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 resilience and survivability. We formalize resilience as points in a state space quantifying network characteristics, from which network service performance parameters can be derived. 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 survivable and resilient networks. In this work, we define a *resilient network* [1]–[3] as a network that has the ability to operate and maintain acceptable level of service under the presence of adverse conditions. These include various factors such as: natural faults of network components; failures due to mis-configuration 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 networks thus covers commonly known categories such as challenged, delay- and disruption-tolerant networks, survivable 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 standardized metrics to define the network space. In the following sections, we discuss the use of metrics to represent network states and evaluate their resilience, and then characterize the network as moving through a *state space* consisting of three regions: normal, partially degraded, and severely degraded operations. The goal is to initially characterize network resilience and ultimately to understand how to design and engineer networks with a higher resiliency.

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 resilient networks, 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 a network taxonomy, the first step is to identify the fundamental properties that affect the performance and the resilience of the network. The second step involves deriving a small set of independent metrics. To this effect, we have identified a comprehensive set of network properties that are broadly classified in to six categories as shown in Table I[1]. Ongoing research in this area is focused on deriving a smaller set of independent 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	speed 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 omitted here for brevity.

III. Resilience and Survivability

Previous research efforts [4]–[6] have presented analytical definitions of some resilient properties (e.g. reliability, availability). We use the 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. A comprehensive view of resilience, thus, would require 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 $\bar{\mathbb{X}} = \{x_1, x_2, \ldots, x_i, \ldots, x_n\}$ be the set of n metrics that represent the network state at a given instant. A metric may be a function of more than one parameter as discussed in Table I. Let S_k be the k^{th} state of any given network. This state can be defined using the network metrics as $\bar{S}_k = \{X_{1k}, X_{2k}, \ldots, X_{ik}, \ldots, X_{nk}\}$. A member X_{ik} in the set $\bar{S}_k$ is in itself a range of *valid* values bounded by $\left(x_{ik}^L, x_{ik}^U\right)$, representing the lower and upper limit of the ith metric. We can now define $X_{ik} \equiv \left(x_{ik}^L, x_{ik}^U\right)$. Thus X_{ik} defines the values of ith metric that belongs to the current network state S_k.

Definition A. *If the ith metric of a network at a given instant of time t is x_i^t, then the necessary condition for the network to be in state $\bar{S}_k$ is $\forall \left\{i : X_{ik} \in \bar{S}_k\right\}, x_i^t \in X_{ik}$.*

Now, consider the problem of determining the values of x_{ik}^L and x_{ik}^U. We propose that these values will be determined by the acceptable performance in that particular network state.

Let $\bar{\mathbb{Y}} = \{y_1, y_2, \ldots, y_j, \ldots, y_m\}$ be the set of m serivce parameters that represent the performance of the network in a given state at a given instant. The performance of the network in kth state, $\bar{S}_k$ can be defined as $\bar{P}_k = \{Y_{1k}, Y_{2k}, \ldots, Y_{jk}, \ldots, Y_{mk}\}$. A member Y_{jk} in the set P_k is in itself a range of *acceptable* values bounded by $\left(y_{jk}^L, y_{jk}^U\right)$, representing the lower and upper limit of the jth performance metric. We can define $Y_{jk} \equiv \left(y_{jk}^L, y_{jk}^U\right)$.

Definition B. *If the jth service parameter of a network at a given instant of time t is y_j^t, then the necessary condition for the network to be in a state $\bar{S}_k$ is $\forall \left\{j : Y_{jk} \in \bar{P}_k\right\}, y_i^t \in Y_{jk}$.*

Following the occurrence of an adverse event, the network state stays $\bar{S}_A$ remains in its current *normal* region, as shown in figure 1, if the change in the ith metric, x_{iA}, does not exceed the allowed range $\left(x_{iA}^L, x_{iA}^U\right)$ and the service parameters remain with in *limits* $\left(y_{jA}^L, y_{jA}^U\right)$. 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, the network goes to state $\bar{S}_B$ in which service parameters remain in the limits $\left(y_{jB}^L, y_{jB}^U\right)$. The network may be engineered so that for a given application, both $\bar{S}_A$ and $\bar{S}_B$ lie in the normal operating region where the performance is acceptable. On the other hand, adverse events of higher magnitude may drive the network to a state $\bar{S}_C$ in the partially degraded region with impaired performance, or to a state $\bar{S}_D$ in severely degraded region with unacceptable service parameters. The range of network metrics for which the network will remain in a each state is clearly quantified along with the expected performance in that state.

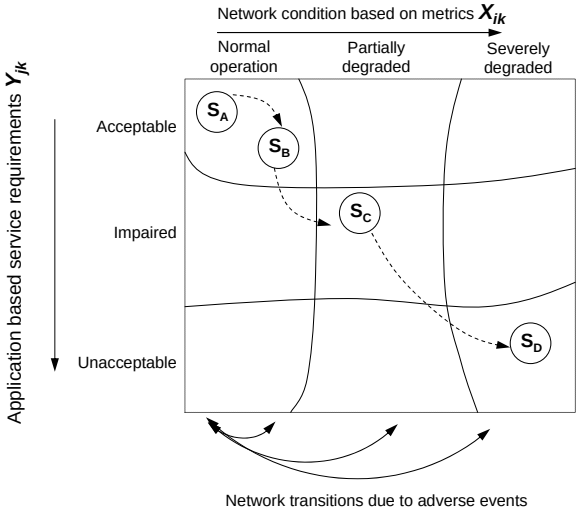

Fig. 1. Network states in the given operating region

IV. Conclusions 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 of, 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 Soshant Bali, Egemen Çetinkaya, Justin Rohrer, 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 *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.