Poster: Towards Quantifying Metrics for Resilient and Survivable Networks

Abdul Jabbar Mohammad*‡, David Hutchison†, and James P.G. Sterbenz*†
*Information and Telecommunication Technology Center (‡student)
The University of Kansas, Lawrence, Kansas 66045–7612
Email: {*jabbar,jpgs*}@*ittc.ku.edu*
†InfoLab21, Lancaster University, Lancaster, LA1 4WA, UK
Email: {*dh,jpgs*}@*comp.lancs.ac.uk*

***Abstract*— This poster discusses methods to characterize the *resilience* of networks to a number of challenges and attacks, with the goal of developing quantifiable metrics to determine the degree of the network's resilience. We formalize resilience as points in a two-dimensional state space quantifying network characteristics, from which network service performance parameters can be derived. One dimension represents the network as normally operating, partially degraded, or severely degraded. The other dimension represents network service as acceptable, impaired, or unacceptable. Our goal is to initially understand how to characterize network resilience, and ultimately how to guide network design and engineering toward increased resilience.**

I. Introduction and Motivation

Considerable research has been conducted on different aspects of resilient and survivable networks. In this work, we define a *resilient network* [1]–[3] as a network that has the ability to operate and maintain an acceptable level of service under the presence of adverse conditions. These include various factors such as: natural faults of network components; failures due to misconfiguration or operational errors; large-scale natural disasters (e.g. hurricanes, earthquakes, ice storms, tsunami, floods); attacks against the network hardware, software, or protocol infrastructure (from recreational crackers, industrial espionage, terrorism, or warfare); unpredictably-long-delay paths either due to length (e.g. satellite) or as a result of episodic connectivity; weak, asymmetric, and episodic connectivity of wireless channels; high-mobility of nodes and subnetworks; and unusual but legitimate traffic load (e.g. flash crowds).

The umbrella of resilient and survivable networks thus covers commonly known categories such as challenged, delay- and disruption-tolerant networks, mobile ad-hoc and personal networks, and sensor networks. The vast region of this resilient network space currently lacks rigorous and efficient representation methods.

Though there has been some preliminary research toward providing analytical definitions of survivability and resilience [4], there is further need for quantitative analysis of the problem. One of the difficulties is the lack of standard metrics to define the network space. In the following sections, we discuss the use of operational metrics and service parameters to represent network states. The resilience of the network is then evaluated as it moves through various states. The goal is to initially characterize network resilience and ultimately to understand how to design and engineer networks with a higher resilience.

II. Network Characterization

Network characterization is a method of defining networks using fundamental properties formulated in concise metrics. A set of well defined metrics not only enables a clear representation of different types of network, but also allows transformation of a given network from one state to another. However, such a set of metrics may not guarantee that all the possible network scenarios can be uniquely represented. Our objective is to present a tractable solution that captures the inherent complexity, but can be efficiently used to quantify resilience for most network scenarios.

In order to develop an efficient network taxonomy, the first step is to identify the fundamental properties that affect the performance and the resilience of the network. To this effect, we have identified a comprehensive set of network properties that are broadly classified in six categories as shown in Table I[1]. The second step involves deriving a smaller set of independent metrics. A network operational metric is a function of one or more network parameters of Table I. Ongoing research in this area is focused on deriving such a set of metrics that can represent a given network completely but are easy to understand and use.

TABLE I
Summary of Network Characteristic Parameters

Density	number of nodes, area of spread, distribution pattern, rate of topology change
Mobility	velocity of the node, mobility model, predictability
Channel	capacity distribution, propagation model, bit error rate, error rate model
Node resources	electrical power, computing power, memory, tx/rx power, location awareness
Network traffic	distribution, packet size, source/sink placement, QoS
Derived properties	degree of connectivity, propagation delay, queuing delay, node willingness

[1]Refer to www.ittc.ku.edu/resilinets for details that are omitted here.

III. Resilience and Survivability

Previous research efforts [4]–[6] have presented analytical definitions of some resilient properties (e.g. reliability, availability). We use network metrics discussed in the previous section to quantify resilience. We formulate that every adverse event transforms the network from one state to another based on the severity of the event. Hence, network resilience can be evaluated in terms of the various network states that can be supported with the existing system. Secondly, an acceptable level of service of a network under adverse conditions can also be quantified using representative functions based on application requirements such as goodput and delay. These are termed as service parameters. A comprehensive view of resilience, therefore, requires the knowledge of quantitative performance of the network in all the states that it may visit under normal or adverse conditions. We now develop mathematical expressions for network states and acceptable performance.

Let $\{n_1, n_2, \ldots, n_i, \ldots, n_x\}$ be the set of x network operational metrics as discussed in section II. Let S_k be the k^{th} state of any given network. The network characteristics of this state can be defined with the help of metrics as $\mathbb{N}_k = \{N_{1k}, N_{2k}, \ldots, N_{ik}, \ldots, N_{xk}\}$. A member N_{ik} in the set $\mathbb{N}_k$ is in itself a set of valid values bounded by $[\underline{n}_{ik}, \overline{n}_{ik}]$, representing the lower and upper limit of the i^{th} operational metric. We can now define $N_{ik} \equiv [\underline{n}_{ik}, \overline{n}_{ik}]$. Thus N_{ik} represents the set of i^{th} metric values that correspond to the network state S_k.

Definition A. *If the i^{th} operational metric of a network at a given instant of time t is $n_i(t)$, then the necessary condition for the network to be in state S_k is $\forall \{i : N_{ik} \in \mathbb{N}_k\}, n_i(t) \in N_{ik}$.*

Next we consider the problem of determining the values of $\underline{n}_{ik}$ and $\overline{n}_{ik}$. The network boundaries for each state are determined by the desired performance of that state.

Let $\{p_1, p_2, \ldots, p_j, \ldots, p_y\}$ be the set of y service parameters that represent the performance of the network in a given state at a given instant. The service of the network in k^{th} state, S_k, can be defined as $\mathbb{P}_k = \{P_{1k}, P_{2k}, \ldots, P_{jk}, \ldots, P_{yk}\}$. A member P_{jk} in the set $\mathbb{P}_k$ is in itself a set of values bounded by $[\underline{p}_{jk}, \overline{p}_{jk}]$, representing the lower and upper limit of the j^{th} service metric. We can define $P_{jk} \equiv [\underline{p}_{jk}, \overline{p}_{jk}]$.

Definition B. *If the j^{th} service parameter of a network at a given time instant t is $p_j(t)$, then the necessary condition for the network to be in state S_k is $\forall \{j : P_{jk} \in \mathbb{P}_k\}, p_j(t) \in P_{jk}$.*

Hence, a network state, S_k, is defined by the tuple $(\mathbb{N}_k, \mathbb{P}_k)$. For simplicity, we divide the operational and service space of the network in to three regions each, as shown in figure 1. Let the current state of the network be S_A. Following the occurrence of an adverse event, the network stays in its current state if the change in the i^{th} metric, n_{iA}, does not exceed the allowed range $[\underline{n}_{ik}, \overline{n}_{ik}]$ and the service parameters remain with in limits $[\underline{p}_{jA}, \overline{p}_{jA}]$. If an adverse event does result in one or more metrics exceeding their range in the current state, the network proceeds to a different state. Say, for a small adverse event, network moves to state S_B in which service parameters are in the limits $[\underline{p}_{jB}, \overline{p}_{jB}]$. The network may be engineered so that for a given application, both S_A and S_B lie in the normal operating region, in which the service is acceptable. On the other hand, adverse events of higher magnitude may drive the network to a state S_C in the partially degraded region with impaired service, or to a state S_D in severely degraded region with unacceptable service parameters. The range of network operational metrics for which the network will remain in each state is clearly quantified along with the expected service in that state.

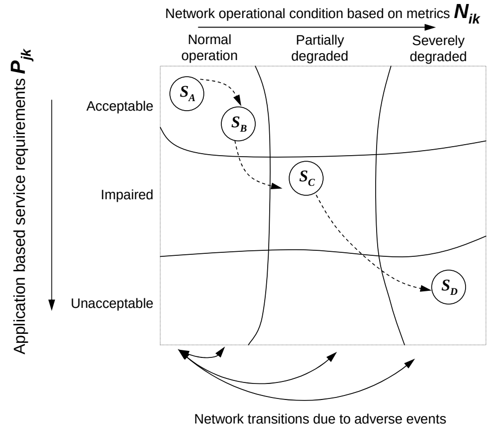

Fig. 1. Network states in the given operating region

IV. Conclusion and Future Work

We believe that characterizing network resilience with a set of metrics in a state space has the potential to lead to the understanding and engineering of more resilient networks. We plan to continue to develop this preliminary analytical framework and to verify with scenario-based simulations. We would like to acknowledge Egemen Çetinkaya, Daniel Fokum, Justin Rohrer, Marcus Schöller, Paul Smith, Weichao Wang, and Alexander Wyglinski for their comments on this work.

References

[1] J. P. G. Sterbenz and D. Hutchison. (2006) Resilinets web page. [Online]. Available: http://www.ittc.ku.edu/resilinets/index.html

[2] L. Xie, P. Smith, M. Banfield, H. Leopold, J. Sterbenz, and D. Hutchison, "Towards resilient networks using programmable networking technologies," in *Proceedings of IFIP IWAN 2005*, Sophia-Antipolis France, November 2005.

[3] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable mobile wireless networks: issues, challenges, and research directions," in *MobiCom WiSE '02: Proceedings of the 3rd ACM Workshop on Wireless Security*. New York, NY, USA: ACM Press, 2002, pp. 31–40.

[4] J. C. Knight, E. A. Strunk, and K. J. Sullivan, "Towards a rigorous definition of information system survivability," in *Proceedings of the DARPA Information Survivability Conference and Exposition DISCEX III*, Washington DC, April 2003, pp. 78–89.

[5] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead, "Survivable network systems: An emerging discipline," Carnegie-Mellon Sorfware Engineering Institute, PA, Tech. Rep. CMU/SEI-97-TR-013, 1999.

[6] W. D. Grover, *Mesh-Based Survivable Networks*. Upper Saddle River NJ: Prentice-Hall PTR Pearson, 2004, ch. 3.