., (2015). Static resilience of large flexible engineering systems: Axiomatic design model and measures. *IEEE Systems Journal*, 1-12. doi: 10.1109/JSYST.2015.2428284.

Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., Mangoubi, R., & Linkov, I. (2016). Operational resilience: Concepts, design and analysis. *Scientific Reports*. doi: 10.1038/srep19540

Heck, H., Kieselmann, O., & Wacker, A. (2016). Evaluating connection resilience for self-organizing cyber-physical systems. *Proceedings of* *the 10th International Conference on Self-Adaptive and Self-Organizing Systems*.

Ibrahim, M., Chen, J., & Kumar, R. (2016). A resiliency measure for electrical power systems. *Proceedings of the 13th International Workshop on Discrete Event Systems*.

Kuipers, F., Wang, H., & Van Mieghem, V. (2005). The stability of paths in a dynamic network, *Proceedings of the CoNEXT Conference*. doi: 1-59593-097-X/05/0010

Kwasinski, A. (2015). Numerical evaluation of communication networks resilience with a focus on power supply performance during natural disasters. *Proceedings of IEEE International Telecommunications Energy Conference*.

Liu, G., & Ji, C. (2009). Scalability of network-failure resilience: Analysis using multi-layer probabilistic graphical models. *IEEE/ACM Transactions on Networking*, *17* (1), 319-331.

Matta, J., (2014). *Comparing the effectiveness of resilience measures*. Southern Illinois University Edwardsville, USA.

Menth, M., Duelli, M., Martin, R., & Milbrandt, J. (2009). Resilience analysis of packet-switched communication networks. *IEEE/ACM Transactions on Networking*, *17* (6), 1950-1963.

Mohammad, A., Hutchison, D., & Sterbenz, J. (2006). Towards quantifying metrics for resilient and survivable networks. *Proceedings of the 14th IEEE International Conf. on Network Protocols (ICNP)*, 17-18.

O'Rourke, T. D., (2007). Critical infrastructure, interdependencies, and resilience. *The Bridge*, *37* (1), 22–29.

Riverbed Technology Incorporation (RTI). (2016). *Opnet modeler*. Retrieved from http://media-cms.riverbed.com/documents/download.html

Salles, R. M., & Jr, D. A. M. (2011). Strategies and metric for resilience in computer networks. *The Computer Journal Advance Access*, Oxford University Press.

Sethi, A. S, & Hnatyshin, V. Y. (2013). *The practical OPNET user guide for computer network simulation*. CRC Press, Tayler and Frances Group.

Shah, A., & Waqas, J. R. (2013). Performance analysis of RIP and OSPF in network Using OPNET. *International Journal of Computer Science*, *10* (6), 1694-0784.

Shi, J. J., & Fonseka, J. P. (1997). Analysis and design of survivable telecommunications networks. *IEE Proceedings-Communication*, *144* (5), 322–330.

Shirazi, F., Diaz, C., Mullan, C., Wright, J., & Buchmann, J. (2013). Towards measuring resilience in anonymous communication networks. *Proceedings of the 6th Workshop on Hot Topics in Privacy Enhancing Technologies*.