Minimization of Vulnerability for a Network under Diverse Attacks

Jose Emmanuel Ramirez-Marquez[a*] and Claudio Rocco[b]

[a] School of Systems and Enterprises, Stevens Institute of Technology, Hoboken, NJ, USA

[b]Facultad de Ingeniería, Universidad Central de Venezuela, Caracas, Venezuela

Abstract: This paper describes an approach to minimize the vulnerability of a network under a defender attacker context. To do so, vulnerability is defined in the context of a resilience-building framework and corresponding mathematical formulations are provided. The solution to network optimization model is based on a three-phased approach consisting on identifying Pareto optimal defense strategies with respect to cost and vulnerability for a known set of network attacks. These solutions are then utilized to identify the network defense strategy that can offer the best protection against any of the attacks. Examples are used to illustrate the approach.

Keywords: Resilience; vulnerability; networks; multi-objective; optimization.

1. INTRODUCTION

During the last decade the concepts of reliability, vulnerability, survivability and resilience as applied to systems have become commonplace and widely discussed. For the last 50 years reliability engineering, theory and methods, have been continuously used to satisfy key stakeholder requirements in a myriad of systems and applications [1]. Among reliability engineers, analysts and researchers there is a standard theory that is understood throughout these communities.

When considering the concepts of vulnerability, survivability and resilience there is neither standard theory nor common language understood among and within these different communities. For example, in the transportation context [2] presents vulnerability as a concept describing "…susceptibility to incidents that can result in considerable reductions in road network serviceability". This definition immediately adds two additional paradigms to be considered: susceptibility and serviceability. Recently, in the same context, [3] describe vulnerability as "…the weakness of a network…" Similarly, survivability has been described as "the capability of a system to fulfill its mission, in a timely manner, in the presence of threats such as attacks or large-scale natural disasters [4]. However, DoD Regulation 5000.2-R states that survivability is "…the capability of a system and crew to avoid or withstand a man-made hostile environment without sustaining an impairment of its ability to accomplish its designated mission. Survivability consists of susceptibility, vulnerability, and recoverability." In fact, Castet and Saleh [5] note that in the engineering context, the concepts of survivability and resilience are sometimes used interchangeably. Finally, for the concept of resilience [6] describes it as related to "…the speed at which an entity or system recovers from a severe shock to achieve a desired state…". However, according to [7], "resilience can be expressed as the post-disruption fraction of demand that can be satisfied by using specific resources while maintaining a prescribed level of service." The reader should note the different measurement in these two definitions: speed in [6] and demand in [7].

From the authors' perspective, the issue at hand is first of definition: a single concept, resilience, is currently used to define one too many ancillary concepts. Thus, due to the conflicting perspectives in the paradigms discussed, this paper has a two-fold contribution: first, to clarify the concepts of vulnerability and survivability as complementary to the resilience framework described in [8] and [9] and second, to provide an optimization based vulnerability reduction approach against diverse number of attacks on a network.

The remaining sections of the paper are organized as follows: Section 2 presents the first contribution of the paper, discussing in detail the resilience framework. Section 3 describes the approach to reduce vulnerability in networks when considering a defender attack contest while section 4 presents examples and results. Finally conclusions are given in section 5.

* *jmarquez@stevens.edu*

2. RESILIENCE FRAMEWORK

With respect to the first contribution, Figures 1.a and 1.b present the resilience building framework as described by [10] and developed based on the model by [9]. In this illustration a system provides a service that is measured or assessed via service function φ(). The system experiences three different states:

Stable Original State (Reliability Theory) – The normal behavior of the system is considered in the interval t_e-t_0. The theory of Reliability Engineering [1] provides models and techniques to analyze and measure the probability that under normal conditions the failure time is greater than some value t: $R(t)=P(T>t)$, $t \in (t_0, t_e)$. In reliability engineering, the period of time t_e-t_0 corresponds to the system time to failure, where at time t_e, a failure event occurs. In the context of reliability failures occur due to events that are intrinsic to the system.

System Disruption (Vulnerability Theory) – The methods [11,12,13] in this area are used to: i) understand how disruptive events affect the service function –for example by analyzing probability that a disruptive event does not affect the service function below some threshold b: $P(\varphi(t)>b|e_j)$– and ii) identifying the components that are critical to the system (i.e. those components that when "degraded" affect system service function the most). As described in figures 1.a and 1.b, the vulnerable period is contained in the interval t_d-t_e. The difference between these two figures is that Figure 1.a considers service functions for which decreasing values correspond to system degradation: throughput, flow, jobs, number of satisfied costumers, etc.. In contrast, Figure 1.b considers those service functions for which increasing values correspond to system degradation: delay, unsatisfied customers, areas without power, etc… Vulnerability and Survivability are strongly related; from this manuscripts perspective, survivability is the study of methods to minimize the vulnerability of systems, mathematically (for the case of Figure 1.a): Min $\varphi(t_e)$-$\varphi(t_d)$.

System Recovery (Resilience Theory) – Recently, mathematical models and methods have been proposed in different areas to understand the recovery of the system service function from some disruptive event e_j. As described in both figures 1.a and 1.b the recoverability period is contained in the interval of lenght t_f-t_d. At the end of this period the service function enters a new recovered state, which may or may not be identical to the original state. The main research question in this area is to understand how restoration policies affect the system recoverability [4, 9, 14, 15].

It is important to note that the system resilience process is a function of time that can be quantified for different service functions and for different disruptive events. To clarify, one cannot discuss system resilience in the absence of system vulnerabilities (i.e. no system disruption implies no system resilience process) and resilience should be discuss in the context of time (i.e. the resilience of the system at time t.) Based on the framework described in Figure 1.a, and for deterministic cases, system resilience has been defined by [9] as the ratio of restoration at time t_r, $\varphi(t_r \mid e_j)-\varphi(t_d \mid e_j)$, to losses up to time t_d, $\varphi(t_0)-\varphi(t_d \mid e_j)$, mathematically as in equation 1:

$$Я\varphi(t_r|e_j)=\frac{\varphi(t_r \mid e_j)-\varphi(t_d \mid e_j)}{\varphi(t_0)-\varphi(t_d \mid e_j)} \qquad \forall e_j \in D,\ t_r \in (t_s\ ,\ t_f) \qquad (1)$$

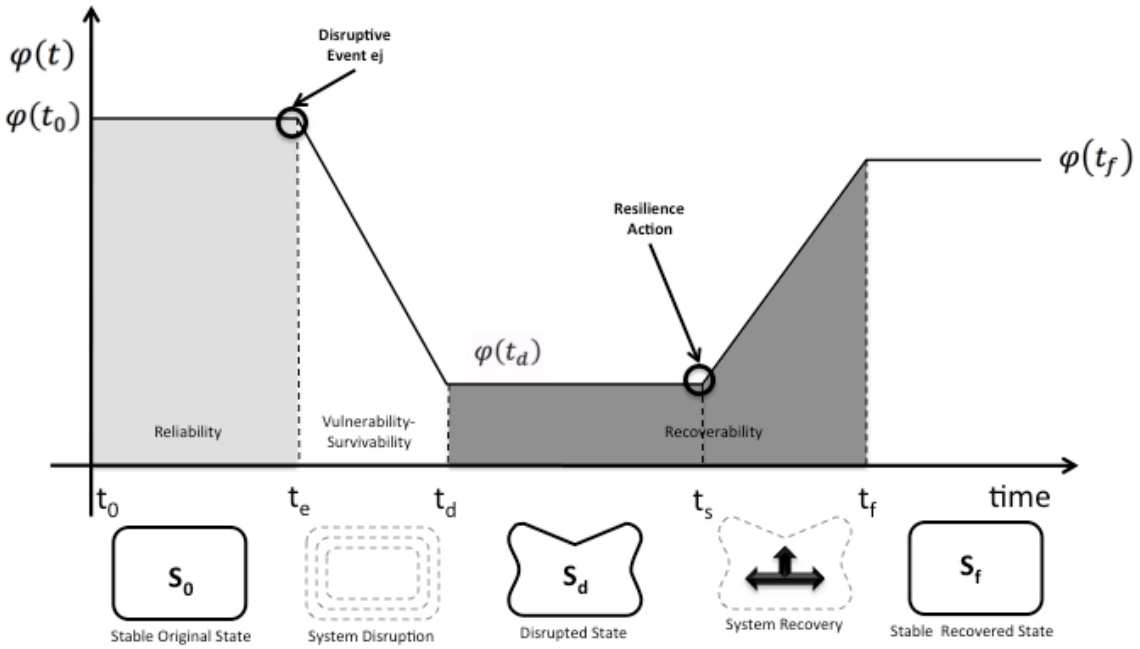

Figure 1a: Decreasing Service Function Resilience Process Illustration

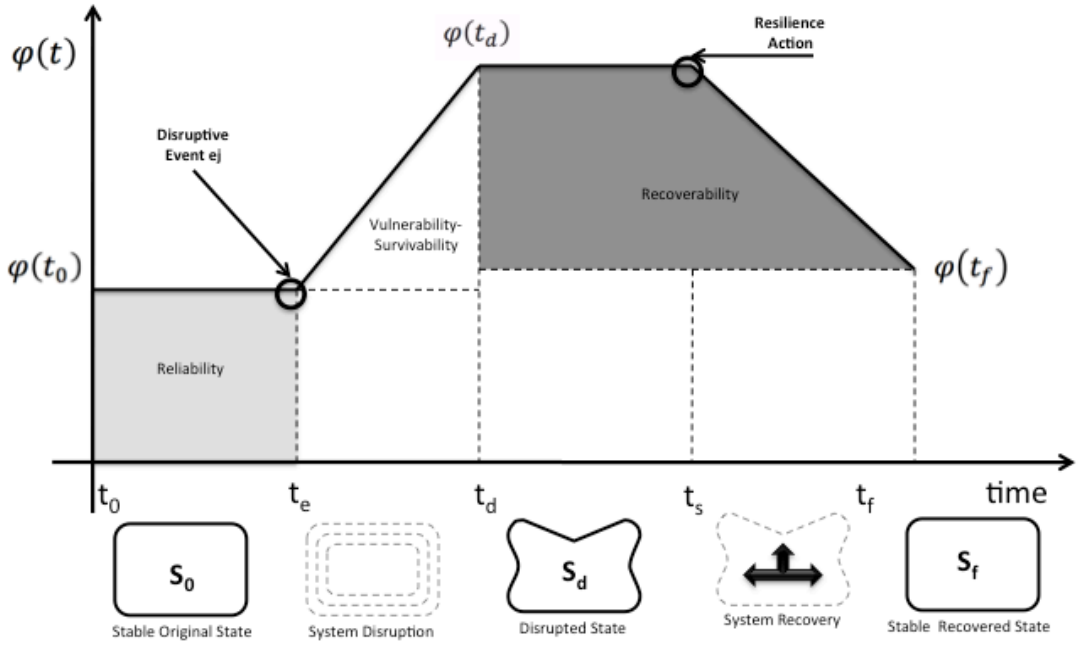

Figure 1b: Increasing Service Function Resilience Process Illustration

Equivalently, based on the framework described in Figure 1.b, and in for deterministic cases, system resilience can be defined as the ratio of restoration at time t_r, $\varphi(t_d \mid e_j) - \varphi(t_r \mid e_j)$, to degradation up to time t_d, $\varphi(t_d \mid e_j) - \varphi(t_0)$, mathematically as in equation 2:

$$Я\varphi(t_r|e_j) = \frac{\varphi(t_d \mid e_j) - \varphi(t_r \mid e_j)}{\varphi(t_d \mid e_j) - \varphi(t_0)} \qquad \forall e_j \in D,\ t_r \in (t_s, t_f) \qquad (2)$$

A number of studies have described related metrics, for example: [15] provide a temporal description of resilience but no mathematical formulation, [7] provide a demand based perspective, and [Rose 2007] analyzes at the economic impact of resilience. However the time dependent description of these two equations is novel and equation (2) is for the first time proposed.

3. NETWORK VULNERABILITY

To address the second contribution, consider that as described by [10] the denominator of equation 1 represents how vulnerable the system is with respect to event e_j: $V(e_j)=\varphi(t_0)-\varphi(t_d)$. And note that $Я_F(t_r|e_j)\rightarrow\infty$ as $V(e_j)\rightarrow 0$. Moreover, $V(e_j)\rightarrow 0$ as $\varphi(t_d)\rightarrow\varphi(t_0)$. Thus, one can claim that the system is survivable to an event as $V(e_j)\rightarrow 0$.

To consider a network context, let G (N, A) represent a capacitated network with known source node s, and sink node t. N represents the set of nodes, and $A=A_1\cup A_2$ where, $A_1=\{(s,i), (j,t) \mid 1 < i,j < n\}$ and $A_2 = \{(i,j) \mid 1 < i\ , j < n\}$ represent the set of links. For G(N, A), $k_{ij}(a_{ij})$ an element of network state vector $\mathbf{k}$, represent the capacity vector of link (i,j), where $a_{ij}=0$ if link (i,j) has been destroyed and $a_{ij}= 1$ if link (i,j) is in its normal state. Under this description, $0=k_{ij}(0)< k_{ij}(1)$ and $\mathbf{k}= (k_{s1}(a_{s1}), k_{s2}(a_{s2}),.., k_{st}(a_{st}), k_{12}(a_{12}),\ldots, k_{ij}(a_{ij}),.., k_{nt}(a_{nt}))$ describes the current capacity of each link in the network.

In the context of this paper, G(N,A) can be disrupted by disruptive event $\mathbf{e}_k$ initiated by an adversary, where $\mathbf{e}_k$ contains a disruption scenario $\mathbf{e}_k= (e_{s1k}, e_{s2k},.., e_{stk}, e_{12k},\ldots, e_{ijk},.., e_{ntk})$, where $e_{ijk} \in \Re^+$ defines disruption resources e_{ijk} allocated to each link i,j of G(N,A). The assumption in this paper is that a network defender is aware about possible attack scenarios, $\mathbf{e}_k$, in set D, |D|=K, but unaware of the specific event that will take place.

To minimize how vulnerable the network is, the defender can implement a defense strategy $\mathbf{h}= (h_{s1}, h_{s2},.., h_{st}, h_{12},\ldots, h_{ij},.., h_{nt})$, where $h_{ij} \in \Re^+$, describes the defense resources invested to protect link i,j . Based on the defender and attacker strategies, the vulnerability $v_{ij}(\mathbf{t},\mathbf{h})$ of network link i,j can be mathematically described using the ratio form of the attacker-defender contest success function as originally presented in [16, 17]:

$$v_{ij}\left(\mathbf{e}_w,\mathbf{h}_v\right)=\begin{cases}\dfrac{e_{ij}^m}{e_{ij}^m+h_{ij}^m} & \text{if } e_{ij}^m>0\\ 0 & \text{if } t_{ij}^m=0\end{cases} \qquad (3)$$

In (3), the attackers' and defenders' resource allocation for attacking/defending the link between nodes i and j, is dictated by the specific attack and defense strategies $\mathbf{e}_w$ and $\mathbf{h}_v$, respectively. In practical terms, as per (3) the vulnerability of the link i, j can be described as the probability that given attack and defense strategies, the flow capacity for link (i,j) is reduced from $k_{ij}(1)$ to $k_{ij}(0)$. It is important to note that that as described in Ramirez-Marquez et al. [18] the contest intensity m is motivated by the history of warfare. While used in this paper, (3) can be substituted for the appropriate contest function relating attack and defense resources to a probability value. Based on the network and vulnerability representation, $\varphi(\mathbf{k})$: $Z^{|A|} \rightarrow Z^+$ maps a network state vector into a maximum network flow between s and t. Note that whenever $\mathbf{e}_w$ and $\mathbf{h}_v$, are known, the capacity of each link in state vector, $\mathbf{k}$, is a random variable taking the following values with corresponding probabilities:

$$k_{ij}=\begin{cases}k_{ij}(1) & 1-v_{ij}\left(e_w,h_v\right)\\ 0=k_{ij}(0) & v_{ij}\left(e_w,h_v\right)\end{cases}$$

It is important to realize that as defined, k_{ij} is a random variable that takes values as dictated by v_{ij}. Then, $\varphi(\mathbf{k})$ can be analyzed for any possible realization of $\mathbf{k}$ given $\mathbf{e}_w$ and $\mathbf{h}_v$. In this manuscript the performance function or figure-of-merit is the expected flow of the network between nodes *s* and *t* given the defense and attack strategy vectors $\mathbf{e}_w$ and $\mathbf{h}_v$. It can be defined as: $E(\varphi(\mathbf{k})|\ \mathbf{e}_w, \mathbf{h}_v)$.

3.1. Bi-Objective Optimal Network Protection

The Model BO-Vulnerability illustrates the optimization model considered for identifying the best defender's strategy against all events included in set D and at minimum cost. Note that in the first objective, the expected network *s-t* flow in G(N,A) is computed for every event *w*, $\mathbf{e}_w \in$D to identify a defense strategy that maximizes flow or minimizes the flow reduction. The second objective minimizes total defenders cost. The constraints of the model include the flow balance conservation equation (where $f(k_{ij})$ describes the flow through link (i,j), $f(k_{ij}) \in (0, k_{ij}(1))$ and the non-negativity behavior of the decision variable h_{ij}.

Model BO-Vulnerability

$$\underset{v}{Max}\ E\left[\varphi(\mathbf{k}) \mid \mathbf{e}_w, \mathbf{h}_v\right] \quad \underset{v}{Min}\ C(\mathbf{h}_v) \quad \text{for every } \mathbf{e}_w \in \text{D}$$

subject to

$$\sum_{i \mid h_{ij}} f(k_{ij}) - \sum_{k \mid h_{jk}} f(k_{jk}) = 0 \quad \forall j \in \text{N-}\{s,t\}$$

$$\sum_{j \mid h_{sj}} f(k_{sj}) - \sum_{k \mid h_{kt}} f(k_{kt}) = 0 \quad \forall j,k \in \text{N-}\{s,t\}$$

$$h_{ij} \geq 0$$

The solution of Model BO-Vulnerability can be obtained via the following heuristic:

Step 1: Determination of Pareto Fronts for every $\mathbf{e}_w \in$D

For each $\mathbf{e}_w \in$D and based on Ramirez-Marquez et al [19] identify the strategies in set H satisfying Pareto optimality as defined by the following conditions:

Condition 1: Feasible defense strategy $\mathbf{h}'(\mathbf{e}_w)$ dominates a feasible strategy $\mathbf{h}(\mathbf{e}_w)$, iff $C(\mathbf{h}'(\mathbf{e}_w)) \leq C(\mathbf{h}(\mathbf{e}_w))$, $E(\varphi(\mathbf{a})|\mathbf{e}_w, \mathbf{h}'(\mathbf{e}_w)) \geq E(\varphi(\mathbf{a})|\mathbf{e}_w, \mathbf{h}(\mathbf{e}_w))$ and $C(\mathbf{h}'(\mathbf{e}_w)) < C(\mathbf{h}(\mathbf{e}_w))$ or $E(\varphi(\mathbf{a})|\mathbf{e}_w, \mathbf{h}'(\mathbf{e}_w)) > E(\varphi(\mathbf{a})|\mathbf{e}_w, \mathbf{h}(\mathbf{e}_w))$. If no solution dominates $\mathbf{h}(\mathbf{e}_w)$, it is said to be non-dominated.

Condition 2: A defense strategy $\mathbf{h}'(\mathbf{e}_w)$ belongs to the Pareto set H^*, $\mathbf{h}'(\mathbf{e}_w) \in \text{H}^*$, iff $\neg \exists\ \mathbf{h}(\mathbf{e}_w) \in \text{H}$: $\mathbf{h}(\mathbf{e}_w)$ dominates $\mathbf{h}'(\mathbf{e}_w)$.

In this manuscript, any defense strategy $\mathbf{h}'(\mathbf{e}_w)$ satisfying conditions 1 and 2 is considered a Pareto optimal solution of the Model BO-Vulnerability with H^* its corresponding true Pareto set. Based on the description of any $\mathbf{h}(\mathbf{e}_w)$, the set H is of infinite cardinality since there are an infinite number of partitions for h_{ij} For MO problems with infinite solution spaces the true Pareto set can rarely be completely characterized and solution procedures are based on approximating such a set.

The result of this step is a set of Pareto fronts $\mathbf{h}'(\mathbf{e}_w)$, for every $\mathbf{e}_w \in$D. Note that the number of possible defense strategies $\mathbf{h}'(\mathbf{e}_w) \in \text{H}^*$is given by the cardinality of H^*.

Step 2: Behavior of defense strategies for every $\mathbf{e}_w \in$D.

This step analyzes the performance of $\mathbf{h}_v(\mathbf{e}_w) \in \text{H}^*$ under every other attack scenario $\mathbf{e}_u \in$ D, $u \neq w$.

Montecarlo Simulation is used to generate: $E\left[\varphi(\mathbf{k}) \mid \mathbf{e}_u, \mathbf{h}_v(\mathbf{e}_w)\right]$ for every $\mathbf{h}_v(\mathbf{e}_w) \in \text{H}^*$. At the end of

this step, each defense strategy, $\mathbf{h}_v(\mathbf{e}_w) \in H^*$ is characterized by the expected maximum flow or the expected flow reduction achieved for every attack $\mathbf{e}_w \in D$, and its associated cost (i.e., $|D|+1$ values).

Step 3: Determination of the most convenient defense strategy.
As a result of step 2, each defense strategy can be represented as a multi indicator matrix with $|D|+1$ indicators. Multi-indicator matrices represent a set of objects characterized simultaneously by several indicators, criteria or attributes. This structure allows assessing each object, by considering simultaneously different criteria, and defining a ranking to synthesize the global characteristic of each object. Assuming that a defense strategy with lower flow reduction and lower cost is preferred, the strategies could be ranked, for example, from best to worst using a multi-criteria technique.

Multi-criteria ranking techniques are classified as parametric and non-parametric. The first group requires information about decision-maker preferences (e.g., weights assigned to each criterion), while non-parametric techniques do not use such information. In this paper the use of the Copeland Score (CS), a non-parametric technique is used, due to its simplicity.

The approach in this case selects the defense strategy with the largest CS, understood as the number of times a defense strategy is better than other defense strategies and subtracting the number of times that defense strategy is worse than other defense strategies, when they are compared pair-wise for each criterion [20]. Comparisons are made for each criterion and no normalization is required. Copeland Scores assume that each criterion has equal importance. Given a set of n objects, characterized by m criteria $q_j()$, j=1, .., m, the method builds a comparison matrix *C*. Each position *C*(i,l) represents the count of comparison between object i and object l, considering each criterion q_j . If $q_j(i) \geq q_j(l)$ then $C(i,l)=C(i,l)+1$. If $q_j(i) \leq q_j(l)$, then $C(i,l)=C(i,l)-1$. Summing up *C*(i,l) over all objects ($1 \leq l \leq n$), yields the CS(i) of object i. Objects are then ranked using the corresponding CS(i).

For the present case, the Copeland approach is able to identify the best "over all" defense strategy given the set of ALL possible defense strategies derived from the attack scenarios considered, along with the effects derived from Step 2.

4. ILLUSTRATIVE EXAMPLES

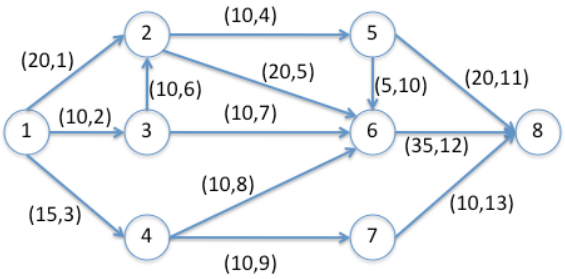

Figure 2: Illustrative Flow Network

To illustrate the proposed approach consider the network presented in Figure 2. Each link in Figure 1 has been assigned two values: capacity and index number, respectively. So for example, the link between nodes 1 and 2 has a capacity of 20 units and is indexed as link 1. In the case of no link failures, the network can handle a maximum flow of 45 units between the source node (node 1) and the sink node (node 8). To illustrate the optimization model and its solution as described in Section 3, an attack budget equal to 520 has been considered for contest intensity m=1 and three different attack scenarios $\mathbf{e}_u$. In each scenario $\mathbf{e}_u$ the attack budget has been equivalently distributed among the following links: $\mathbf{e}_1$: 2,5,9 and 12; $\mathbf{e}_2$: 2,5,6 and 12; and $\mathbf{e}_3$: 1, 2, 11 and 12.

Step1: Determination of Pareto Fronts - The procedure in [18,19] is used to derive the Pareto front for each scenario. The graphical results of the approximate Pareto front obtained for each scenario is displayed in Figure 3. Each point in the frontier represents a defense strategy with its corresponding maximum flow reduction and associated cost. The number of defense strategies derived for each scenario is: 225, 194 and 201 respectively.

Figure 3 allows for an initial understanding of the vulnerability of the network in Figure 2 for the attacks considered. For example, Attack 2 does not has the lowest effect in flow reduction as a function of cost and when compared against attacks 1 and 3. Table 1 shows 7 out of 225 defense strategies of the Pareto optimal set generated for attack 1. Pareto optimal defense strategies associated with attack 1 and evaluating each against attacks 2 and 3. Clearly from Figure 4 it is becomes evident that the defense strategies obtained for attack 1 do not provide as good defense against attack 3 but do relatively fine against attack 2. Table 2 shows the flow reduction for the selected defenses described in Table 1. As illustrated by Table 1, the point with the highest cost in Figure 1 has a value equal to 3709 with an associated expected flow reduction equal to 5.21. In this case, the defender must allocate resources of 911, 892, 709 and 1197 to links 2,5,9 and 12 respectively.

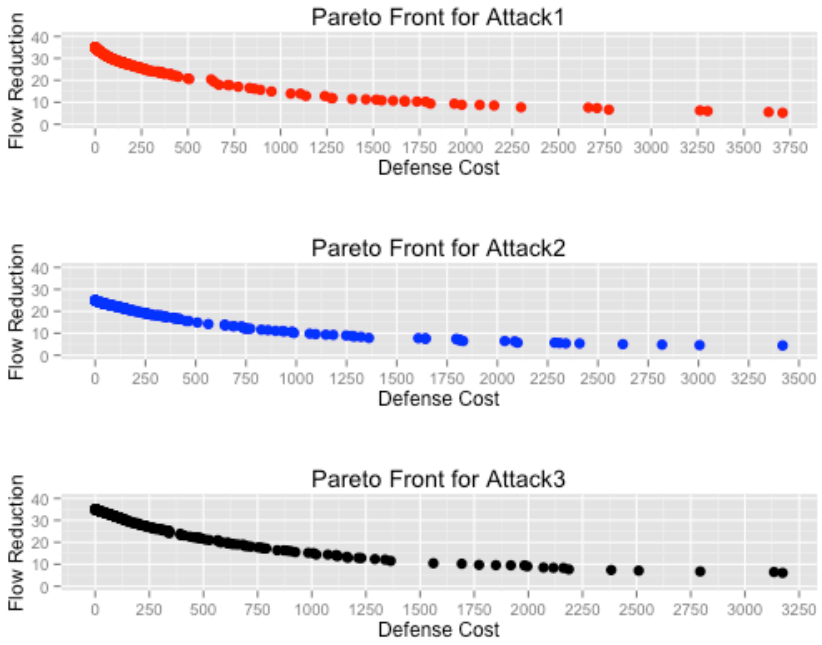

Figure 3: Pareto Fronts for Each Attack

Table 1: Selected Pareto Optimal Defense Strategies under Attack Scenario 1

Def Str	Flow Red.	Cost	Defense Resource Allocated to Links												
			1	2	3	4	5	6	7	8	9	10	11	12	13
a	35.00	0	0	0	0	0	0	0	0	0	0	0	0	0	0
b	29.95	84	0	0	0	0	0	0	0	0	49	0	0	35	0
c	25.08	266	0	15	0	0	33	0	0	0	90	0	0	128	0
d	20.42	626	0	236	0	0	108	0	0	0	157	0	0	124	0
e	14.90	951	0	198	0	0	267	0	0	0	183	0	0	303	0
f	10.24	1783	0	397	0	0	587	0	0	0	191	0	0	608	0
g	5.21	3709	0	911	0	0	892	0	0	0	709	0	0	1197	0

Step 2: Behavior of defense strategies under different attacks - The next step consists on evaluating each of the defense strategies identified in each of the three Pareto fronts described in Figure 3. Figure 4 shows the effect of selecting each of the Defense Strategies Against Attack 1 evaluated on every attack. Figures

5 and 6 show the corresponding plots when considering the Pareto optimal defense strategies associated with attack 2 and 3 respectively and evaluating each, against the remaining attacks
The analysis of figures 4, 5 and 6 illustrates that both the optimal defenses against attacks 1 and 3 do relatively good against attack 2. Yet, both the optimal defenses against attacks 1 and 3 do relatively bad in protecting against attack 3 and attack 1 respectively.

Step 3: Selection of the most convenient defense strategy - The determination of the most convenient defense strategy considering all possible attack scenarios is performed using the Copeland approach. Each defense strategy derived form the optimal defense strategies against attacks 1, 2 and 3 (for a total of 620 strategies) is represented by four criteria: the flow reduction under the three attack scenarios and the cost of the strategy. The defense strategy with the highest Copeland Score is the best "over all" strategy to be selected. Figure 7 shows the Copeland score (when considering all Pareto fronts) for each defense strategy in the Pareto fronts described in Figure 4. Table 3 shows the attributes of the best twenty strategies identified using the Copeland Score approach. Note that, no defense strategy is selected from the third Pareto front.

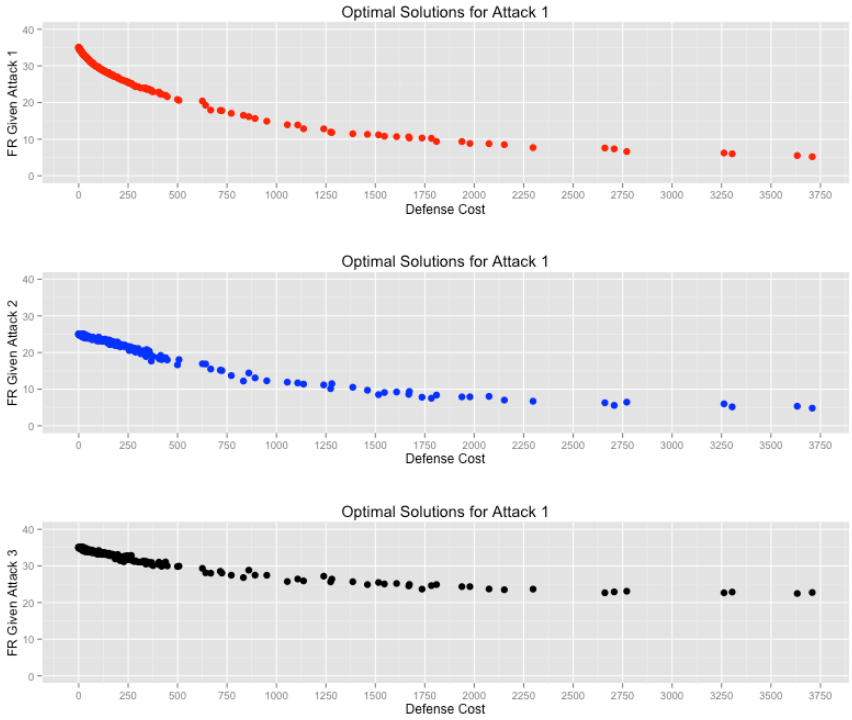

Figure 4: Optimal Defense Strategies Against Attack 1 evaluated on Every Attack

Table 2: Selected Pareto Optimal Defense Strategies under different Attack Scenarios

Defense Strategy	Flow Reduction Given Attack 1	Flow Reduction Given Attack 2	Flow Reduction Given Attack 3	Defense Cost
a	35.00	25.00	35.00	0
b	29.95	24.20	34.11	84
c	25.08	22.18	32.81	266
d	20.42	13.08	27.49	626
e	14.90	16.93	29.33	951
f	10.24	12.29	27.45	1783
g	5.21	7.90	24.35	3709

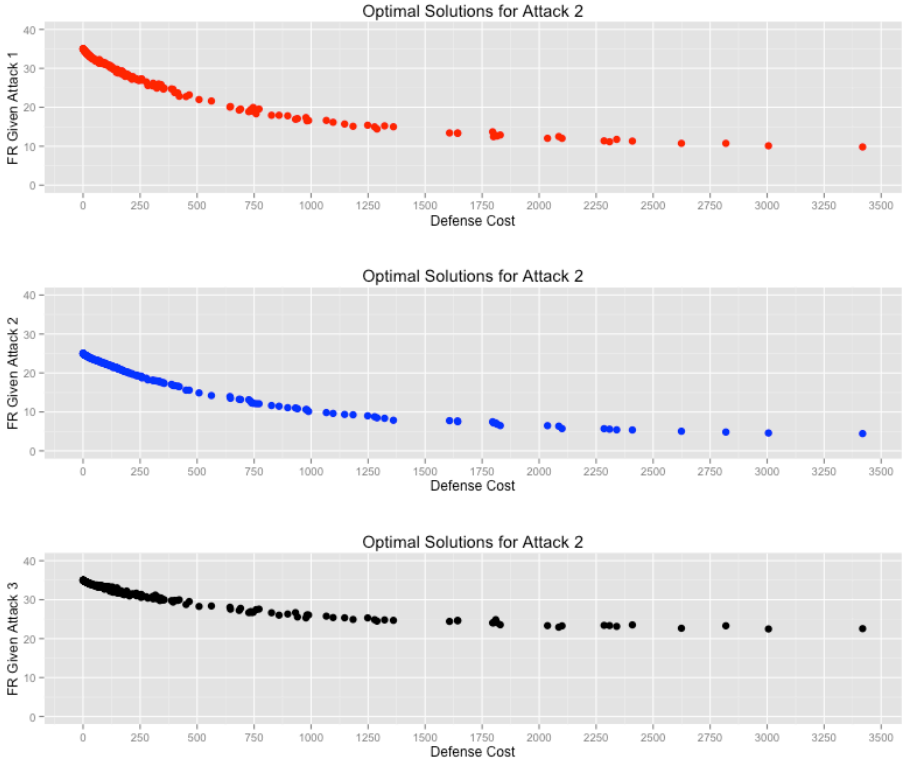

Figure 5: Optimal Defense Strategies Against Attack 2 evaluated on Every Attack

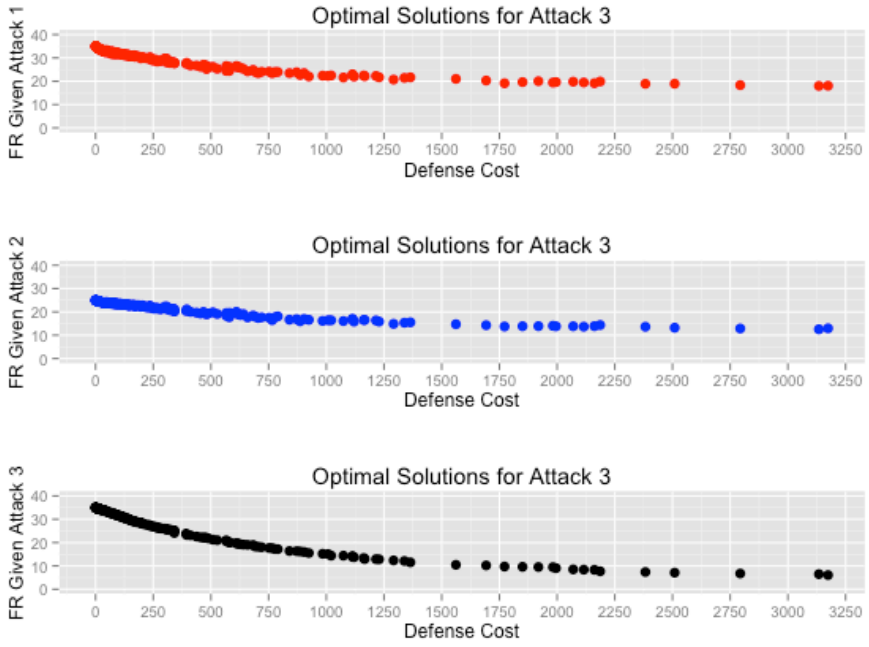

Figure 6: Optimal Defense Strategies Against Attack 3 evaluated on Every Attack

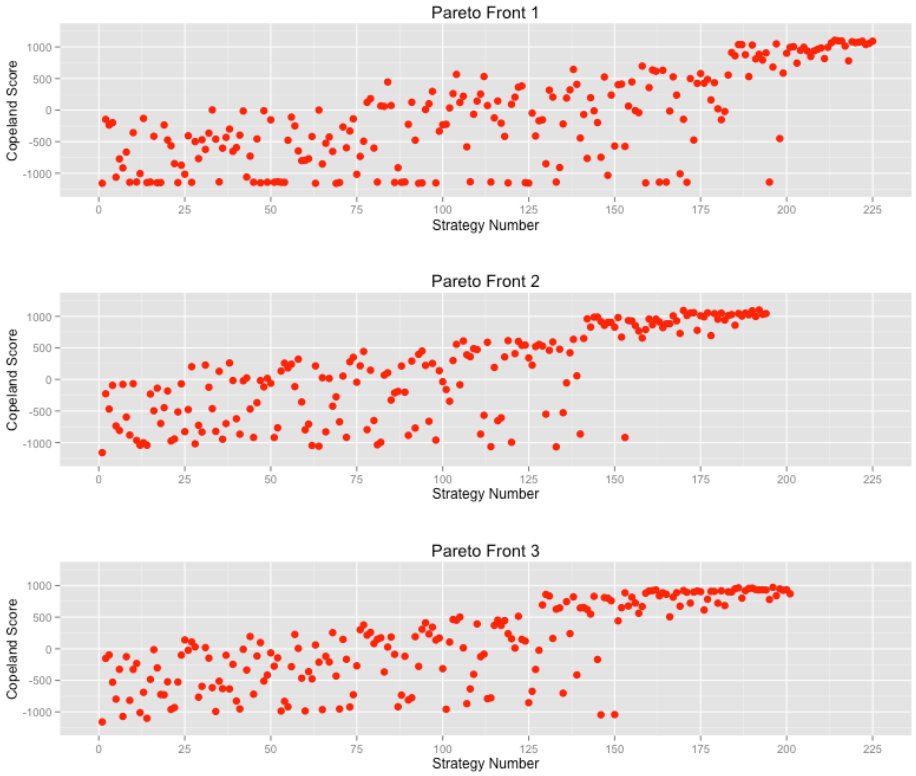

Figure 7: Copeland Score for Each of the Optimal Defense Strategies

Table 3: Attributes for the first best ranked defense strategies.

Rank	Pareto Front, #defense	Flow Reduction Given Attack 1	Flow Reduction Given Attack 2	Flow Reduction Given Attack 3	Defense Cost
1	1,214	5.30	5.35	22.47	3633
2	2,192	10.11	4.15	22.48	3006
3	1,215	5.08	4.83	22.74	3709
4	1,225	7.56	5.58	22.91	2707
5	1,216	6.04	5.18	22.86	3304
6	2,170	9.81	4.67	22.56	3419
7	1,222	8.54	6.29	22.67	2660
8	1,219	6.85	5.99	22.67	3263
9	2,190	10.74	5.65	22.66	2624
10	1,221	7.59	6.46	23.09	2771
11	1,213	8.69	7.02	23.50	2152
12	2,177	11.15	5.87	23.35	2309
13	2,173	10.74	4.99	23.30	2819
14	1,220	11.30	7.81	23.66	1736
15	1,197	9.83	7.53	24.62	1783
16	1,224	8.72	6.71	23.66	2297
17	2,188	12.02	6.35	23.28	2101
18	2,181	12.49	6.39	22.94	2086
19	2,186	11.38	5.92	23.41	2285
20	2,194	12.03	6.48	23.33	2037

5. CONCLUSIONS AND FUTURE RESEARCH

This paper clarifies the concept of resilience as a time based metric in the systems context. The resilience framework has been defined for the first time for both increasing and describing service functions as a function of time. Moreover, the framework presented ties together the engineering concepts of reliability, vulnerability, survivability and recoverability as a continuum in the resilience analysis. The manuscript also provides an optimization approach to reduce the vulnerability of a network for different attack scenarios as a function of flow and cost.

References

[1] Elsayed, E. (1996) " Reliability Engineering", Prentice Hall, New Jersey.

[2] Berdica, K. (2002), "An introduction to road vulnerability: what has been done, is done and should be done", Transport Policy, Vol. 9, No. 2, pp. 117-127

[3] Knoop, V., Hoogendoorn, S. and Van Zuylen, H. (2007) Approach to Critical Link Analysis of Robustness for Dynamical Road Networks, In Traffic & Granular Flow, Springer Verlag, Berlin, pp. 393–402

[4] Sterbenz, J., Hutchinson, D., Çetinkaya, E. Jabbar, A., Rohrer, J, Schöller, M. and Smith P. (2010) "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines", Computer Networks, Vol. 54., pp1245-1265.

[5] Castet, J. and Saleh, J. (2008) "Survivability and Resiliency of Spacecraft and Space-Based Networks: A Framework for Characterization and Analysis" American Institute of Aeronautics and Astronautics, AIAA Technical Report 2008-7707.

[6] Rose, A. (2007) "Economic resilience to natural and man-made disasters: Multi- disciplinary origins and contextual dimensions," Environmental Hazards, Vol. 7, No. 4, pp. 383–98.

[7] Nair, R., Avetisyan, H. and Miller-Hooks, E. (2010) "Resilience Framework for Ports and Other Intermodal Components" Transportation Research Record: Journal of the Transportation Research Board, No. 2166, Transportation Research Board of the National Academies, Washington,D.C., pp. 54–65

[8] Ramirez-Marquez, J.E. and Rocco, C. (2012) "Vulnerability Based Robust Protection Strategy Selection in Service Networks", Computers and Industrial Engineering, Vol.63, No.1, pp.235-242

[9] Henry, D. and Ramirez-Marquez, J.E., (2012) "Generic Metrics and Quantitative Approaches for System Resilience as a Function of Time" Reliability Engineering & System Safety, Vol. 99, No. 1, pp.114-122

[10] Ramirez-Marquez, J.E. and Rocco, C. (2012) "Towards a Unified Framework for Network Resilience" Proceedings of the Third International Engineering Systems Symposium CESUN 2012, June 18-20, Delft, Netherlands.

[11] Apostolakis, G.E., Lemon, D.M. (2005), "A Screening Methodology for the Identification and Ranking of Infrastructures Vulnerability Due to Terrorism." Risk Analysis, vol. 25, No. 1, pp. 361-376

[12] Bier, V., Haphuriwat, N., Menoyo, J., Zimmerman R. and Culpen, A., (2008) "Optimal resource allocation for defense of targets based on differing measures of attractiveness" Risk Analysis, Vol. 28, No. 3, pp. 763-770.

[13] Hausken, K. (2008) "Strategic defense and attack for series and parallel reliability systems", European Journal of Operational Research, Volume 186, Issue 2, pp. 856-888

[14] Haimes, Y.Y. 2009. On the Definition of Resilience in Systems. Risk Analysis, 29(4): 498-501.

[15] Sterbenz, J. P., Çetinkaya, E. K., Hameed, M. A., Jabbar, A., Qian, S., & Rohrer, J. P. (2011). Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation. Telecommunication Systems, 1-32.

[16] Skaperdas, (1996) "Contest success functions", Economic Theory Vol. 7, pp. 283-290
[17] Levitin, G. and Hausken, K. (2008) “Protection vs. redundancy in homogeneous parallel systems” Reliability Engineering & System Safety, Vol. 93, pp. 1444–1451.
[18] Ramirez-Marquez, J. E., Rocco, C. and Levitin, G. (2011) “Optimal Network Protection Against Diverse Interdictor Strategies” Reliability Engineering & System Safety, Vol. 96, No.3, pp. 374-382.
[19] Ramirez-Marquez, J.E., Rocco, C. and Levitin, G. (2012) “Network Protection Against Diverse Attacks - A Multi-objective Perspective” Proceedings of ESREL 2012, Helsinki, Finland.
[20] Al-Sharrah G. (2010) “Ranking Using the Copeland Score: A Comparison with the Hasse Diagram”, Journal of Chemical Information Models, Vol. 50, pp :785–791